AALBORG UNIVERSITY
COPENHAGEN

Aalborg University Copenhagen
A.C. Meyers Vænge 15
2450 København SV

Secretary: Maiken Keller

Semester:
ICTE4

Title:
Adoption of Human Microchip Implants for Business Organizations

Project Period:
February – June 2019

Semester Theme:
Short thesis project

Supervisor(s):
Morten Falch

Project group no.:
4BUS 4.5

Members
(do not write CPR.nr.):
Arnab Podder 20144269
Kardo Ismail 20135166
Nicolai Olsen 20145273

Pages: 153
Finished: 06.06.19

Abstract:

Since its introduction, the controversial technology of human microchipping has seen limited use, especially in corporate scenarios. The aim of this thesis is to shed light on the adoption and acceptance of human microchipping and to explore how a human microchipping can be applied in a corporate setting in order to reduce one's management burden as well as providing personalization. The rate of adoption is analyzed using Rogers' Diffusion of Innovations theory as a lens through which a survey is conducted to determine factors facilitating or impeding the adoption. Furthermore, relevant legal and regulatory frameworks related to the rights of employees in human microchipping corporate scenarios are investigated. Lastly, a conceptual design along with a simple prototype is developed by applying a security-by-design framework to ensure security and privacy. The aim of the solution is to provide personalization in the office in addition to lowering the general management burden.

ACKNOWLEDGEMENT

A great number of people contributed to the realization of this master's thesis.

First off, we would personally like to thank our main supervisor Morten Falch of the Innovative Communication Technology and Entrepreneurship program at Aalborg University Copenhagen. His insights, knowledge and expertise were of incredible help. He consistently supported our core idea and workflow, steering us in the right direction, when needed.

We would also like to thank our participants involved in our interviews:

- Alexander Kristensen, Marc Göranson-Svare, and Nikoline Christensen of TUI
- Amal Graafstra of Dangerous Things and VivoKey Technologies

Their contribution to this master's thesis has been invaluable. The experience of interviewing them, and presenting our idea, was both exciting and extremely enriching. Their competencies and inputs were paramount in the development of this very project. Is it safe to say that, without their addition, this project would not look the same.

Finally, we must express our deep gratitude to a few more special contributors. Iwona Windekilde for her unmeasurable assistance and inspiration, Szymon Izydorek for his constant support and help and Ivan Gelov for his help and encouragement.

The authors:

- Arnab Podder
- Nicolai Olsen
- Kardo Ismail

Table of Contents

1 Introduction

Microchip implants for pet and agricultural identification use have existed for several years. However, it was not until some years later that the use of implants for humans were explored. Implantable RFID (Radio Frequency Identification) microchips intended for humans were patented in around 1997 with the intention of safeguarding against kidnapping and facilitating prompt medical emergency procedure in case of acute illness (Graveling, Winski, & Dixon, 2018). In 2004, the first human-implantable microchip by the name VeriChip received FDA (Food and Drug Administration) approval as a medical device. Microchip implants are based on RFID technology, which is used in a variety of different applications ranging from passport control to management of toxic and medical waste (Graveling, Winski, & Dixon, 2018). The chips used for implants must be encapsulated within a biocompatible material for human use, which is usually a form of glass. *Figure 1.1* below shows an example of an implantable RFID chip covered in glass.

Figure 1.1: RFID chip shown on top of a hand for scale (Graveling, Winski, & Dixon, 2018).

In this project, the objective is to explore the low adoption of human microchipping thus far. Furthermore, the second objective is to analyze how an innovative human microchip implant service can be developed for business organizations to allow for easy entry to the office building, printing, personalization use cases and more. More specifically, replacing regular ID and key cards and thus reducing one's management burden while also providing features such as personalization.

Thus far, the acceptance levels of microchip implants have been on the lower end. In a study by Graveling, Winski, and Dixon (2018), it was estimated that the number of chips implanted in humans on a global scale is ranging from 3,000 to 10,000. They further stated that the number of companies which have adopted and embraced the technology is very small and is

on a purely voluntary basis. Moreover, the individuals wearing implants seemed to do so for the sake of convenience, such as for opening doors or to show that they embrace the technology. Finally, they found that the most significant adoption of the technology seemed to be that of the Swedish Rail company called SJ allowing the wearers to verify their ticket details using the chips.

The low uptake and adoption of the technology may be due to a variety of different factors. As mentioned by Graveling, Winski, and Dixon (2018), several implications have been identified with the introduction of RFID-implants for humans. First off, legal issues include challenges associated with data protection and human rights legislation. Secondly, ethical concerns related to the inviolability of human dignity and religious concerns. Health and safety concerns have also been expressed in terms of possible carcinogenicity, migration of the implant, interactions with MRI signals and its potential impact on pharmaceutical effectiveness. Lastly, RFID chip technology does not seem to entirely secure, where possible vulnerabilities include eavesdropping, cloning, and unauthorized tag modifications. Several of these concerns will be explored for this project.

1.1 Motivation

The aim of this project is to explore how an innovative human microchipping solution can be developed for business organizations to provide improved convenience and personalization while taking privacy, security and legal aspects into consideration. Additionally, the acceptability of the technology will be investigated to determine the main factors affecting its rate of adoption. To accomplish this, the project is divided into two main parts.

For the first part, in order to investigate the regulatory and legal aspects of adopting human microchipping in a business organization scenario, in addition to determining the rights of potential implanted employees, relevant legislation such as the GDPR (General Data Protection Regulation) and Human Rights regulation will be analyzed. To limit the scope, the focus will be on EU (European Union) regulation.

In addition, the acceptability of the technology will be explored by applying Everett Rogers' Diffusion of Innovations theory. Specifically, the five perceived attributes of innovation will provide the focal point for the analysis. The aim is to shed some light on the factors affecting the rate of adoption, and as a result, identify some of the biggest potential barriers and facilitators affecting the diffusion.

The second part will be concerned with the security and privacy of human microchipping, as there are many concerns and assumptions regarding this aspect. To accommodate this

aspect, a suitable security-by-design framework will be applied during the entirety of the development phase of the solution. Specifically, a proposal for a conceptual design will be presented followed by the development of a prototype. Here, the emphasis will be on getting familiar with the technology and relevant components in a practical way a well as exploring the potential uses of the technology in a business organization setting while taking security and privacy into account.

1.2 Problem Definition

The objective of the project can be summarized in the following problem definition:

How can a solution be developed for business organizations utilizing human microchip implants to improve convenience and provide personalization for employees whilst taking security and privacy into consideration?

- *What does the legal environment look like for human microchip adoption in an enterprise setting within the boundaries of EU?*
- *By applying Rogers' Diffusion of Innovations theory, what are the main elements affecting the rate of adoption among potential adopters?*
- *By applying a security-by-design framework, how would a conceptual design and prototype for the solution look like?*

1.3 Delimitation

To narrow the scope for the legal environment, the boundaries of EU are chosen, which are also applicable to Denmark. Furthermore, the potential health hazards of using human microchip implants will not be investigated deeply, as it is beyond the scope.

The later development phases of the System Development Life Cycle (SDLC), such as implementation, operations/maintenance, and disposal (*Chapter 8.1*), will not be provided in this report. This is because of the conceptual nature of the solution in this present time which results in these phases not being conducted. However, if the solution and its system design were to be approved and adopted by a particular company, then these next phases could be set in motion. Consequently, the Security-by-Design framework is only applied to the three initial development phases; initiation, acquisition and design/development.

The proof of concept developed for this project is created for testing purposes and to become familiar with the components of a human microchipping solution. The result of this is gained

insights, inspiration, and knowledge of the inner working of the microchip and RFID reader devices.

Lastly, the five perceived attributes of innovations from Rogers' Diffusion of Innovations theory will provide the main focal point when exploring the acceptance rate of the innovation.

2 Theory

There are many factors which affect how a new technology or idea is adopted by individuals, as well as many models which aim to identify and explain these. In this chapter, the two popular adoption models and theories known as the Technology Acceptance Model (TAM) and Diffusion of Innovations (DOI) theory will be reviewed, including limitations of each. Out of these two, the DOI theory was selected as a theoretical framework for the project. It was introduced by Everett Rogers and aims at analyzing how innovations spread for adoption along with corresponding main elements which affect the rate of adoption. In addition, an overview of how researchers have applied the theory in similar contexts to that of this project will be presented. Lastly, the way in which this project seeks to apply the theory will be explained. Specifically, the project aims to use the theory to shed light on the acceptance levels of human microchip implant technology in order to identify main factors affecting its rate of adoption.

2.1 Adoption Models and Theories

Several models and frameworks have been developed over the years in order to explain user adoption of new technologies or innovations within a wide range of areas. As put by Taherdoost (2018) in a journal article reviewing adoption models:

> "Technology acceptance models and theories have been applied in a wide variety of domains to understand and to predict users' behavior such as voting, dieting, family planning, donating blood, women's occupational orientations, breast cancer examination, choice of transport mode, turnover, using birth control pills, education, consumer's purchase behaviors, and computer usage." (2018, p. 961)

As such, there are many relevant adoption models to choose from when looking to explore the user adoption of new technologies, be it family planning, computer usage or, in this case, human microchip implants.

Two widely used models were considered for this project; the Technology Acceptance Model (TAM) and the Diffusion of Innovations (DOI) Theory.

Let us first consider TAM. As Lai explains (2017), Davis used the model to explain computer usage behavior as well as determinants of computer acceptance in 1989. The basic model included the main beliefs of Perceived Usefulness and Perceived Ease of Use. Perceived Usefulness refers to the potential user's subjective likelihood that the use of a certain system will improve their action. Perceived Ease of Use refers to the degree to which a potential user

perceives the system to be easy to use. In other words, if a user finds a system useful to them and easy to use, then they will be willing to use it (Ajibade, 2018).

As Chuttur (2009) suggests, the model has been criticized for its poor theoretical relationship between the different constructs in the model, since the intention of a potential user may not be representative enough of the actual use of the system. Furthermore, according to Bagozzi (2007), the model is too simple and leaves out some important variables and processes. For these reasons, the TAM was dismissed as a suitable model for exploring the adoption of human microchip implants in this project.

Having reviewed TAM, let us now consider Rogers' DOI theory. This model looks at the way or manner in which innovations spread for adoption. According to Ismail (2006), this is one of the most popular adoption models. Also, it has been used extensively in a broad range of disciplines such as political science, public health, technology, economics, etc. Furthermore, it is widely used as a theoretical framework in the area of technology diffusion and adoption (Ismail, 2006). Moreover, the theory has been applied before in a similar context by Michael and Michael (2010), in which the poor uptake of RFID implants for access control was analyzed using Rogers' DOI theory. This study will be delineated in a subsequent section.

As this project aims at exploring the diffusion and adoption of human microchip implants, DOI theory was selected as the theoretical framework for the study. However, similarly to the TAM, the DOI theory also has a number of limitations. One of these limitations, as mentioned by Rogers (2003) is the so-called recall problem. Inaccuracies may occur when respondents are asked to recall the time at which they adopted a new idea. However, this will most certainly not be an issue in this project, as human microchip implants are still in its early diffusion stage, meaning only a small percentage of people have adopted the technology.

The DOI theory has also been criticized for using the same set of attributes for all innovations, even though these innovations may be vastly different from each other (Lyytinen & Damsgaard, 2001). This is quite important to take into consideration as human microchip implants are arguably very different from, for example, a new TV.

As suggested by Meyer (2004), most studies using the theory have been focusing on a single innovation as opposed to a cluster of innovations. Furthermore, investigators have mostly been collecting data at a single snapshot in time, and often in a post-diffusion scenario. For this project, the focus will also be on a single innovation, human microchip implants, at a certain point in time. Contrary to the majority of studies, this study will explore the adoption rate in the early diffusion stages, in order to better understand the underlying factors affecting the adoption rate of the innovation.

In the following subchapter, a more in-depth overview of the DOI theory will be delineated.

2.2 Rogers' Diffusion of Innovations Theory

Diffusion of innovations is a theory which seeks to explain in what way or manner innovations spread for adoption. As defined by Rogers (2003):

> "*Diffusion* is the process by which (1) an *innovation* (2) is *communicated* through certain *channels* (3) over *time* (4) among the members of a *social system.*" (2003, p. 11)

As such, he argues that the following four main components affect the process of diffusion of innovations:

1. *Innovation*
2. *Communication channels*
3. *Time*
4. *Social system*

Rogers (2003) describes an innovation as the following:

> "An *innovation* is an idea, practice, or object that is perceived as new by an individual or other unit of adoption. It matters little, so far as human behavior is concerned, whether or not an idea is "objectively" new as measured by the lapse of time since its first use or discovery. The perceived newness of the idea for the individual determines his or her reaction to it." (2003, p. 12)

In other words, it does not matter to what extent an idea is considered to be new as measured by the lapse of time since it was first used or discovered. The important factor is to what extent the individual perceives the idea as new.

In addition, there are five different perceived attributes of innovations, which can help explain different rates of adoption of innovations (Rogers, 2003). These will be described more in-depth later in this chapter.

The second element to consider in the diffusion process is that of communication channels. As argued by Rogers (2003), communication must take place in order for an innovation to spread:

> "Diffusion is a particular type of communication in which the message content that is exchanged is concerned with a new idea. The essence of the diffusion process

> is the information exchange through which one individual communicates a new idea to one or several others." (2003, p. 18)

As such, communication channels are a necessity for an innovation to spread. According to Rogers (2003), interpersonal channels, involving a face-to-face exchange between two or more individuals, are the most effective in terms of persuading an individual to accept a new idea or innovation, particularly if these individuals share socioeconomic status, education and so on.

Time is the third element of the diffusion process. As argued by Rogers (2003), it is involved in diffusion in the innovation-decision process, the innovativeness of an individual and an innovation's rate of adoption.

The so-called innovation-decision process is a process in which an individual goes from first knowledge of an innovation to forming an attitude toward this innovation, to a decision to either adopt or reject, to implementing and using the innovation and lastly to confirmation of the decision (Rogers, 2003). This can be conceptualized as the following five steps: knowledge, persuasion, decision, implementation, and confirmation.

Rate of adoption is another way in which the element of time is involved. This metric is defined as the relative speed with which an innovation is adopted by members of a social system (Rogers, 2003).

Rogers (2003) explains that by plotting the number of individuals adopting an innovation on a cumulative frequency basis over time, the result is an S-shaped curve as seen in *Figure 2.1* below. Here, only a few individuals adopt the innovation in each time period at first. These are called the innovators. Once approximately 10-20% adoption is reached, the curve starts to take off as more and more individuals adopt the innovation in each following time period. Eventually, the curve starts to level out as the number of people who have left to adopt the innovation decreases. Lastly, as the curve becomes horizontal, the diffusion process is finished.

It is worth noting that the slope of the S-curve varies from innovation to innovation, as some ideas may diffuse at a more rapid pace than others (Rogers, 2003).

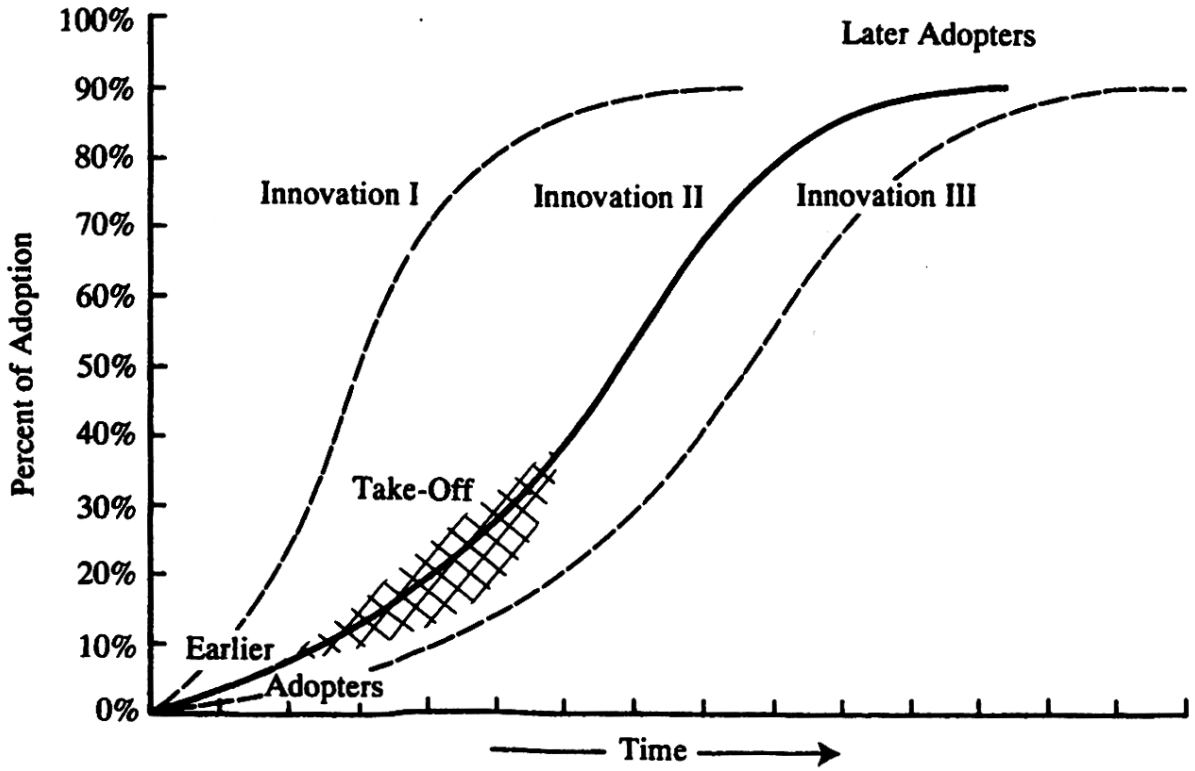

Figure 2.1: The process of diffusion (Rogers, 2003).

The fourth and final main element mentioned by Rogers (2003) is the social system. He defines such a system as a set of interrelated units which are engaged in joint problem solving to accomplish a common goal, where the members could be individuals, organizations, etc. An example of a social system could be doctors in a hospital or all consumers in a country. As put by Rogers (2003):

> "Diffusion occurs within a social system. The social structure of the system affects the innovation's diffusion in several ways. The social system constitutes a boundary within which an innovation diffuses." (2003, p. 24)

As such, the social structure of the system has an influence on a new idea's diffusion. In addition, other elements such as norms within a social system, the role of opinion leaders and change agents, and the type of innovation-decisions also affect the diffusion of innovations (Rogers, 2003).

The norms within a social system may vary greatly from system to system. Norms can be seen as established behavior patterns for the members of a social system and tell them what behavior they are expected to perform (Rogers, 2003). An example could be different contraceptive behavior from village to village in close proximity of each other, resulting in different levels of adoption of family-planning methods, even though one might think the levels would be similar.

Within a social system, the type of innovation-decision is also important. Rogers (2003) distinguishes between the following three types:

> "(1) *optional innovation decisions*, choices to adopt or reject an innovation that are made by an individual independent of the decisions of other members of the system, (2) *collective innovation-decisions*, choices to adopt or reject an innovation that are made by consensus among the members of a system, and (3) *authority innovation-decisions*, choices to adopt or reject an innovation that are made by relatively few individuals in a system who possess power, status or technical expertise." (2003, p. 38)

So, a distinction can be made between optional decisions (where the individual has nearly complete responsibility for the decision of adoption), collective decisions (where the individual has a say in the decision), and authority decisions (where the adopting individual does not have any say in the decision). Generally, the latter yields the fastest rate of adoption of innovations (Rogers, 2003).

Having described the four main elements of diffusion of innovations, let us now consider the first element, innovation, in greater detail. As previously mentioned, Rogers (2003) describes five different characteristics of innovations, as perceived by individuals, which can help to explain their different rates of adoption. These are as follows:

- *Relative advantage* (Rogers, 2003) is the extent to which an innovation is perceived to be better than the technology or idea it supersedes. The greater the perception of its relative advantage is, the faster the rate of adoption will be.
- *Compatibility* (Rogers, 2003) is the degree to which an innovation is considered to be consistent with the existing values, past experiences, and needs of potential adopters. If an idea is incompatible with the values and norms of a social system, it will not be adopted as rapidly. An example of incompatibility could be the use of contraception in countries where religious beliefs discourage the use of contraceptive methods.
- *Complexity* (Rogers, 2003) is to be understood as the extent to which an innovation is perceived as being difficult to understand and use.
- *Trialability* (Rogers, 2003) is described as the degree to which an innovation may be experimented with on a limited basis. Generally, the greater the degree of trialability, the greater the rate of adoption. For example, a farmer who can experiment with new seeds will be more likely to adopt the new idea as less uncertainty is present.

- *Observability* (Rogers, 2003) is the extent to which the results of an innovation are visible to others. The easier it is for other individuals to see the results, the greater the likelihood of adoption. For example, home computers have relatively low visibility to other individuals, which in turn reduces the speed of diffusion.

As argued by Rogers (2003), past research indicates that the above five perceived attributes of innovations are the most important indicators when explaining the rate of adoption. Specifically, the first two attributes, relative advantage, and compatibility are particularly important when analyzing the rate of adoption for an innovation.

As seen in *Figure 2.2* below, the rate of adoption is also dependent on other variables beyond the aforementioned perceived attributes of innovations. This includes the type of innovation-decision, so whether it is an optional, collective or authority decision to adopt the innovation. Furthermore, the communication channels, the nature of the social system as well as the promotion efforts of change agents are also variables affecting the rate of adoption.

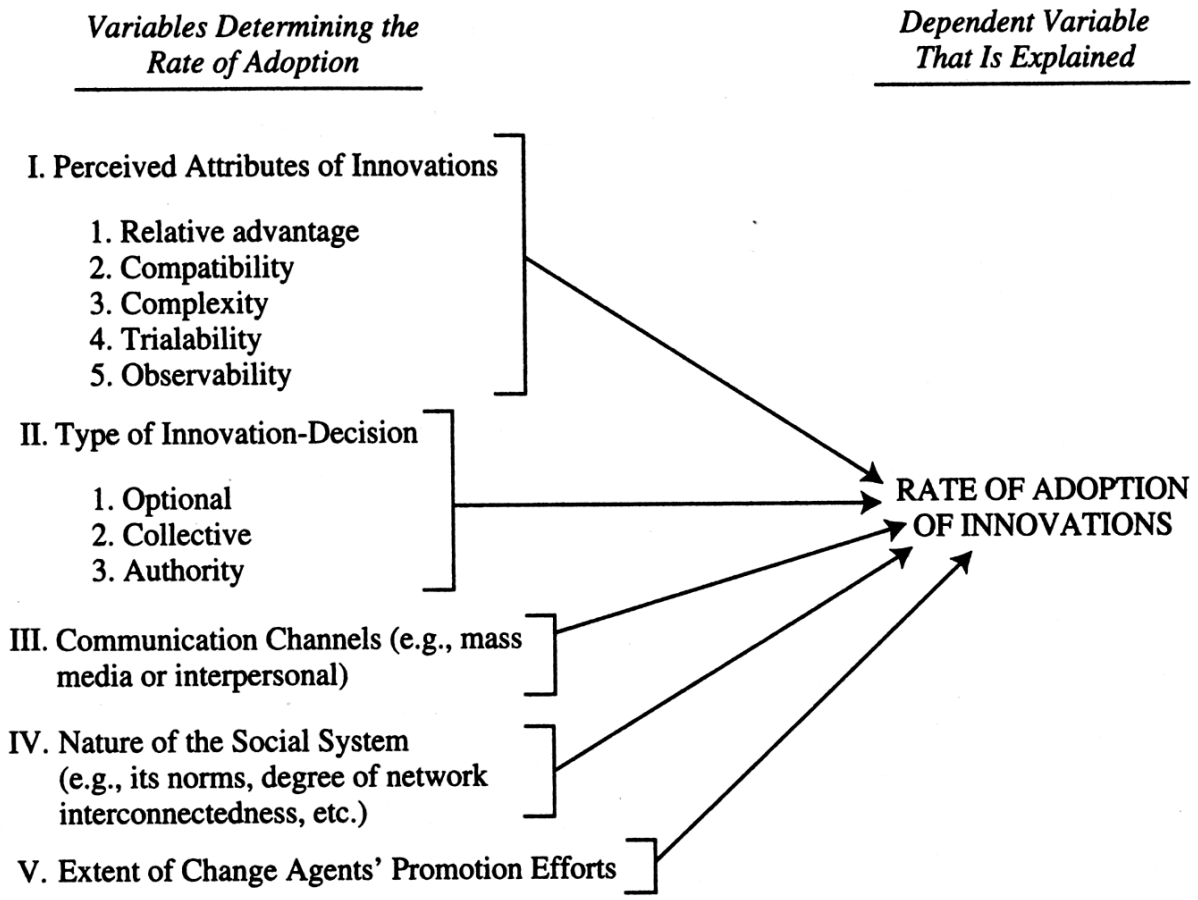

Figure 2.2: Variables determining the rate of adoption of innovations (Rogers, 2003).

For this project, the perceived attributes of innovation will be the focal point in order to shed light on the rate of adoption of human microchip implants.

2.3 Applying the Theory

In this chapter, synthesis articles of existing research will be presented. Furthermore, a specific paper in which researchers used Diffusion of Innovations theory in order to explore why the adoption of implantable RFID solutions has been so slow for access control use, will be presented. Lastly, an overview of how the theory will be applied for this project will be detailed.

In a meta-analysis conducted by Kapoor, Dwivedi, and Williams (2014), 226 relevant innovation articles were studied to identify trends pertaining to Rogers' five perceived attributes of innovations. The findings were discussed in direct relation to guidelines on a hypothetical ideal study adopted from a meta-analysis journal article by Tornatzky and Klein (1982) on innovation characteristics and innovation adoption-implementation.

In the meta-analysis, Kapoor, Dwivedi, and Williams (2014) found that the majority of the studies were retrospective with a focus on the adoption of an innovation. Additionally, the studies preferred using quantitative data in the shape of surveys and questionnaires. Nearly all studies explored multiple perceived attributes of an innovation as opposed to only one. Out of these, a high proportion only considered one innovation, primarily with an organization as the unit of adoption as opposed to individuals.

As per Tornatzky and Klein (1982), the ideal study should be predictive as opposed to retrospective. They argue that this is due to the fact that perceived attributes of an innovation may be affected by the perceiver's knowledge of that decision of adoption or rejection. This is interesting considering the majority of studies analyzed in the meta-analysis conducted by Kapor, Dwivedi, and Williams (2014) were of retrospective origin, and as a result, do not adhere to this criterion.

Kapoor, Dwivedi, and Williams (2014) also concluded that the perceived attributes of relative advantage, compatibility, and complexity were the most important ones when determining adoption. These findings closely resemble the argument previously presented by Rogers, as he argues that according to research, competitive advantage and compatibility are the most important attributes when analyzing the rate of adoption of an innovation (Rogers, 2003). However, Rogers omits the attribute of complexity in his argument.

Let us now consider an actual study conducted in a context similar to that of this project. In a case study by Michael and Michael (2010), they applied DOI theory in order to analyze why the uptake of implantable RFID solutions has been so low for access control applications. They chose the case study approach and looked intensively at one specific case, a bar in Spain, to observe phenomena which could shed light on the current situation of low adoption

of implantable RFID microchips. In this study, a retrospective approach was chosen similar to the majority of other studies as previously mentioned. Data collection for the case study was provided via an interview with a former employee at the club who was responsible for the implementation as well as exhaustive online documentation. The way in which the data was analyzed was by applying the five perceived attributes of innovations defined by Everett Rogers: relative advantage, compatibility, complexity, trialability, and observability.

In the paper, Michael and Michael (2010) found that the complexity of the technology during trialability is what may have led to its poor uptake. However, they also pointed out that the slow rate of adoption may only be a short-term trend. In addition, the paper also ponders on what factors might need to be overcome in order for widespread diffusion to occur of the technology.

For this project, the five perceived attributes of an innovation will be the focal point for the analysis, similar to that of Michael and Michael (2010), albeit in a predictive approach and using a survey method. According to Rogers (2003), these five attributes have been the most extensively investigated and have been found to explain around 50% of the variance in innovation's rate of adoption. Specifically, an approach in which the acceptability levels of the innovation is investigated in its early diffusion stages will be conducted. To investigate this, a survey of potential adopters' perceived attributes of human microchip implants will be conducted. The aim is to shed some light on how potential users perceive human microchip implant technology at this point in time, and as a result, explore which factors may be impeding and facilitating the rate of adoption of this innovation.

In the following chapter, an overview of the methodology for this project will be presented.

3 Methodology

In this chapter, the methodological approach for the project is presented. In order to visualize the interlinked steps performed over the duration of the project, a diagram was created displaying the interrelated blocks representing different steps. The project is divided into two main parts. In the first part, relevant theory was applied in order to investigate the rate of adoption and identify some of the potential barriers. In addition, relevant technologies and legislation were investigated. In the second part, focusing on implementation, a conceptual design and prototype were developed integrating a security-by-design framework. Here, the knowledge acquired from the technology background section laid out the foundation.

3.1 Overview of Methodology

As shown in the figure below, the blocks represent the methodological flow throughout the project. Shortly after the topic was chosen, the sequential step was to gather and review literature of relevance. This was the first step in the first part of the project. This led to the choice of a theoretical framework to use for investigating the adoption of the technology. In addition, a relevant framework to incorporate security by design was chosen. The literature review also led to a state of the art section covering research conducted by other researchers in the field as well as relevant technologies. Also, security, ethical and legal concerns were explored. Following the state of the art section, the legal environment for human microchip technology was assessed in addition to the creation of a technology background section. In addition, an analysis based on Rogers' Diffusion of Innovations theory was conducted through surveying potential adopters. These components concluded the first part. Looking into the second part, focusing on implementation, the knowledge acquired in the technology background section combined with the security by design framework, led to a conceptual design and prototype of the proposed microchip solution. Finally, a discussion and conclusion were conducted based on the findings throughout the project, in terms of the legal environment, rate of adoption and technological aspect, in which the project was put into perspective and the problem formulation was answered.

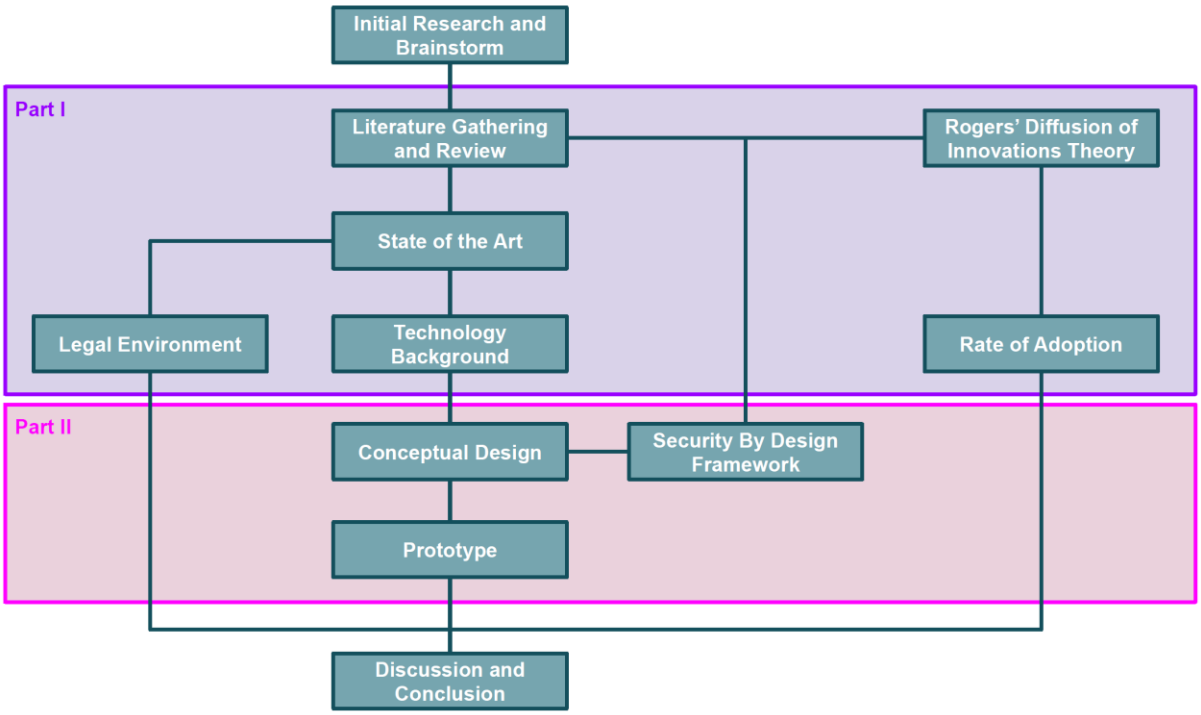

Figure 3.1: Overview of methodology (own figure).

3.1.1 Part I

In this section, the blocks related to the first part of the project will be presented in more detail. This part consists of the initial literature gathering and review process. The review led to the choice of the theoretical framework to subsequently analyze the rate of adoption of human microchip technology as well as a state of the art section. The first part also includes a technology background section, based on the state of the art, to provide the foundation for the implementation part, Part II. Lastly, the legal environment in the context of human microchips in a workplace scenario was explored.

3.1.1.1 Literature gathering and review

After the topic of human microchip implant technology had been chosen, the scope was subsequently identified. Enterprise and business adoption was chosen as the focus since the technology has yet to see many applications in this environment.

Once the topic and scope had been defined, a suitable problem definition was formulated. Here, the thought process was to look at different relevant aspects, such as regulation, rate of adoption and technical aspects. The first aspect was looking at the legal environment of the technology, in order to get an overview of the regulatory landscape and identify any challenges to consider when developing a human microchip implant solution for workplace scenarios. To

accommodate this, the project looked at relevant legislation such as the GDPR and human rights laws.

The second aspect was to look into the rate of adoption of the technology. In order to investigate this, a suitable theoretical framework was chosen. Specifically, Rogers' Diffusion of Innovations theory was chosen in order to shed light on the rate of adoption and potential barriers slowing down the adoption of the innovation.

As for the technical aspects of the problem formulation, the aim was to acquire a deeper understanding of the main technologies related to human microchipping and explore how these could be applied in a workplace setting in order to provide convenience and personalization in a secure manner.

For the initial research phase, the databases of IEEE, Scopus, Google, and Google Scholar were used to obtain and review relevant literature to provide the foundation for the state-of-the-art section. In addition, different relevant adoption models were reviewed before choosing Rogers' Diffusion of Innovations theory.

3.1.1.2 State of the art

After the subject of human microchipping had been chosen for this thesis, it was realized that this technology is yet to be adopted in a mass scale in a conventional way. So, a guideline or a roadmap was required to guide the thesis in its desired outcome. The Food and Drug Administration (FDA) approved human microchipping in 2004, but the question arises, what are the obstacles this technology has faced for not having been adopted on a wide scale.

After the problem formulation had been framed for this thesis which focuses on the challenges such as legislative regulation, adoption of the technology by Rogers' Diffusion of Innovation theory, security concerns, etc., the state of the art chapter was formulated to present the initial research touching multiple aspects to provide the preliminary knowledge necessary for the progress of this thesis. The RFID technology which is the backbone of the microchipping solution has been analyzed with the perspective of this thesis. Emphasis was also given on different forms of identity and access management techniques using RFID to figure out the distinction between the existing technology and the human microchipping. Since RFID technology is classified into 3 main types and each solving different use cases, it was important to establish the focus area to be investigated further in the due course of the thesis.

Among different factors which impeded the adoption of this technology were the religious beliefs and ethical considerations. It was important for the thesis to understand those barriers

which proved to be quite a hindrance. After the initial investigation, it was decided not to analyze deep in these aspects as it is not the primary focus of the thesis.

After the introduction of GDPR, it was realized to consider the legislative and privacy issues concerned with the project scope. Since the solution will be designed for the workplace in different enterprises, it was important to analyze the legal obligations on part of the employer and the right of the employees who had adopted the chip. This was further investigated on the perspective of GDPR and other European laws and legislation protecting the rights of the employees in a separate section of the project.

The final part that was investigated was the security and the privacy issues since it is important to protect the data on the chip from intruders and thus different security issues were presented and further researched in the course of the thesis.

3.1.1.3 Rate of adoption and data analysis

Having chosen the theoretical framework of Rogers' Diffusion of Innovations theory, the project decided to use the perceived attributes of innovations for investigating the rate of adoption. This led to a survey in order to determine the perceived attitude of different attributes by potential adopters. This resulted in a substantial data analysis section in which key areas which may reduce the rate of adoption were identified.

Interviews were also conducted with early adopters of the technology. Here, the objective was to learn more about their motivation for adopting the technology, both from the perspective of customer (TUI) but also as a service provider (Dangerous Things and Vivokey Technologies), as well as learning about potential issues in terms of use or security. One interview was conducted in person, whereas the other one was conducted online due to the person being located in the United States. The transcripts of the interviews can be found in the appendix. An attempt was also made to interview the biggest service provider of human microchips in Sweden, Biohax International, who also happens to be a piercer. However, due to scheduling conflicts, this interview was not conducted.

3.1.1.4 Technology background

In the initial research from different literature and State of the Art analysis of different existing RFID access and authentication mechanisms, the project decided to perform a deep investigation into the different parts of the RFID technology. From the State of the Art analysis, the focus was more on investigating the following identified keywords.

- RFID Technology and Architecture

- Passive RFID
- RFID Standards
- Power Considerations
- RFID Protocol

After gathering the overall knowledge related to RFID, the next phase was to put all the emphasis on the RFID implant technologies including the design and architecture and other relevant considerations.

3.1.2 Part II

In this section, the second part of the project will be presented. This includes the choice of framework to ensure security by applying a security-by-design (SBD) approach. In addition, the conceptual design and prototype processes will be delineated.

3.1.2.1 Security-by-design framework

The development of a microchip web solution is dependent on security considerations and requirements being applied in each step of the development phase. The reason for this is that the proposed solution is a web service that enables easy access to facilities and facility technologies. Without the implementation of security in the development phases, it would result in the solution negatively impacting the overall security posture of the system. Furthermore, technologies such as the microchip, do cause a lot of security concerns and risks, that needs to be identified and mitigated. The consequence of this is that using regular development frameworks which are only concerned with the functional requirements e.g. SDLC (Systems Development Life Cycle), will result in an inadequate conceptual solution which would not be a responsible solution to propose. So, it was necessary to use a development methodology with security-by-design principles. The security-by-design principles are defined by the Open Web Application Security Project (OWASP), as being a security development framework, where security is integrated and considered in every part of the development phases, in order to ensure and secure the confidentiality, integrity, and availability of the system (OWASP, 2016). This security-by-design framework and how to apply the security processes are presented and described in *Chapter 8.*

3.1.2.2 Conceptual design and prototype

Information regarding the technologies behind the microchip and RFID, together with gathered input from interviews, were used to propose and develop a conceptual microchip web solution. The conceptual solution was developed using the system development life cycle. Furthermore,

the development of the solution includes the security-by-design framework, which is introduced in *Chapter 8*. The development phases of the solution began with the specification and definition of functional requirements. Thereafter, came the Acquisition phase where the technologies that are a part of the system are defined, assessed, and acquired. This then lead to the Design phase where the functional requirements were modeled and designed into the final conceptual solution.

Microchips and microcontrollers were acquired, in order to provide a proof of concept regarding the aspect of the microchip together with the RFID (Radio Frequency Identification) enabled access control device. This device was built from the bottom up using an Arduino board and IDE (integrated development environment) to program some of the functional requirements of the solution. The proof of concept developed in this project was for inspiration and solution testing purposes.

The SBD framework has processes in each of the SDLC development phases. The processes' activities for phases 1, 2 and 3 are provided and described in each of the corresponding development phases in *Chapter 9*.

4 State of the Art

Human microchipping or a human microchip is a form of either an integrated circuit (IC) or a Radio Frequency Identification (RFID) tag encapsulated in a silicon case which is typically the size of a grain of rice implanted in the body of a human being (Techopedia, n.d.-a). The chip contains a unique identification number which can be retrieved from an external database for several purposes like personal identification, access management, medical history, payment system, etc. (Wahlquist, 2017). Though microchip implantation on pets exists a long time ago, it was in 2004, when the US Food and Drug Administration (FDA) approved the RFID microchip for human use after looking into the privacy and the confidentiality issues of the patient bearing the microchip implant (in-Pharma, 2017). From 2004 until now, not a significant effort has been made to promote and develop this technology. There is a number of reasons behind it. Some of them are legal issues, ethical considerations, health and safety risks, security issues, etc. (Brown, 2016). There are a few organizations who have already adopted the human microchipping as a voluntary approach with their employees. It is expected that in the coming days, this technology is going to be adopted in more use cases. This chapter is mainly divided into three sections. The first section will present the existing RFID technology along with its use in different forms in different use cases very briefly since a broad overview will be presented in the next chapter (*Chapter 5*). The second section will discuss the legal issues with the implantation of a microchip in the human body followed by the ethical considerations and the medical issues. The final section will discuss the security issues that need to be considered as the chip can be quite vulnerable to the hacker without any proper security measures.

4.1 RFID Technology

The technology used for human microchipping is the implantable Radio Frequency Identification (RFID) chip which generally comes in two forms (Bright Alliance Technology, n.d.). Passive (read-only) as opposed to the most sophisticated active devices where additional data can be added to them and used mainly for medical purposes. This section will briefly present the basic overview and function of implanted passive RFID tag generally used for the workplace use cases like access and authentication. The RFID chip used as a part of a system has four components.

- *RFID chip*: RFID chip is also known as a tag which stores information about the chip bearers and transmits this information on request of the RFID reader when the signal with the correct frequency is sent to the chip by the reader (Chen, 2015). Since the

chip plays both the role of a transmitter and responder, it is classified as a transponder. The RFID chip is implanted in the human body for a number of applications depending on their use cases. As already mentioned, the chip is passive (read-only) in nature, so it gets its power from the electromagnetic wave emitted from the reader.

- *RFID reader*: The RFID reader broadcasts the electromagnetic signal to which an RFID chip operating at the same frequency can respond to with the encrypted signal. The encrypted signal can be decoded by the RFID reader and then pass the information to the network using it (Techopedia, n.d.-b).
- *Network*: The RFID reader sends the decrypted information to the network which then transmits it to a computer for processing. Sometimes, the network part is skipped and a simple interface is used between the reader and the computer (Graveling, Winski, & Dixon, 2018).
- *Computer*: It controls the RFID reader with the software. The information received from the network is processed by the computer and allow the operator to make a decision (Graveling, Winski, & Dixon, 2018).

The type of information that is transmitted depends on the type of application. Since this thesis is more focused on the application where RFID chip is implemented for identification, the type of information must be identification code which is processed and analyzed where it is installed. The overall RFID operation of the passive RFID device can be explained with the following figure (*Figure 4.1)*.

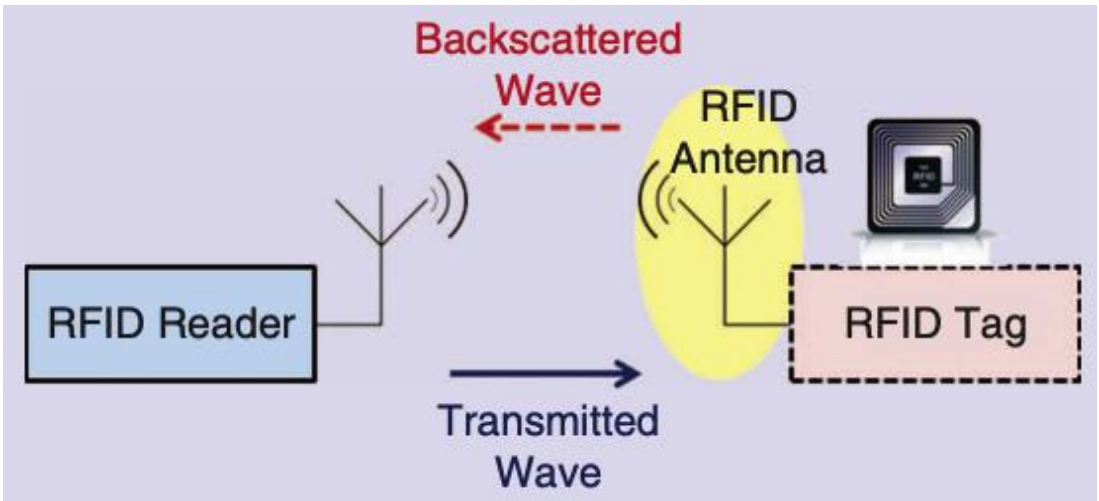

Figure 4.1: The operation principle of a passive RFID device (Kiourti, 2018).

The following section will discuss some of the medium used for identity and access management purposes in different use cases using RFID as a key component.

4.1.1 RFID smart card and tags

The use of smart cards for accessing the door control is quite common in many places and organizations which ensures the expected level of protection. It can also track the flow of people in a building or crowded place like a stadium. The operation of the chip is quite simple as discussed in the previous section (*Chapter 4.1*). Here, the smart card contains the data encoded on the machine-readable RFID chip. As soon as the card comes close to the reader antenna, the data is transmitted by the RFID chip and the user is identified (Papiewski, n.d.).

The integration of access control smart card with other applications can deliver a lot of value to the organization and its members. The convergence of identity and access management also enable a layered security approach across the organizations which counter different security threats along with fulfilling compliance requirement like the GDPR (EdgeConnector, n.d.).

There are a few benefits of using RFID smart cards and tags:

- *Low Cost***:** The cost of the RFID smart cards is quite cheap where the main expense lies in the electronic reader, locks, computers, and software (Papiewski, n.d.).
- *Data Security***:** Data recorded on the chip can only be readable with the special equipment meaningful to one's own organization. Even if the card gets lost, the information cannot be used without the detailed knowledge of the organization's security (Inner Range, 2017).
- *Flexibility***:** The existing RFID card can be reprogrammed with new information without replacing the existing one. For example, if the employees got promoted with more security clearance, the security department can just update the card without issuing a new one (Kaur et al., 2011).

However, there are some security concerns with it which are:

- *Copied, Cloned or Spoofed***:** RFID smart cards can be easily copied, cloned or spoofed and thus make it quite vulnerable in respect to security threat (Gaille, 2015).
- *Lost or stolen***:** RFID smart cards canbe easily lost or stolen which required the card to be deactivated immediately (Smith, 2017).

Many companies use the state of the art technology to provide solutions in multiple use case. One such company is Tigrisnet which will be presented in the next section.

4.1.1.1 Tigrisnet smart card solution

Tigrisnet is a solution integrator who provides different solutions according to the needs of the customer. They provide multiple solutions in the Telecom industry and in recent time, they offer smart security solution including smart card technology and access control which has been found to be interesting for this thesis for solving similar use cases (Tigrisnet, n.d.-a).

Tigrisnet has multiple smartcard solutions ranging from the government to the health sector (Tigrisnet, n.d.-b). Since government project demands high security and card protection, so it gives the security concern the highest priority in developing their solutions. The smart card solutions for the government include National ID, driving license and military cards. The biometric information is embedded in the smart card chip provided by the Tigrisnet. Besides that, they also provide payment card solutions in the financial sector in the form of debit cards and credit cards. The smart card encoding option developed by them allows the client to personalize the e-payment card instantly beside the security and quality required by the customer (Tigrisnet, n.d.-c).

Besides smart card and tags, the wearable RFID has gained a significant market share in recent times and will be discussed in the next section.

4.1.2 Wearable RFID

Wearable technology is another form of medium which will play a big role in the future of access management control in the organization (Ocampo & Ambrose, 2015). There are various forms of wearables available today ranging from wrist band to headset etc. The underlying technology in those devices are mostly RFID, NFC (Near Field Communication) or WiFi and the choice of this technology depends on the range of the communication and the data volume. Here, the WiFi represents the longest range followed by Bluetooth while the RFID and NFC represent the short range and low data rate solution (Marie-Sainte et al., 2016). Most wearable technology depends on some form of wireless communication to send the data captured by the sensor to an information gateway like a computer. The operation of RFID tag in the wearables is similar to that in the smart card. Looking at some of the merits which are quite distinguishable from the smart card and tags are the following.

- *Staying connected***:** Unlike smart card solutions, the wearable can alert the user with messages, notifications, phone calls and many other integrated IoT (Internet of Things) functions in one device (Humavox, 2016).

- *User Interface***:** Wearables more often come with the user interface option like touch screen which enables them to give input and control the options in a much convenient way and thus helps in customizing the information (Medynskiy et al., n.d.).

But, the advantages in the features sometimes comes with certain cons which are:

- *Price***:** Wearables are much expensive compared to the smart card and thus quite a problem to produce in a large number for big organizations (CLODOC, 2017).
- *Battery life***:** Battery life is also a critical issue which requires day to day charging and is thus quite frustrating (CLODOC, 2017).

One of such organizations is Stark RFID who provides RFID tag and wearables and will be presented in the following section.

4.1.2.1 Stark RFID

Stark RFID is an enterprise who are RFID system integrator and solution provider. They are one of the industry's leading RFID solution provider in event and venue management (Stark RFID, n.d.-a). One of the distinct product developed by the Stark RFID is the RFID wearables for event or venue management. It uses the UHF (Ultra-High Frequency) Generation 2 RFID tags for high-speed data transfer and longer read range (Stark RFID, n.d.-b). It helps tracking people in event and venue management. Stark RFID also introduces customize RFID LED (Light-Emitting Diode) wristbands which replace the barcode ticket and credentials in managing access controlled venues. They can also be programmable for layered access control and social media integration and thus ideal for events like concerts. RFID wristbands have faster access management and soon it will obsolete the barcoded tickets (Stark RFID, n.d.-b).

Apart from the RFID access control, there are different biometric access control used in many organizations today.

4.1.3 Biometric access control system

Biometric is a science of measurement and analysis of biological data (Thakkar, n.d.). This data contains the unique characteristics of the human body and serves as an excellent parameter in the process of identification, verification, authentication and access control. The biometric characteristics include fingerprints, eye retinas, face recognition, voice patterns, etc. The most common form of biometric character that is implemented in many restricted premises is the fingerprint access control. It is also used to record employees attendance. The biometric system is mainly a pattern recognition unit which has an emphasis on gathering the specific

type of biometric data with relevant features from the individuals and compares it with features from the present group of attributes in the database (ThomasNet, n.d.). Then it performs its action based on the accuracy of the comparison whether to accept or reject the request. Biometric access control mainly consists of four types of components: a sensor device, a quality assessment unit, a feature comparison, and a matching unit and a database.

Some of the standalone features in the biometric access control system which is quite efficient compared to other access system mentioned above are presented below.

- *Security*: It provides extra security with its unique biometric character for every individual (PC Dreams, 2016).
- *Maintenance Cost*: The maintenance cost is quite low compared to other solution once the installation is complete.
- *Two-factor authentication*: Generally does not require additional authentication mechanisms unless it demands to protect high-value security with an additional keypad to enter the password (FERMAX, 2017).

However, there are some disadvantages in installing the biometric access system in the organizations.

- *Convenience*: Quite inconvenient for organizations where the employees been repeatedly changed and expect a large number of outside visitors in the course of the day (Best Quality Services Singapore, 2018).
- *Cost of installation*: Although the maintenance cost is lower, the cost of installation is quite expensive (PC Dreams, 2016).

The following section will discuss one of the leading biometric solution in the world named Bayometric.

4.1.3.1 Bayometric

Bayometric is one of the leading global providers of fingerprint scanners, biometric software solutions, and services (Bayometric, n.d.-a). The product and solutions developed by Bayometric help organizations like government agencies, integrated application developers to meet their security, identification, and access management requirements (Bayometric, n.d.-b). There is a multiple of products offered by Bayometric which includes fingerprint reader, digital fingerprint scanners, fingerprint access control system and fingerprint time and attendance system. They also develop biometric identification software which is integrated into the biometric applications (Bayometric, n.d.-a).

The next section will discuss another form of authentication and access mechanism which is gaining some momentum in recent years: the human implanted chip.

The first human-implanted RFID chip available in the market was developed by the Digital Angel Corporation which is a subsidiary of the VeriChip Corporation (Foster & Jaeger, 2008) and will be presented in the following section.

4.1.4 Human-implanted chip by VeriChip Corporation

The United States Food and Drug Administration (FDA) has approved the human-implanted microchip developed by the VeriChip Corporation in 2004. VeriChip first introduced the Verichip Health Information Microtransponder System called Verimed and classified it as a Class II medical device (Foster & Jaeger, 2008). For the medical purpose, Verimed is implanted under the skin of the patient which contains a unique identification number that the emergency personnel in the hospital can scan the microchip to identify the patient and access the health information for immediate treatment without any delay (MD Magazine, 2007). But, due to the poor acceptance of this product which is primarily due to the privacy concerns, in July 2010, the marketing of this product was discontinued. Despite that, PositiveID, which is the parent company of VeriChip still makes the implanted chip available for specific customers (Prutchi, 2011).

Apart from the introduction of Verimed, Verichip also introduces a non-medical application of human-implanted RFID chip called Veriguard which control individual access in secured areas. Veriguard found its utility in a variety of areas such as security, financial, emergency identification and other applications. The Veriguard secure access control reader contains a high power RFID antenna enclosed in a plastic panel mounted near a doorway or building entrance. The Veriguard scanner reads the implanted VeriChip by transmitting a low-frequency radio signal and receive the returned radio signal by the Verichip transponder. Both the software and the hardware work together in the Veriguard system to authenticate personnel authorized to enter in a restricted area. The Veriguard secure access control system can even track both the location and the movement of the authorized person in the perimeter of the restricted access area (Business Wire, 2003). In 2004, the Attorney General of Mexico and at least 18 of his staffs adopted this technology to gain access in areas with sensitive data (Foster & Jaeger, 2008).

Another company who has introduced the Internet of Things with the implanted microchip is a Swedish company name Biohax International which will be presented in the following section (Michael, Michael & Ip, 2008).

4.1.5 Biohax International

Biohax International is a microchipping company based in Sweden, a country which is known for its technological advancement and more than thousands have already inserted a microchip in their hand (NPR, 2018). With the implementation of this chip associated with a number of applications, Biohax international has made the IoT possible with human microchipping (Nanalyze, 2017). The company offers its employees to be implanted with microchips with functionalities like swiping card to open doors, operate printers with hand gestures (CNBC, 2017). But, this new technology also raises some security and privacy issues. It can track employees when they come to work or what they buy and thus compromises their privacy to some extent.

In 2015, the Swedish rail company SJ became the client of Biohax and the Swedish rail conductors started scanning the hands of the passenger for scanning the paperless or electronic ticket linked with the implanted chip (Jefferson, 2017).

Biohax is also offering its microchip services to several renowned UK companies who are planning to offer microchip implants to their employees. The aim of those companies with microchip implant is to make everyday tasks faster which includes buying food, entering premises or restricting access to certain areas (Wolfe, 2018).

Another organization named Dangerous Things, which is a biohacking company who focused on human augmentation through implanted devices is presented in the following section.

4.1.6 Dangerous Things

Dangerous Things is a biohacking retailer who sells kits which contains everything needed to implant an RFID tag in the body (Thompson, 2015). Dangerous Things let users choose between the RFID or NFC chips depending on the use cases. RFID tags are typically used to replace the keys and passwords to enter restricted area like home or enter the car or log on to the laptop. On the other hand, NFC chips functionalities include storing vCards (Virtual Cards) or Bitcoin wallet address among many other things (Grauer, 2018). Dangerous Things sells a different variety of chips. Among them, the two most important chips are elaborated further.

Dangerous Things 125 KHz xEM chip has programmable memory space with additional security features. It allows the user to program or clone a tag’s ID.

xNT is an NFC compliant RFID tag that is implanted underneath the skin in hand. It allows the device to use the radio frequencies to send and receive data wirelessly to another device enabled with NFC tag (Soper, 2013).

The 13.56 MHz xNT chip of Dangerous Things operates at a higher frequency and is based on the NTAG216 chip. NTAG216 have been developed by NXP Semiconductors as standard NFC tag in wide market application like retail, gaming and consumer electronics (NXP, n.d.). It contains 888 bytes of user programmable memory and a 32-bit password protection security features (Grauer, 2018).

The xNT tag is encased in a 2mm x 12mm cylindrical bioglass which is sterilized in ethylene oxide gas (Soper, 2013).

4.1.7 VivoKey

VivoKey provides a platform for digital identity, authentication and a cryptographic payment application which is secured with implantable NFC devices underneath the skin (KSEC Solutions, n.d.-a). It is developed by KESC solution which provides open source tool and a range of service (KSEC Solutions, n.d.-b). KESC provides a range of RFID/NFC solutions which can integrate different applications and the implants allow to connect different applications as a keyless access card. VivoKey focuses on the power of cryptography using traditional security token but removes the hassle of managing or carrying it whenever anyone goes by replacing it with a chip implant (KSEC Solutions, n.d.-a). It literally works against the malicious way of intruding the cryptographic key and thus help it from getting stolen or lost.

VivoKey is also partnered with Fidesmo, which is a multi-application platform with an ambition to replace every card in the wallet and key with a single device (Fidesmo, n.d.). Fidesmo also allows the developer to develop their own Java Card application and directly deploy in the VivoKey. This gives the user ultimate control and flexibility in the implanted VivoKey platform.

It has been discussed before, that though the human microchipping came into existence since 2004, but among many reasons, one of them was ethical considerations which proved to be a hindrance in the conventional use of it. The following section will discuss the ethical considerations involved in human microchipping.

4.2 Ethics of Human Microchip Implants

The ethical considerations surrounding the implantation of a chip in human bodies is quite complex and often overlap with others concerned aspects like medical risks as well as privacy and security concerns along with the legal parameter which will be presented in the following sections of this chapter. As already pointed out before regarding the privacy and security concerns with the RFID chip, the ethical debate questions the value and the need for RFID in public goods. This is quite a fact that, most of the consumers are unaware of the RFID

technology in this chips and what information these RFID chips are storing and transmitting and who is receiving this information and how the information is being used (Chen, 2015). In this section, only the primary ethical concerns related to human microchipping will be presented.

4.2.1 Safety

One of the major areas of ethical concern that every organization has to consider before introducing the human microchipping to its employees is to ensure safety. It is the responsibility of the employer to address the health and safety of its employee who gave consent to the chip implantation (Khan, 2015). So, if there is any possible consequences or side effects that the employer is aware of, they must reveal to the employees before they give consent for the implantation (Foster & Jaeger, 2008). As argued by Roosendal (2012), it is required to hold someone responsible if the chip causes damages to the host.

Another aspect related to safety is considered on the issue of physical health which includes the safe removal of chip and deactivates it on the termination of the employment contract.

4.2.2 Efficacy

It is an ethical practice for the organizations to declare whether they are promoting the chip implantation for the convenience in the workplace or they are enhancing security in the organizations which is also termed as 'Truth in Advertising' (Foster & Jaeger, 2008). The ethics of giving moral considerations less priority than business security is always questionable, even though the individual privacy and security associated with human microchipping are properly addressed.

4.2.3 Privacy

It is always been a concern of compromising privacy with human microchipping. This depends on how and where the chips are used and the possibility of tracking the chip bearer in some way which is considered as an interference in the privacy. With the introduction of the GDPR in the European Union, this is no longer remain a privacy or dignity issue, rather it becomes a legal issue as well with the ownership of data fetched from the chip (Graveling, Winski, & Dixon, 2018). Apart from that, the informed consent is also the criteria for the GDPR and it will also raise some questions as to how such consent will be given and how the organizations will safeguard the data of the vulnerable individuals.

4.2.4 Religious beliefs

There are many religions around the world whose beliefs are strongly against the insertion of an implant. The insertion of such a chip without choice is also considered a form of religious discrimination and even unacceptable in the strongest medical ground. So, religious belief is considered a strong ethical challenge for this project (Graveling, Winski, & Dixon, 2018).

As seen from the previous section, there are many ethical considerations which are also a part of legal and legislative concerns in organizational jurisdiction and a brief discussion will be presented in the next section.

4.3 Legal Implications of Human Microchipping

From the previous section, it is quite clear that the acceptance of human chip implantation will be challenged by a number of ethical as well as legal implications. Although the FDA approved the use of human microchipping back in 2004 as mentioned in the introduction, the main legal challenge in the compulsory implant of RFID chip will be data protection and human right legislation. In European Union, there is no specific legislation which banned or refrain the use of RFID human microchipping but, there are regulatory laws related with the storing, processing and the use of data by this RFID chip. With the introduction of EU general data protection regulation (GDPR) in May 2018, the requirement of consent from the employer is required which establishes an informed description and indication of the data being processed (Graveling, Winski, & Dixon, 2018).

The power of an employer to microchip its employees in their organization in EU countries is governed by the principle and laws of EU labor law and human rights law. The key areas of these laws will be addressed in a later chapter (Chapter 6).

The final section will look into different security concerns associated with human microchipping.

4.4 Security Aspects of Human Microchipping

A biometric method like human microchipping is always considered to offer more security and convenience compared to other identification methods available today. Several identification and authentication mechanisms as discussed in the previous sections are mostly hand-carried objects or access cards which can be stolen, forgotten, misplaced. The integration of RFID technology with biometric aspects like human implantation enhances the accuracy and security of biometric identification and the data can be easily accessible by a reader on RFID

enable objects. Now, the biggest challenge is to control the huge junk of information which is mostly personal information and that leads to policy and privacy issues (Perakslis & Wolk, 2006). Currently, there are few threats which compromise the system security and user privacy and are presented in the following section.

4.4.1 Security issues

The following are the few dominant issues in regard to RFID security.

- *Eavesdropping***:** It is a technique in which the hacker observe the data send from the RFID tag to the reader or vice versa. It is very difficult to detect since the hacker uses passive means to communicate without emitting any signal. One way to countermeasure this issue is to encrypt the signal so that the hacker can not understand it (Rotter, 2008).

- *Unauthorized Tag Cloning***:** It is a form of attack in which the attacker clone or duplicate the RFID tag which has similar functionality. The functions may include accessing the restricted data or modifying it and even may carry out a transaction on behalf of the user. One way to counter this attack is to introduce the tag authentication and also measures can be taken on the circuit manufacturer to protect the tag from duplication by reverse engineering (Smiley, 2016-a).

- *Man-in-the-middle attack***:** Between the actual tag and the reader, if a foreign object pretends to be either a tag or a reader. Some of the technique includes fake readers at the door or eavesdropping device near the legitimate reader. The countermeasure techniques already discussed for the previous issues are also effective to fight this attack (Smiley, 2016-a).

- *Unauthorized Tag Disabling***:** When an unauthorized device disables a legitimate tag and can not be utilized again and thus perform a denial of service attack (Rotter, 2008).

- *Replay Attack***:** As seen from the unauthorized cloning which can be countered with an authentication mechanism but this authentication mechanism can be abused with the replay attack. Here, the attacker uses the clone tag and repeat the authentication sequence. To do that, the attacker or the intruder must obtain the information beforehand when the tag and the reader exchanged the information in normal communication. One way to counter this attack is to implement the challenge-response protocol in which the tag evaluated its authentication code based on the challenge sent by the reader (Mitrokotsa, Rieback, & Tanenbaum, 2010).

Apart from the different security issues and solutions in respect to RFID technology mentioned in the previous section, there are some additional privacy concerns in reference to the RFID implants in general and is presented in the following section.

4.4.2 Privacy risks of RFID implants

The privacy risk of RFID implant slightly differs from that of other contactless tokens used for authentication, access, and other payment options. Some of the privacy concerns are listed below.

- RFID implants are predominantly linked to a person's personal information which makes it quite prone to the privacy information and in worst scenario make the person towards physical danger (Gasson, Kosta, & Bowman, 2012).
- The RFID implants answer a reader request with a unique identifier which is linked with absolute certainty to a physical person. This is unlike the case of other RFID tokens where the association cannot be ensured and it allows people to share the access card or the car keys. But with RFID implants, the random set of owners are reduced to one and can thus facilitate traceability (Gasson, Kosta, & Bowman, 2012).

4.5 Subconclusion

This chapter is quite important to build the founding block for this thesis. It makes a multidimensional approach to look into different aspects of human microchipping. The knowledge gathered from different aspects helps the thesis to narrow its focus on the subsequent chapters. In the early research phase of the thesis, it was found that, though the concept of microchip implant started a long time ago, the acceptance of this technology remains subdued for other reasons like ethical, legal, medical and other security aspects. Several other applications of RFID technology has also been researched to figure out the importance of human microchipping than other wearable technologies. From the presentation of ethical and legal analysis, it was found that these factors need to be taken into consideration for the final implementation of our solution in the workplace scenario. From this point, the main focus area of this thesis which found out to be the RFID technology and the legal and regulatory environment will be elaborated further in the coming chapters.

5 Technology Background

In recent time, the market based on Radio Frequency Identification (RFID) technology has witnessed significant innovation and growth with the introduction of several applications which includes payment system, authentication, and access control, device tracking, etc (Thrasher, 2013). Human microchipping which is the main area of this thesis is also based on RFID technology. This chapter will present RFID in details along with a description of different parts. The architecture along with the system design will be discussed in the course of this chapter. The detailed analysis of RFID technology is quite important to understand the role and its impact on human implanted microchipping among other applications based on RFID.

Although the use of RFID technology has gained momentum in a large number of applications in recent years, the technology has been in use over a decade. The allied and the enemy aircraft used to be distinguished by RFID technology during the Second World War. Since then, the RFID tag has found its applications for many purposes (Roberti, 2005). In 1969, passive radio transponder with stored memory was invented by Mario Cardullo and the central component of this radio transponder is now used as an automatic payment system in toll booths (Global Venture, n.d.). Agricultural industry found the application of RFID in tracking and monitoring the livestock in the 1980s (Adrion, 2018). In 1984, the technology was used in the automotive industry for assembly purposes. In the ’90s, RFID technology was widely used in for supply chain management purposes.

5.1 Overview

This section will look into the various aspect of Radio frequency identification technology which ultimately will be narrowed down to passive human-implantable RFID devices. However, it is important to understand RFID in its entirety in order to get an overall understanding of the technological aspects.

RFID technology is broadly speaking about wireless use of radio frequency electromagnetic fields to read and transfer data, with the aim to automatically identify and track tags to attached objects (Dimov, 2014). As mentioned earlier, the market for RFID technology is rapidly increasing and is adopted and advancing in many industries not only human microchipping but also many others such as in retail stores to prevent shoplifting. Here, ID badges with an RFID transponder are used to notify the shops when a “customer” walks out of the shop without paying (Dimov, 2014). Further, it is used for supply chain management which allows producers to track the progress of a product through the entirety of the process. For example, the automotive industry where progress is monitored throughout the assembly line (Dimov,

2014). Other worth mentioning examples that famously are using RFID technology are Livestock or pets for identification and tracking, as well as in casinos to identify counterfeit chips and all this and much more thanks to the advancing RFID industry (Dimov, 2014).

The so-called passive RFID basis is built upon two main discoveries. Firstly, the development of crystal-based radios which cleared the way for a tag to power itself (Chen, 2015). The way this is done will be thoroughly explained later on, but for the time being it can be said that, crystal set radios use energy contained in the radio frequency signal to move a diaphragm in the headset of the radio allowing people to listen to radio broadcasts outside big cities without electricity in the 20th century (Chen, 2015) and this phenomenon will be explained later called mutual induction (*Chapter 5.5*).

The second major discovery that laid the foundation for the development of far-field passive RFID devices is in the field of radar technology, which was developed in the second world war. The radar technology works by receiving backscattering signals from enemy aircraft and sailing vessels, From a scientific perspective, every object reflects RF signals back but an RFID tag can change the characteristics of the signal by changing the matching at the connection between the chip and the antenna making up the tag (Chen, 2015). Again, this part will be described later in the next subchapter. The next subpart will break up analyze and thoroughly describe the integral parts and its functions that together make up the passive RFID tag & reader. Before dive deep into the different components of RFID, it is important to present the backscatter communication which is the means of communication between different RFID components.

5.1.1 Backscatter communication

Backscatter communication is based on the principle of reflection of radio waves by objects. A backscatter communication system consists of two components. An RFID tag which is also called the backscatter node and an RFID reader which is either transmitter or receiver (Roy & Boyer, 2014). A passive tag as discussed in *Chapter 4* contains an antenna which stores the energy from the reader signal and creates the carrier wave to communicate with the reader as seen in *Figure 5.1*. The energy receives by the tag depends on the distance between the reader and the tag, the transmitted power of the reader and the efficiency of the RFID tag antenna. The tag does not use any active RF components but it is the reader which actually use the RF electronics to produce a sinusoidal wave signal and demodulate the backscatter.

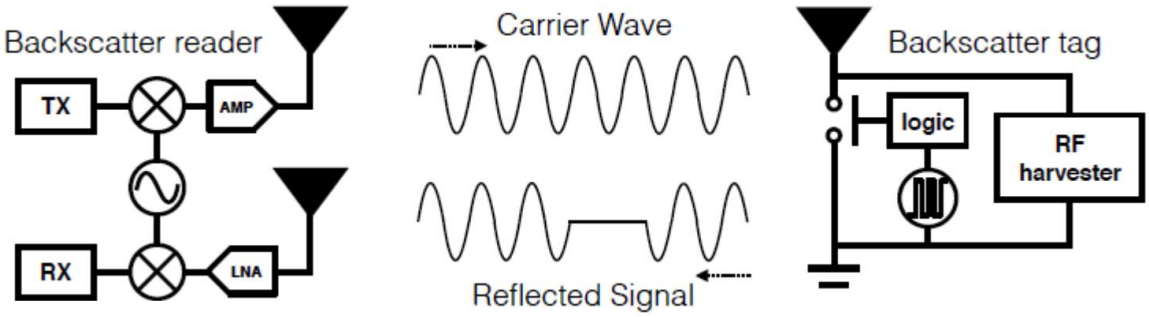

Figure 5.1: Operation principle of passive RFID device (Zhang, n.d.)

The following section will now present the RFID technology and architecture in a much broader way.

5.2 RFID Technology and Architecture

RFID stands for Radio Frequency Identification. In this technology, the digital data is encoded in a smart level or RFID tag which is captured by a reader via means of radio wave (ABR, n.d.). The data captured by the reader is stored in the database. RFID mainly consists of 3 components:

- RFID tag
- RFID reader
- Antenna

5.2.1 RFID tag

An RFID chip is an electronic tag which communicates and exchange data with RFID reader through radio waves (Techopedia, n.d.-c). An RFID tag consists of two main parts:

- An *antenna* which receives the RF waves and
- An *Integrated Circuit* (IC) for processing and storing data

RFID tags are classified into three main types:

- *Active*: Active RFID tags are battery powered tags that broadcast their own signal continuously. They are more expensive compared to passive tags but provides a much longer range with larger memory. They are generally used in large assets like containers and cars which need to be tracked over a large distance. There are two types of active RFID available today which are transponders and beacons (Smiley, 2016-b).

- *Semi Active/Semi Passive***:** This tags have batteries but only activates when they are in the reading range. It communicates with the reader using backscatter communication like passive RFID as explained in *Chapter 5.1.1*. (RFID Journal, 2011). The battery used here is mainly to power the sensor and run the chip circuitry. The battery allows more energy to be reflected from the reader antenna to the interrogator and thus provides a longer range compared to ordinary passive tag.
- *Passive***:** As already mentioned in *Chapter 4*, passive RFID is used in the human implant devices and thus have a special significance for this thesis. With no power source and no transmitter, passive tags are much cheaper compared to the active RFID tags. Their read range is relatively shorter depending on the frequency from few inches up to 30 feet. Since the passive tag has no power source, the tag reader or the interrogator power the communication with the tag (Sisodiya, n.d.). The transfer of power from the reader to the tag can be done in two ways either through inductive coupling or electromagnetic coupling which is explained in detail in *Chapter 5.5*.
    - *Operating frequency***:** Passive Tag can operate at (Danish Technological Institute, 2016):
        - *Low Frequency***:** 124 kHz, 125 kHz or 135 kHz
        - *High Frequency***:** 13.56 MHz
        - *Ultra High Frequency (UHF)***:** 400-960 MHz

5.2.2 RFID reader

RFID reader or the interrogator are devices which collects data from the tags. They are connected to a network and use Radio Frequency (RF) wave to activate the tags. The activated tags then send a wave back to the reader where it is read or translated. The range of transmission of a tag with a reader depends on the frequency used and it is not a requirement for the RFID tag to be scanned directly or aligning to the line of sight with the reader (Rouse, 2018).

The following image (*Figure 5.2*) shows the general architecture of the RFID reader.

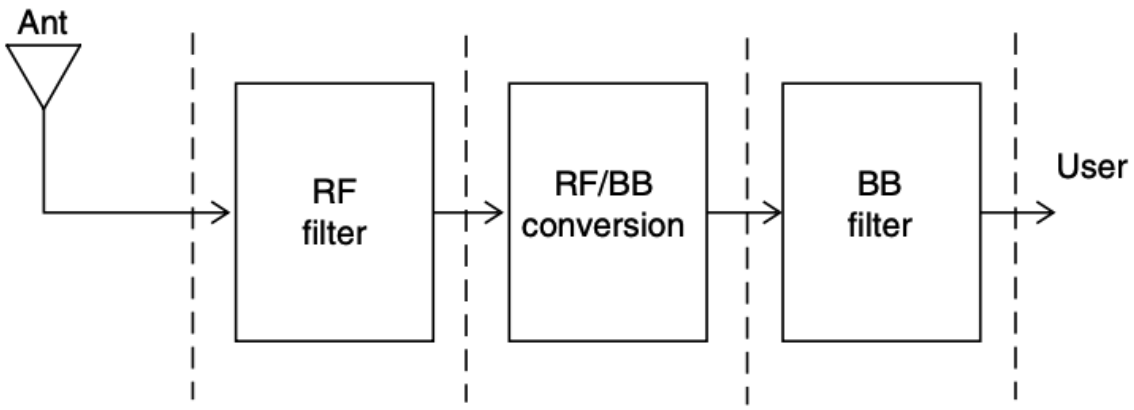

Figure 5.2: Simplified architecture of the RFID reader (Ahson & Ilyas, 2008)

The RFID reader consists of many analog components. The radio signal received by the antenna is amplified by the low noise amplifier (Ahson & Ilyas, 2008). A mixer and a local oscillator convert the RF signal into a baseband (BB) signal. The RF filter and the BB filter are shown in *Figure 5.2*. They are used to separate the signal outside the frequency band.

5.2.3 RF antenna

The RF antenna which is contained in the RFID tag as discussed in the backscatter communication (*Chapter 5.1.1*) mainly exists in two forms.

1. *Omnidirectional* which emits RF energy in all directions.
2. *Directional* which emits RF energy in a specific direction.

The nature of antenna suitable for RFID is quite important to consider especially for the operation of passive RFID which operates in a power constrained environment (Ahson & Ilyas, 2008). The power required for the passive tag is obtained from the electromagnetic wave (*Chapter 5.5*) and the choice of antenna provides the maximum power transfer to the load.

After presenting the architecture and different components of RFID, it is important to define the different RFID standards which makes it possible to use in a variety of applications on a much wider scale.

5.3 RFID Standards

The different elements of RFID are defined by a number of industry standards which make it possible for different manufacturers to make the same product for different manufacturers and thus achieve the economies of scale. RFID standards are guidelines for product development and use. Guidelines include how RFID systems works, their operating frequency, how the reader and the tag communicates and how the data is transferred (Impinj, n.d.). As already

explained in the previous section (*Chapter 5.2*) that, RFID architecture consists of a tag, reader, and antenna, which is quite possible to be manufactured by different companies but need to be operated together. RFID is governed by two main international RFID standard organizations:

- ISO (International Standards Organisation)
- EPCglobal - Electronics Product Code Global Incorporated

The main RFID ISO standards can be summarised in the figure below (*Figure 5.3*).

RFID STANDARDS

RFID STANDARD	DETAILS
ISO 10536	ISO RFID standard for close coupled cards
ISO 11784	ISO RFID standard that defines the way in which data is structured on an RFID tag.
ISO 11785	ISO RFID standard that defines the air interface protocol.
ISO 14443	ISO RFID standard that provides the definitions for air interface protocol for RFID tags used in proximity systems - aimed for use with payment systems
ISO 15459	Unique identifiers for transport units (used in supply chain management)
ISO 15693	ISO RFID standard for use with what are termed vicinity cards
ISO 15961	ISO RFID standard for Item Management (includes application interface (part 1), registration of RFID data constructs (part 2), and RFID data constructs (part 3).
ISO 15962	ISO RFID standard for item management - data encoding rules and logical memory functions.
ISO 16963	ISO RFID standard for item management - unique identifier of RF tag.
ISO 18000	ISO RFID standard for the air interface for RFID frequencies around the globe
ISO 18001	RFID for item management - application requirements profiles.
ISO 18046	RFID tag and interrogator performance test methods.
ISO 18047	The ISO RFID standard that defines the testing including conformance testing of RFID tags and readers. This is split into several parts that mirror the parts for ISO 18000.
ISO 24710	Information technology, automatic identification and data capture techniques - RFID for item management - Elementary tag license plate functionality for ISO 18000 air interface.
ISO 24729	RFID implementation guidelines - part : RFID enabled labels; part 2: recyclability of RF tags; part 3: RFID interrogator / antenna installation.
ISO 24730	RFID real time locating system: Part 1: Application Programming Interface (API); Part 2: 2.4 GHz; Part 3: 433 MHz; Part 4: Global Locating Systems
ISO 24752	System management protocol for automatic identification and data capture using RFID
ISO 24753	Air interface commands for battery assist and sensor functionality
ISO 24769	Real Time Locating System (RTLS) device conformance test methods
ISO 24770	Real Time Locating System (RTLS) device performance test methods

Figure 5.3: RFID ISO Standards (Electronics Notes, n.d.-a).

Apart from that, another standard body named Auto-ID consortium was set up by a number of industrial companies in association with MIT and they classify a series of classes for RFID tag (Electronics Notes, n.d.-a) which are presented below.

- *Class 0*: Basic read-only passive tag which uses backscatter communication and the tag was programmed at the time of manufacture.
- *Class 1*: It has the same features as Class 0 but, the tag has one-time non-volatile program capability.

- *Class 2*: Passive backscattered tag with 65k of read-write memory.
- *Class 3*: Similar to class 2 but a battery is incorporated to increase the range.
- *Class 4*: Active tag with battery including extra functionality in the tag and provides power to the transmitter.
- *Class 5*: Classified as an active tag that provides additional circuitry to communicate with the tags belong to Class 5.

The above presentation of different standard bodies or organizations are quite significant to understand the governance of different RFID tags, now different protocols are developed to describe the specifications of the reader and tag communications which are implemented to encourage global adoption. Since the thesis is more focused on passive RFID as mentioned earlier, the following section will present the important passive RFID protocol.

5.4 Passive RFID Protocols

As discussed in *Chapter 5.2*, RFID technology uses different radio frequencies to identify different tags. The RFID system functions with the reader sending and receiving information at the same time from different tags in the range of the antenna. So, when more than one tag transmits at the same time to the reader, then their backscattered signal cancels out each other which results in a collision. This results in a loss of identification time and the power consumptions of the reader increases (Cmiljanic, Landaluce, & Perallos, 2018).

Generally, RFID collision problem can be classified into two types:

1. *Reader collision***:** When one reader tries to communicate with the tags that are in communication range of another reader, then reader collision occurs (Technovelgy, n.d.). It results in signal interference when the fields of two or more readers overlap. Another problem that can arise is the multiple reads of the same tag. This phenomenon can be depicted with the below diagram (*Figure 5.4*).

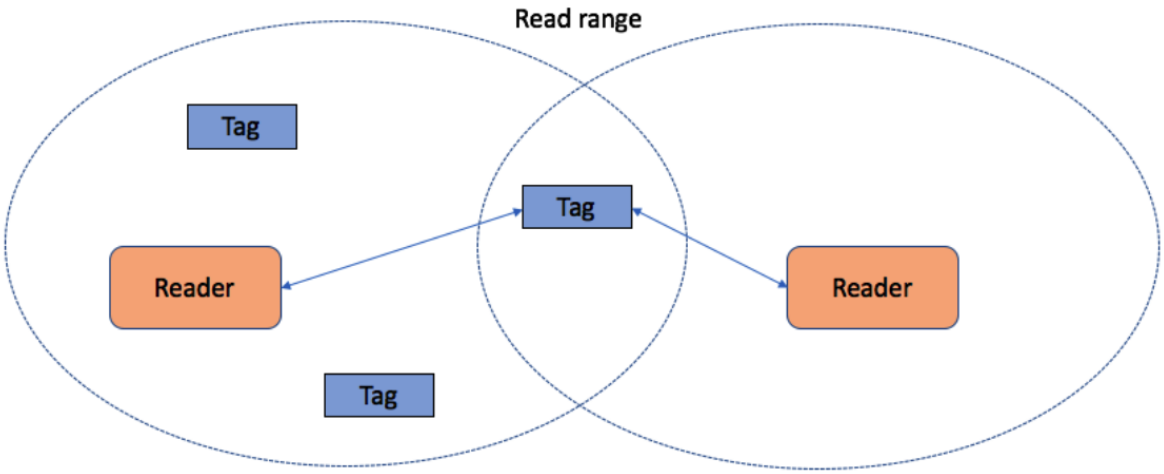

Figure 5.4: Reader Collision (Cmiljanic, Landaluce, & Perallos, 2018)

2. *Tag Collision*: When more than one tag transmits its ID at the same time, a tag collision occurs which results in a mixture of tag signal which reader cannot read. It results in multiple tags reflects back to the reader in the exact same time frame which results in data confusion and false identification (GAO RFID, n.d.). This phenomenon is represented with the below diagram (*Figure 5.5)*.

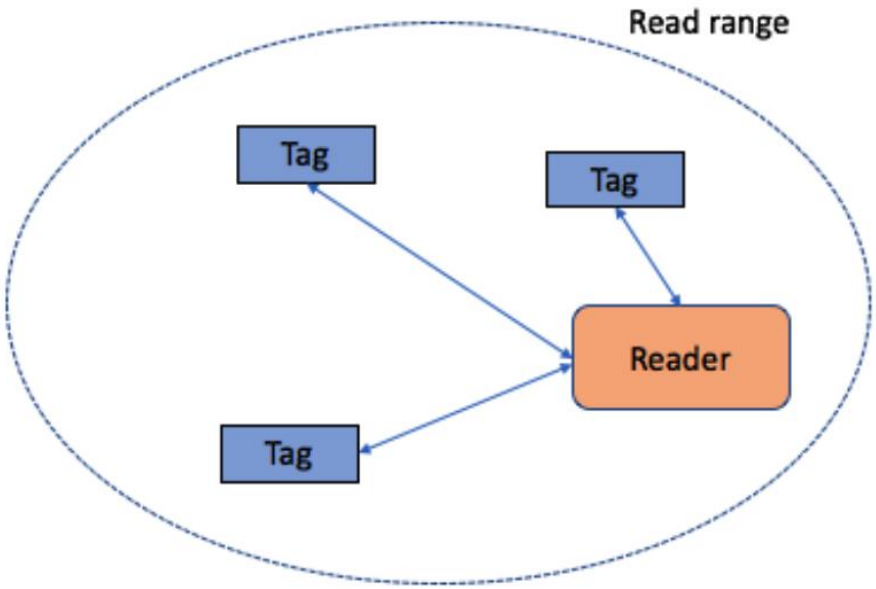

Figure 5.5: Tag Collision (Cmiljanic, Landaluce, & Perallos, 2018).

It is not possible for low functional passive tags to neither detect the collision nor to identify its neighboring tag and thus rise for a need of a tag anti-collision protocol which can recognize the tag with few collisions and can perform its function in real time (Ahson & Ilyas, 2008).

5.4.1 Anti-collision protocols

Tag anti-collision protocols are classified into two broad categories.

- *Aloha-based Protocol***:** It is based on a random access strategy to successfully identify the number of tags in the reading range or the interrogation area (Cmiljanic, Landaluce, & Perallos, 2018). In order to minimize the possible collision, the tag communicates with their own ID in randomly selected slots in a frame and thus they belong to the group of the probabilistic protocol. But, there is no guarantee of identification of all the tags in the interrogation process. This protocol also has a limitation which is known as tag starvation problem which implies that the tag will not be correctly read during the interrogation process due to excessive events of collision with other tags. The tags can only respond once in each frame with a certain number of slots given to every frame (Cmiljanic, Landaluce, & Perallos, 2018).

- *Tree-based Protocol***:** Unlike Aloha-based protocol, the tree-based protocol is designed to identify the whole set of tags in the interrogation area (Cmiljanic, Landaluce, & Perallos, 2018). This protocol functions based on queries which are actually broadcast commands transmitted by the reader and the tag respond on these queries. Comparing the query with the tags ID, the reader command is either rejected or accepted and so the collision can be avoided (Cmiljanic, Landaluce, & Perallos, 2018).

As seen from the earlier discussion regarding the functionality of passive RFID which is quite dependent on the transfer of power from tag to the reader. So the following section will now discuss the power source or the energy consideration required for the passive RFID tag.

5.5 Power Resource Considerations

The previous section describes the use of passive RFID tag implemented in different applications which functions in a power constraint environment. For powering the passive RFID implanted device, wireless techniques are used which overcome different limitations of the battery like lifetime, reliability and the size since it is as small as the size of a grain. The electromagnetic field generated from the reader is the only source of power supply to the passive transponder (Ahson & Ilyas, 2008). Currently, there are two techniques used for wireless power supply to the passive RFID chip and will be presented in the following sections.

- *Inductive Coupling:* The power required by the passive implanted transponder can be provided by the RFID reader through inductive or near field coupling. Through inductive coupling, energy is transferred from one circuit to another via mutual inductance between the circuits (Electronics Notes, n.d.-b). The RFID inductive coupling requires both the tag and the reader to have induction or antenna coils. When the RFID tag is placed close to the reader, the tag coil and the reader coil will couple and the voltage

will be induced in the tag which will be rectified and power the RFID tag circuit as shown in the figure (*Figure 5.6*) below (Electronics Notes, n.d.-b).

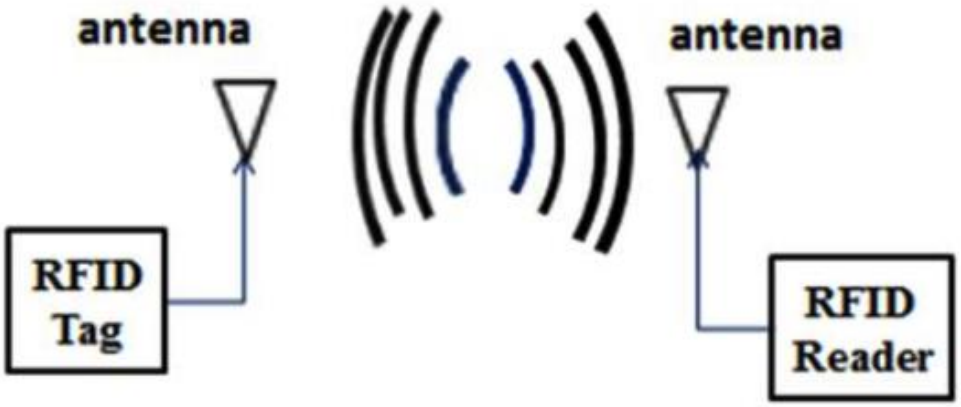

Figure 5.6: RFID system based on inductive coupling (Zahran et al., 2016).

- *Electromagnetic Coupling*: To power the RFID chip, this technique is based on the electromagnetic wave propagates from the antenna in the far field region. This way the tag is energized and generally, some of the power transmitted by the reader gets reflected by the tag after changing some of the properties (Electronics Notes, n.d.-b). RFID backscattering signal, as discussed in the earlier section, operates outside the near field region unlike inductive coupling and the radio signal propagates away from the RFID reader. On signal reaching the RFID tag, it interacts with the ingoing signal and a portion of the energy is reflected back towards the RFID reader. The whole process can be depicted in the following figure (*Figure 5.7*).

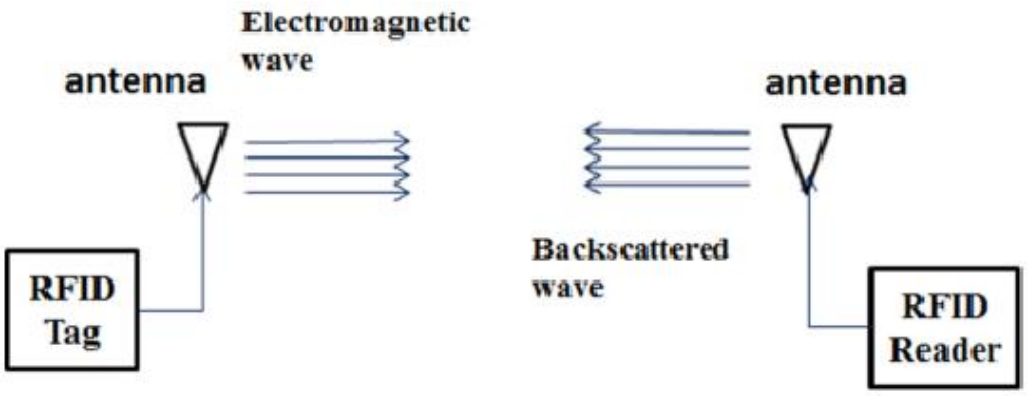

Figure 5.7: RFID system based on electromagnetic coupling (Zahran et al., 2016).

The previous sections presented and described RFID technologies in general. The following sections will narrow its focus to the implanted RFID technologies which is the primary focus of this thesis.

5.6 Human-implanted RFID

In recent times, RFID technologies have attracted significant interest in the aspects of body area application including both wearables as well as implantable applications. The RFID technology allows the user to use the implant as identification tag which can be used as access control to open doors, used as a car key or other authentication process (Biohackinfo, n.d.). This section will present a holistic and critical overview of design challenges associated with the human-implanted RFID technologies including operation frequencies, effects on the biological tissues, RFID antennas, etc. The aim of this section is to understand the critical challenges in developing the RFID implanted applications and future directions.

The technical requirements and standards for human-implanted RFID chips are different from other RFID applications in terms of sensing, computing and communication capabilities. Since the chip is implanted inside the body, the size has to be as small as possible and thus there are design constraints which need to be taken care off. Moreover, biocompatible material used for implant coating and packaging to avoid any tissue reaction inside the human body (Ahson & Ilyas, 2008).

The following subsection will discuss the different technological aspects of human-implanted RFID.

5.6.1 RFID implant technologies

In reference to *Chapter 5.2* on RFID technology and architecture, RFID technology is defined as a wireless application which employs backscattering communication (*Chapter 5.1.1*) to communicate and extract information from the remote or nearby object. From wearable to implants, RFID technologies offer several advantages. As also mentioned in *Chapter 4*, passive RFID devices are mainly attractive for body area applications particularly RFID implants and are completely batteryless and will be the focus area of this section. The basic components of RFID technology and architecture for the implanted device is similar to general RFID applications and has been previously presented in *Chapter 5.2*.

5.6.2 Design considerations for implanted RFID devices

Figure 5.1 shows how the RFID tag will operate inside the human body in case of an RFID implanted device. But, a number of considerations have to be taken into account for implanted RFID applications compared to other RFID applications. This includes the selection of the operating frequency, influence of the human body, antenna design and miniaturization since the chip has to be as small as possible to be inserted inside the human body and human safety concerns against the radiated electromagnetic field (Kiourti, 2018).

5.6.2.1 Operation frequency

There is a wide variety of frequency band that can be observed for the RFID application depending on their operation. The low operation frequencies that can be operated for RFID applications in the near field are in the range of 125-134 kHz and 13.56 MHz which uses the induction technique (*Chapter 5.5*) to transfer power from the reader to the tag. RFID devices that operated in the far field range are typical works at a frequency higher than 100 MHz and also the Ultra High-Frequency band of 840-960 MHz (Kiourti, 2018).

For the implanted RFID applications, low frequency or equivalent high wavelength is required for the high penetration power to the human tissues. But, they will be confined to the limited read range from the tag to the reader. In the contrary, the higher frequency will have greater difficulty in penetrating the biological tissues and thus not suitable RFID implanted application for the purpose of identification and authentication.

5.6.2.2 Influence of human body

As explained from the previous *Chapter 5.6.2.1*, the biological tissue exhibits a frequency dependent permittivity level. The dielectric loss, which is the dissipation of energy through the movement of charges in an alternating electromagnetic field (DoITPoMS, n.d.) in human tissue exceeds far than that of free space (Kiourti, 2018). So, for designing the antenna for human implantable purpose, it has to be taken into account of the human tissue in contrary to the designing in free space.

5.6.2.3 Antenna design and miniaturization

The antenna in the RFID implants plays an important role in maintaining the performance, especially its reading range. As already mentioned, it is also important to account the dispersal nature of the human tissue in which the tag or specifically the antenna is embedded. All these factors determine the antenna efficiency, radiation pattern and the input impedance (Sani et al., 2010).

For miniaturization, the size of the antenna is quite important which sometimes may result in a less efficient antenna. There are a number of techniques adopted worldwide to reduce the size of the antenna, like increasing the electrical length of the antenna by optimizing its shape or by applying resistive or reactive loading, etc. (Sathya, n.d.).

The following section will present the design of an implanted RFID tag by VeriChip Corporation.

5.6.3 VeriChip implanted RFID

The Verichip RFID tag also known as Verimed as previously presented in *Chapter 4.1.4* was the first FDA approved human-implanted RFID for the medical purpose as shown in the figure below (*Figure 5.8)*.

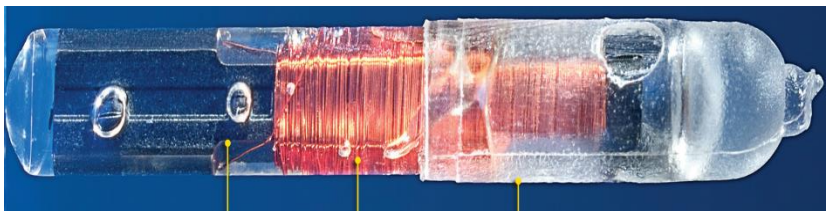

Figure 5.8: Verichip Implantable RFID Tag (Foster & Jaeger, 2007).

The detailed examination of the above-mentioned chip will be presented in the next section.

5.6.3.1 Design and components

The design of Verichip implanted chip is quite simple consisting of a coil of wire and an airtight sealed microchip within a glass capsule. The coil functions as an antenna and use the varying magnetic field of the RFID reader to power the microchip and transmit a radio signal (*Chapter 5.5*). The signal transmitted by Verichip is a unique identifying number which is linked to the medical record of the person having the implant. The chip resembles a grain of rice which is 11 mm long and 1 mm in diameter (Foster & Jaeger, 2007). The different components of the chip are presented in the next section.

- *Tissue Bonding Cap*: A cap which can be seen at the top of the chip in *Figure 5.8* is made from a special plastic cover which is an airtight glass capsule contain the RFID circuitry. It is designed in such a way that the capsule does not move around once it is implanted and has bound with the human tissue (Foster & Jaeger, 2007).
- *Antenna*: The coil which can be seen just below the tissue bonding cap in the middle part of the VeriChip in *Figure 5.8* which converts the readers varying magnetic field to power the RFID circuitry. The coil is coupled with a capacitor and together they form a circuit which resonates at the frequency of 134 kHz (Foster & Jaeger, 2007).
- *ID Chip*: The bottom part of the capsule in *Figure 5.8* contains the ID chip. The function of the ID chip is to modulate the amplitude of the current transmitting through the antenna to repeat a 128-bit signal. The change in amplitude from low to high or vice versa represent the bits (Foster & Jaeger, 2007).

5.4 Subconclusion

The aim of this chapter was to present a detailed analysis of the RFID technology and to understand the underlying technology for the development of the proposed prototype. The chapter has been mainly divided into three sections. The first section describes the overview and history of RFID technology which has been used from time to time in many applications. The second section presents the classifications of RFID technology and made a detailed analysis of passive RFID which is the boundary of this thesis. The knowledge of the RFID architecture along with different standards and protocol is quite significant to understand the adoption of this technology on a broader scale. The final section narrowed its focus on the human microchipping and pointed out different design constraints and classify different parts of the human implanted microchip.

The next chapter will analyse the legal environment associated with the human microchipping in the enterprises or workplace including the employees' rights and data privacy factors.

6 Legal Environment of Human Microchipping

In this chapter, the regulation and the legal environment associated with enabling the human microchipping in workplaces are presented and discussed particularly in focus with the EU regulation. In the initial research, it was found that the laws concerned with data protection and privacy are quite different in different parts of the world. So, EU regulation is narrowed down for this thesis because of the more protection of data privacy after the introduction of GDPR. In reference to *Chapter 4.3*, it is quite clear with the facts that, there is no clear legislation and legal framework with microchip implantation since the technology is yet to be conventionally adopted in a much wider scale. It is also feared that the implanted chip functions are much more than just opening the secured door, rather it gives the employer much greater power to control over their employees which is contrary to the human dignity (Firfiray, 2018). Though, business demands some way of monitoring to evaluate the performance of the employees but, in recent time the surveillance has gone beyond the expectations in terms surveillance of employees email account, wearable technology to monitor and track the movement of the workers. With the introduction of human microchipping, it will enable a new level of monitoring where the employees can not just remove or turn the microchip off. Even though the implants are technically voluntary, but, from the analysis from *Chapter 4.3*, it is quite clear about the discrimination or unfavorable consequences the employees might face if they do not agree for the implantation. Though a strong legal framework is absent at his moment related to human microchipping, the introduction of GDPR in EU countries will provide protection against the data privacy to the employees along with other existing treaties to protect the rights of the workers in workplaces. The following section will discuss different GDPR rule along with other EU treaty which is expected to conduct a privacy impact assessment.

6.1 Data Protection Regulation

The data protection law ensures that the employers in the organization opted for microchipping will voluntarily take consent to the collection, processing, and maintenance of both the personal and sensitive data required by the microchip to do the desired function (Graveling, Winski, & Dixon, 2018). As already mentioned in the previous chapter (*Chapter 4.3*), regarding the high demand for consent from the employees under the GDPR. It is also quite important to raise the concern regarding the application of the chip whose function can be quite critical to the data protection issues if in any way the chip can be used by the employer for recording purposes or transferring of personal data to the third parties. But, with the implementation of GDPR, the employer has to comply with each of the requirements that will be presented in

this chapter. By virtue of Article 16 of the Treaty of Functioning of the European Union (TFEU), EU has the complete power in the area of the Data Protection Regulation. Article 16 of the Treaty on the Functioning of the European Union states:

> "1. Everyone has the right to the protection of personal data concerning them.
>
> 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities." (European Union, 2016)

This regulation is a way of protecting the personal data concerning a citizen from Union institutions, bodies, offices and agencies by the action of the European Parliament and Council. All the European Union members fall under this regulation while carrying out activities including the free movement of such data. By virtue of Article 16 of TEFU, EU has the sole legislation in the data protection regulation.

Beside TEFU, EU's General Data Protection Regulation demands a strict consent from the workers by their employer in the form of an agreement which is a freely given, specific, informed and unambiguous manner indicates the processing of their personal data.

Article 7 of the GDPR states:

- "Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
- If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
- The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

- When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract." (GDPR, 2018)

It can be also noted from the interview with TUI (*Appendix B*), that the implantation of the microchip is voluntary but the application of this chip inside the workplace, for example, while accessing the locker, it raises a data protection issue if the employer of TUI is recorded in some manner. If this information in any way recorded by the employer, under the GDPR regulation, it must take the consent of the employees including any third party transfer of data along with other requirements mentioned under Article 7.

6.2 Human Rights Regulation

The concern of compromising the human right with the implementation of the human microchipping depends on how much the data gathering and processing interferes with the private life of the employee. There are a few issues associated with the violation of human rights in this particular case. Firstly, the implantation of a microchip and the subsequent collection of data would have to constitute the personal data of the employee and subsequently, it has to be analyzed or examined whether the processing and transferring of this data interfere with the personal life of the employees. Lower the level of interference, the more likely that the human microchipping will be lawful. But, still, the employer has to establish the need or the emergency for such implementation to legitimate the objectives of microchipping. Apart from that, discrimination may also occur among the people who give consent for the implant than the people who opted out of it as they considered relatively inferior (Gasson, Kosta, & Bowman, 2012).

Article 8 of the European Convention of Human Rights (ECHR) directs the Human rights of the workers in the workplace:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others." (Council of Europe, 2019)

The significance of Article 8(1) of ECHR in the event of human microchipping is important to solve issues in case of the collection of data which might constitute the collection of personal data even though the implant may be voluntary. Now, the collection of personal data may interfere with the private life of the employees. This regulation direct the employers to notify the employees of certain measures that will be required to monitor and these measures should be compatible with the requirements of article 8 of ECHR. It is also required for the employer to give a legitimate justification for the monitoring and accessing the data to the employees.

Article 8(2) prevents the public authority to interfere in the right stated in Article(1) and as seen from the previous discussion that the employer has to balance the proportion between the actual purpose of the implementation and the employees' private life. Since the use of human microchipping is voluntary so far, it dilutes the proportionality exercise in the question of the level of interference by human microchipping. In the future, when the human microchipping is more conventional, then if the employee experience less interference in their private life, there is more chance that human microchipping will remain lawful. But, it will always be a requirement for the employer to establish the legitimacy of the microchipping in their organizations which may be sighting the reason of freeing employees from the hassle or the security concerns with the access card, password, pin, and fear of losing the important credentials.

6.3 Regulation on Data Ownership

From the analysis in *Chapter 4.3*, it is found to be a concern in situations when a particular employee leaves the organizations who seem to have voluntary agreed for microchipping in his/her employment period. So, the basic areas of concern are the ownership of the chip and the data collected and stored on the chip. If the basic regulation regarding the same is stated in the employment contract, then the employer can produce it and claim their ownership. But, in contrary, if there is no previous agreement between the employer and employee, then the default regulation can be derived from some of the regulation put up by General Data Protection Regulation and will be discussed in the following section.

Article 13 of the GDPR states that:

> “Information to be provided where personal data are collected from the data subject.” (GDPR, 2018)

Furthermore, Article 13(2) in particular states:

> “The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability.” (GDPR, 2018)

The above mentioned GDPR regulation clear states the employee's ‘Right to be forgotten’ as well as the employer’s responsibility to furnish every possible information to its employees.

Article 15 of the GDPR laid down the right of access by the data subject which implies that the data collected and stored on the microchip has the right to be accessed by the employees. (GDPR, 2018)

Article 17(1) of the GDPR directs that employees have the right to erase the personal data concerning them (GDPR, 2018) and Article 17(2) includes the ‘Right to be forgotten’ (GDPR, 2018) which states:

> “Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.” (GDPR, 2018)

However, Article 17(3) curtail the rights granted under Article 17(1) and Article 17(2) if it interferes or collides with certain public interests (GDPR, 2018).

6.4 Religious Discrimination Law

Religious discrimination is treating a person unfavorably on the basis of his/her religious beliefs (Equal Employment Opportunity Commission, n.d.). This is quite a concern in the workplaces and there are certain laws protecting against these practices.

EU under Article 19 of the Treaty of Functioning of the European Union states:

> “1. Without prejudice to the other provisions of the Treaties and within the limits of the powers conferred by them upon the Union, the Council, acting unanimously in accordance with a special legislative procedure and after obtaining the consent of the European Parliament, may take appropriate action to combat discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation.
>
> 2. By way of derogation from paragraph 1, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, may adopt

> the basic principles of Union incentive measures, excluding any harmonisation of the laws and regulations of the Member States, to support action taken by the Member States in order to contribute to the achievement of the objectives referred to in paragraph 1." (European Union, 2008)

It provides a framework which protects the employees or workers against any discrimination based on religious belief. As already discussed in *Chapter 4.3*, in some religions it is considered as a sin to implant foreign objects in the body. So, a compulsion to implant on the working place thus constitute a breach in the religious belief of a particular employee. On the part of the employee to establish this particular breach of the law, it must prove that the implant of microchipping to the particular section of the employee whose religious belief is not contradicting in this particular case has more advantages in the workplace than those whose religious belief breaches with human microchipping.

6.5 Subconclusion

This chapter presented and analyzed the legal and regulatory environment from the perspective of human microchipping in the workplaces. It is quite clear that, since human microchipping is not yet a conventional and adopted technology at this moment, so there is an absence of a regulatory framework for protecting the rights of the employees. But, with the introduction of GDPR, several regulations and rights protecting the employees under EU law can be inferred from the same. It can also be drawn as a conclusion to this chapter that, several laws at a time contradict each other, for example, when it comes to protecting the data in view of public interests. This means the law will not be applicable in certain context if the data is in favor of protecting the public interest.

In the following chapter, the rate of adoption of human microchipping will be explored and analyzed by using Rogers' DOI theory as a lens and applying a survey approach. In addition, microchipped individuals from different businesses will be interviewed.

7 Data Collection and Analysis

Having explored the state-of-the-art technologies associated with RFID, along with potential issues regarding the legal environment, this chapter aims at shedding light on the rate of adoption of human microchip implant technology. To accomplish this, a survey was conducted in which Rogers' Diffusion of Innovations (DOI) theory was used as a lens to learn about perceived attributes of the innovation by potential adopters. In addition to this, early adopters of the technology were interviewed. Specifically, employees of a travel and tourism company were interviewed to learn about the reasons behind adoption along with potential encountered issues. Another early adopter, an owner of two microchipping retailing and manufacturing business, was also interviewed, in order to learn more about his perspective on the technology from a service provider's point of view.

7.1 Survey

As mentioned above, the first part was using Rogers' Diffusion of Innovations theory in order to explore the rate of adoption of the innovation and thus gain insights into potential factors impeding or facilitating the speed. Specifically, the theory will provide the foundation for exploring the acceptance of the solution by conducting a survey to obtain quantitative data on the perceived attributes of the solution as seen from the perspective of potential adopters. In the following subchapters, the chosen approach for the study will be detailed, along with a presentation of the questionnaire, data collection, and finally, the rate of adoption will be analyzed based on the survey results.

7.1.1 Study design and approach

For the design of the study, meta-analyses identifying ideal innovation study characteristics were used as a guideline (Kapoor, Dwivedi & Williams, 2014; Tornatzky & Klein, 1982). This was done in order to increase the validity of the study.

Let us first consider the approach. According to Tornatzky and Klein (1982), the ideal study should be predictive as opposed to retrospective. They argue that because the perceived attributes of an innovation may be affected by the perceiver's knowledge of the decision of rejection or adoption. Even though the majority of studies have been conducted in a retrospective fashion according to Kapoor, Dwivedi, and Williams (2014), the study in this project will adopt a more predictive approach. This will eliminate the issue raised by Tornatzky and Klein (1982) in their meta-analysis article. Furthermore, it will suit the implantable

microchip technology as it is arguably still in its early diffusion stages looking at the number of adopters being a maximum of 10,000 (Graveling, Winski & Dixon, 2018) on a global scale.

In terms of the type of study, a quantitative survey research design was chosen using questionnaires as the data collection instrument. As argued by Tornatzky and Klein (1982), they suggest using a quantitative research design approach as this type of data contributes more significantly as opposed to theoretical studies and qualitative data. Furthermore, it enables the use of replicable measures of innovation attributes instead of inferring the level of a certain attribute using qualitative data as argued by Tornatzky and Klein (1982).

Specifically, survey research will be conducted online. The online approach has several benefits. As argued by Wright (2006), online surveys can provide access to groups and individuals who would otherwise be difficult to reach. In addition, he argues that it can save researchers time as it can reach many people in a short amount of time. Also, it allows researchers to potentially work on other tasks while collecting the data. Lastly, he argues that there can be vast savings in terms of monetary cost by using this approach. For these reasons, in addition to the scope of this project being limited by time and resources, an online survey is suitable.

However, online survey research also has its limitations. For example, as mentioned by Wright (2006), information about the characteristics of people may be limited to the basic demographic variables included in the survey. Also, there is no guarantee that the participants provide accurate information in the survey. Some people may just look to finish the questionnaire as soon as possible, and get on with their day. To combat this aspect, the questionnaire will include an introductory paragraph asking people to answer as truthfully as possible. Furthermore, there will be an estimation of the time needed to answer the survey. Lastly, the questionnaire will be made as simple as possible to encourage people to answer truthfully and put in the necessary time. The simplicity of questions was also maintained to make it as easy as possible for people to understand the questions and thus help prevent misunderstandings, as they will be left to themselves when filling out the questionnaire.

Another point being mentioned by Wright (2006) is the fact that it can be hard to obtain email lists as organizations will likely be reluctant to provide this information to researchers. This means that the channels to which the questionnaires are distributed can be limited significantly. For this reason, the sample of respondents may be limited to the workplace and social media channels of the researchers, which will result in a less diverse sample of respondents.

Let us now look at the ideal number of perceived attributes to consider. According to Tornatzky and Klein (1982), the ideal study should consider more than one perceived attributes of innovations. For this project, all of the five attributes mentioned by Rogers (2003) of relative advantage, compatibility, complexity, trialability, and observability will be considered.

The adopting unit for this study will be recognized as organizations as the target group for the proposed solution is aimed at business organizations. Organizations as the unit of adoption also form the largest chunk of studies as opposed to individuals according to Kapoo, Dwivedi, and Williams (2014).

The number of innovations studied will be limited to one, even though Tornatzky and Klein (1982) recommend using more than one. They argue that single innovation studies may not be sufficiently robust to allow for generalization to a population. Furthermore, Tornatzky and Klein (1982) also make an argument for using more than 'adoption' as the dependent variable. However, considering the scope, timespan, and resources of this project, one innovation was chosen along with adoption as the only dependent variable.

7.1.2 Questionnaire design

The questionnaire was divided into two parts. The first part was concerned with statements related to the five perceived attributes of innovations as presented by Rogers'. Here, the idea was to get an overview of how potential adopters perceive different attributes of microchip implant technology for use in the workplace. Specifically, the areas of relative advantage, compatibility, complexity, trialability, and observability were considered in order to analyze the rate of the adoption. Before the statements, an introduction was included in which the overall purpose of the questionnaire was explained as well as a simple definition of human microchip implants. This text can be found in *Appendix D*. The second part was concerned with demographic details such as age, gender, education, occupation as well as the type and size of business.

In order to measure the individual perceptions of the attributes and make them quantifiable, a Likert-scale was chosen. Likert-scales are commonly used to measure the attitude of people by providing a range of responses to each statement or question (Jamieson, 2004). The main benefits of using a Likert-scale include that they are easy to construct and easy to read and complete for respondents (Bertram, 2007). Usually, there are 5 categories of responses. For example, 1 = 'strongly disagree' to 5 = 'strongly agree'. The questionnaire in this project uses a 7-point scale, using end-labels of 1 = 'strongly disagree' to 7 = 'strongly agree'. A 7-point scale was chosen to add additional granularity to the measurement as opposed to a 5-point scale (Bertram, 2007).

It is worth noting that Likert-scales may be subject to several response biases. One example is acquiescence bias, where the respondents tend to agree with the statements which are presented in the absence of a balanced scale, such as a Likert-scale (Watson, 1992). For example, respondents may be inclined to answer in a positive way if they have an inherit eagerness to please people. Another response bias worth mentioning is that of social desirability. Social desirability bias is when the respondent distorts their answers to appear more favorably to others and presenting oneself in a positive light (Furnham, 1986). An example of this could be answering in a negative fashion if that aligns with the mentality of friends, family or one's workplace. Other biases include central tendency bias, where participants may avoid selecting extreme response categories (Bertram, 2007).

As mentioned, the aim of the questionnaire was to explore the rate of adoption using Diffusion of Innovations theory. This piece of information was not mentioned in the questionnaire in order to make it as simple as possible for the respondents and to ensure that the information did not affect their answers in any way.

An English and a Danish version of the questionnaire was created. This was done in order to make it more accessible to people who are not comfortable with English or simply prefer Danish when given the choice. However, this may have made the questions slightly different from one version to another, which may affect the results slightly. The intended population for the survey was any potential adopters of the technology, as the amount of implanted individuals is still very small at the global scale.

7.1.2.1 Statements related to Diffusion of Innovations theory

The first section of the questionnaire aims to identify and quantify the perceived attributes of human microchip implant technology for use in the workplace. The five perceived attributes of relative advantage, compatibility, complexity, trialability, and observability are, according to Rogers (2003), some of the most important indicators when explaining the rate of adoption. To create the statements, work by (Atkinson, 2007; Baghi, 2015; Ali, 2017) were used as an initial starting point.

The first part explores the perceived relative advantage of human microchip implants. The more advantageous an innovation is perceived to be relative to the technology or idea it supersedes, the faster the rate of adoption will be. The statements here revolve around measuring how human microchip implants are perceived to be more convenient, prestigious, faster and secure relative to usual methods for accessing the workplace, payment, printing, etc. The statements are listed in the table (*Table 7.1*) below.

Part 1: Relative advantage
1.1 Using a human microchip implant to access the workplace, print, pay, etc. would be more convenient than using usual methods
1.2 Using a human microchip implant for accessing the workplace, printing, payment, etc. instead of usual methods would be seen as something prestigious by others
1.3 Using a human microchip implant for accessing the workplace, printing, payment, etc. would be more secure than using usual methods
1.4 Using a human microchip implant would allow me to more quickly gain access to the workplace, print, pay, etc. compared to using usual methods

Table 7.1: Statements related to relative advantage (own table).

The second part explores the degree to which human microchip implants are perceived as being consistent with existing values and needs of the potential adopters. If an innovation is not considered compatible with the existing values and needs of a social system, the rate of adoption will be slowed down. As seen in the table below (*Table 7.2*), to identify the compatibility, statements were asked regarding how the use of human microchip implants would fit into the way they would like to access the workplace, print, etc as well as how the technology would fit into their lifestyle.

Part 2: Compatibility
2.1 Using a human microchip implant would fit right into the way I would like to access the workplace, print, pay, etc.
2.2 Using a human microchip implant would fit right into my lifestyle

Table 7.2: Statements related to compatibility (own table).

Part three identifies the perceived complexity of the innovation. The more difficult an innovation is to use and understand, the slower the rate of adoption will be. Here, the statements explore the perception of the simplicity of human microchip implant technology by potential adopters. The question can be seen in *Table 7.3* below. For the sake of keeping the questionnaire simple, the question is formulated in a way in which it measures the degree of perceived simplicity as opposed to complexity. This also makes it so that a high score on this statement has a positive relationship with the rate of adoption instead of a negative one, which would be unlike the relationship of the other perceived attributes.

Part 3: Complexity
3.1 I think a human microchip implant would be simple and easy to use for accessing the workplace, printing, paying, etc.

Table 7.3: Statement related to complexity (own table).

Perceived trialability is measured in the fourth part. Trialability is the degree to which an innovation may be experimented with on a limited basis. In general, there is a positive relationship with the degree of trialability of an innovation and its rate of adoption. As such, the statement, as shown in the table below (*Table 7.4*), is formulated in a way in which it explores the degree to which a potential adopter would be willing to try out a human microchip implant on a limited basis in order to get familiarized with its features, before ultimately deciding to adopt the technology or not.

Part 4: Trialability
4.1 I would be willing to try out a human microchip implant on a limited basis to get to know its functionalities before deciding to adopt the technology or not

Table 7.4: Statement related to trialability (own table).

Finally, the fifth part explores the perceived observability of human microchip implants by potential adopters. The easier it is for other individuals to observe the results of an innovation, the greater the likelihood of adoption. As seen in the table below (*Table 7.5)*, the statements revolved around how easy it would be to explain the results of using a human microchip implant to others as well as how easy it would be for others to observe the benefits of using said technology.

Part 5: Observability
5.1 It would be easy to explain the benefits of using a human microchip implant in the workplace to others
5.2 It would be easy for others to observe the benefits of using a human microchip implant in the workplace

Table 7.5: Statements related to observability (own table).

7.1.2.2 Questions related to demographic information

As demonstrated by Czaja et al. (2006), there are several important demographic characteristics which may influence the successful adoption of technology. Therefore, the second and final part of the questionnaire revolves around the demographic information of the respondents. Furthermore, by including demographic information, it is possible to say something about the characteristics of the sample of participants, and thus, determine whether the sample size can represent the desired target group.

The first question asks how old the respondent is. As put by Czaja et al. (2006), data indicate that older adults, in this case in the United States, have more difficulty in learning to use and operate current technologies compared to younger people. As such, it is worth looking into the

ages of the participants since there may be an abundance of one age-group which can affect the results.

In the second question, the respondent is asked of its gender. This question was introduced in order to explore whether there are any gender biases towards the innovation. According to Kotze, Anderson, and Summerfield (2016), women tend to be less optimistic than men about high-technology consumer products. The question also helps identify whether the sample size has an even distribution of genders.

As data suggests that education and socioeconomic status also influences technology adoption (Czaja et al., 2006), questions three and four asks for the highest level of education completed as well as employment status.

Finally, questions five and six address the type of industry, type of company and size thereof, given the respondent is employed. By asking these questions, one may identify whether certain types of industries and companies are more open to this type of innovation, as well as how big the respective companies are.

7.1.3 Distribution and data collection

As mentioned previously, the questionnaires were distributed online using Google Forms. The channels of distribution included social networks of Facebook and LinkedIn. Additionally, the questionnaire was also posted to the internal enterprise social network of an IT project and procurement organization.

Once the questionnaires had been distributed, an error was identified and quickly fixed. Specifically, the option of selecting ‘Unemployed’ in the Danish version was accidentally omitted. However, this should not have affected the results significantly, if at all.

From the start, the aim was to obtain as many responses as possible. The questionnaire was conducted over a span of 7 days. Once the number of responses stopped increasing day by day, the survey was closed. In total, 88 responses were collected. Out of these, based on the demographic information, it is estimated that the majority of the responses consisted of employees from the above-mentioned IT project and procurement organization. As such, even though the sample size is relatively small, it can arguably still provide and capture the general attitude towards this technology based on business organizations within Denmark, such as an arbitrary IT project and procurement business.

Let us now consider the demographic information of the sample size collected. As shown in *Figure 7.1* below, there was a reasonable distribution of participants between ages 20-69.

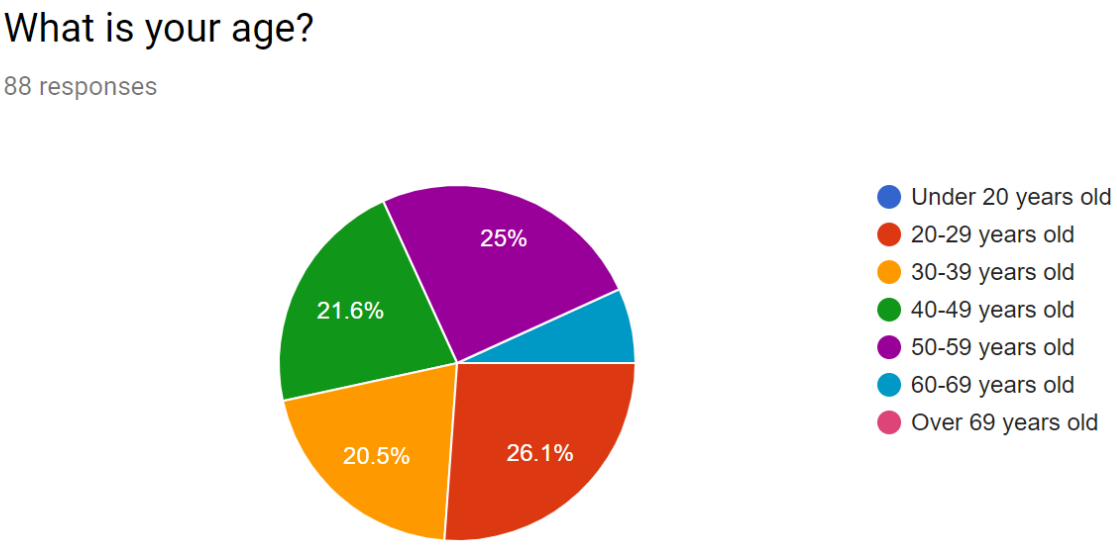

Figure 7.1: Distribution of age among participants (own figure).

Furthermore, looking at the distribution between the genders in *Figure 7.2* , a reasonable split can also be identified. However, there is a slight overrepresentation of males at 54.5%.

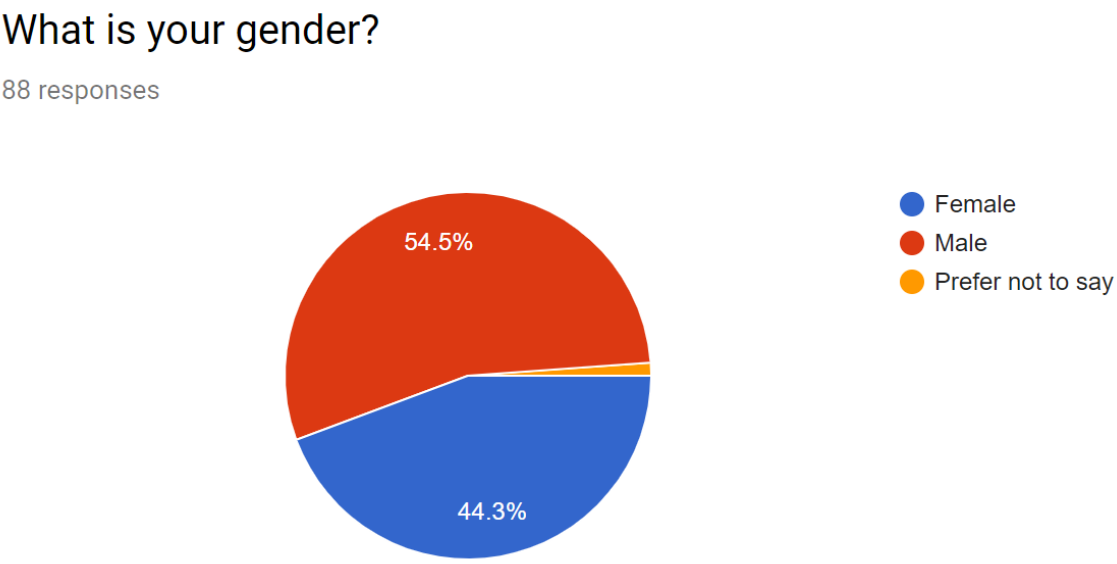

Figure 7.2: Distribution of gender among participants (own figure).

Let us now consider the education level of the participants. As seen in *Figure 7.3* below, 42% of respondents have completed a Master's degree (42%), followed by a segment of 30.7% who have completed a Bachelor's degree. As such, there is an overrepresentation of respondents with a high-level academic background. This is to be expected when the majority of the sample size consists of employees from the same organization.

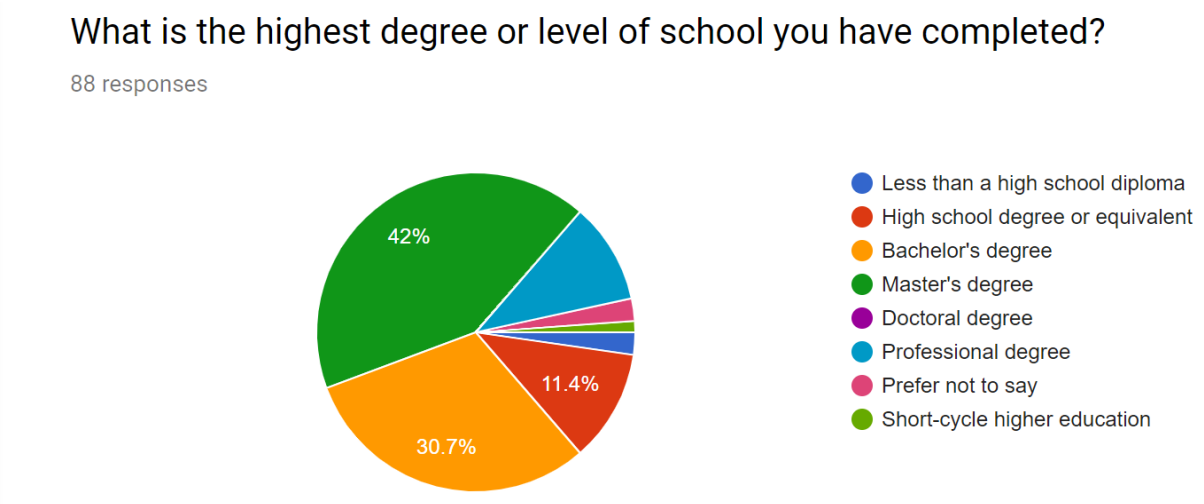

Figure 7.3: Distribution of education among participants (own figure).

In terms of employment status, the majority of participants are employed full-time (68.2%) as shown in *Figure 7.4* below. This is also to be expected when having such a large portion of the sample size being from the same organization.

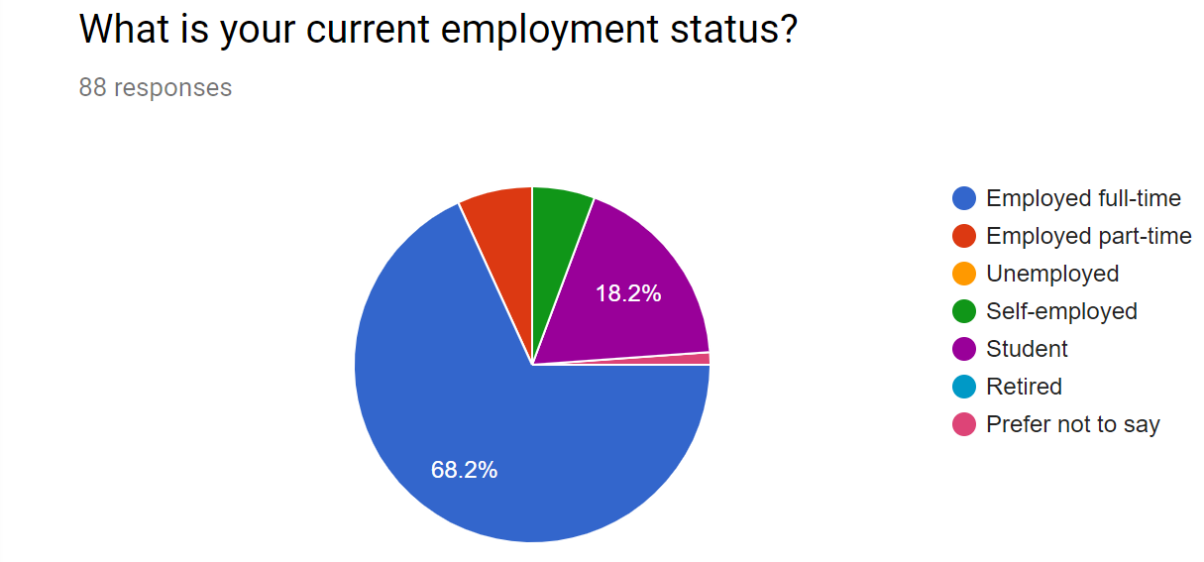

Figure 7.4: Distribution of employment status among participants (own figure).

When participants were asked in which type of industry and type of company they worked in, the following 64 responses were collected as shown in the *Table 7.6* below. As expected, once again, there is an overrepresentation of items connected to the IT project and procurement organization. These were all huddled together into an IT sector group for further cross-sectional analysis. Other interesting items such as medical technology, telecom, healthcare, and contractors were also present albeit in fewer numbers.

• IT • IT company • Public sector • IT Procurement • NGO • FMCG - Lantmannen Unibake • Telecom • Hearing Instruments • Consulting • It • Medical technology • Software development • Information Security • Contractor • IT services • Digitization • Security and privacy	• IT development • Public IT organization • Healthcare sector • IT sector • Civil engineer • Government/State • Education sector • IT consultant • Process excellence in Copenhagen • Retail industry • Accounting • Coaching and equivalent • Jeweler • Consultant • Economics, consultancy house • IT sector, procurement • IT-project house

Table 7.6: Type of industry and type of company among participants (own table).

Lastly, let us consider the estimated size of the company the participants work in. As seen in the *Figure 7.5* below, 62.8% of the respondents belong to the 50-250 employees group, followed by 15.4% of respondents in the group for more than 250 employees in the company. Once again, this is to be expected considering the proportion of participants belonging to the same company.

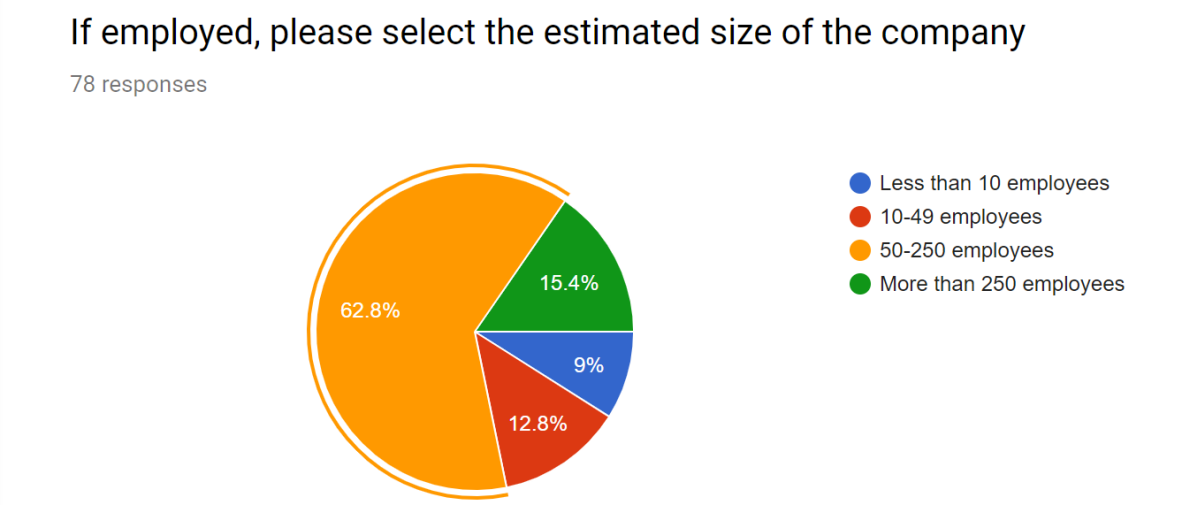

Figure 7.5: Distribution of estimated size of company of participants (own figure).

To summarize, there is a large proportion of the sample size which shares many traits such as education, employment status, industry type, company size, however, with varying ages and gender. This is due to these participants being from the same organization.

Over the course of the survey period, several participants from the IT project and procurement organization were requesting more questions in the questionnaire and provided feedback. Specifically, questions and statements related to whether they wanted to have a human microchip implanted or not in the first place, privacy concerns, piercing concerns, not being able to leave the implant behind once leaving the workplace, potential side-effects, surveillance, changing the workplace, and ethics. In general, some people missed more about the potential barriers of the technology. Other people were also positive and eager to try out the implants if given the chance. Since the participants were unaware of the use of Rogers' DOI theory as a lens for the survey, as it was deliberately not mentioned anywhere, it is understandable that they were missing many aspects. For future research, it may be worth considering to incorporate some of the above aspects.

7.1.4 Analysis of perceived attributes of human microchip implants

Before diving into the data analysis through the lens of Rogers' DOI theory, let us consider how to present Likert-scale data in an optimal way. As Jamieson (2004) points out, Likert scales fall into the category of ordinal data. This is due to the response categories having a rank order with intervals between the values which cannot be presumed equal. Jamieson (2004) also points out that many researchers consider the intervals between values equal, so considering the scale as an interval scale, which may lead to researchers coming to the wrong conclusions. Overall, the debate between ordinal versus interval scales in the context of the Likert scale is highly controversial. In the case of this project, an argument can be made for both ordinal data and interval data, as there were only end-point categories described on the Likert-scale, which makes the numbers between 1-7 on the scale uncategorized. However, to err on the side of caution, the data will be considered ordinal in this context.

As argued by Jamieson (2004), when dealing with ordinal data, determining the mean and standard deviation are inappropriate, and instead, one should find the median or mode to determine the central tendency. In the context of this project, the median will be calculated to determine the central tendency of each statement.

In addition to determining the central tendency of the data for each statement, diverging bar charts will be used to visually represent the data using Excel. Diverging bar charts are useful when presenting Likert-scale data, as they can present the information in such a way that it is

easy to compare the ratings given by different demographic groups, as shown by Heiberger and Robbins (2014) with several examples.

For the diverging stacked bar charts, demographic groups consisting of less than 10 individuals were omitted, in order to limit the number of groups displayed and to avoid displaying groups consisting of very few respondents. For the type of business sector, only the respondents from the IT sector were considered and grouped together, as the other groups were too small. Furthermore, 'Strongly disagree' is represented by a dark red color, and 'Strongly agree' is represented by a dark green color. The nuances in between correspond to the numbers in between 1-7. A neutral score of 4 is represented by gray colors. All portions of the bars leaning towards disagreement are denoted with negative percentages. Lastly, all of the diverging stacked bar charts can be found in *Appendix A*, comprising of all of the different demographic groups. This means that the below figures are only a part of the full charts.

7.1.4.1 Relative advantage

Starting off, let us consider the perceived relative advantage, which is an important determinant for an innovation's rate of adoption. The statements connected to this aspect look at potential advantages such as convenience, speed, prestigiousness, and security.

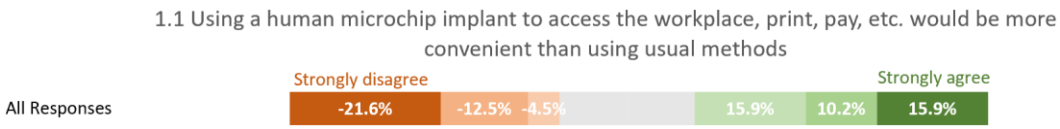

Figure 7.6: Part of diverging stacked bar chart showing all responses for statement 1.1 (own figure).

As seen in *Figure 7.6* above, the majority of respondents strongly disagreed with the statement. Aside from that, the answers are somewhat evenly distributed all over the scale. However, there is a slight trend towards agreeing with the statement. Looking at central tendency, the median is 4, which is to be expected when looking at the distribution among respondents. Comparing this to the responses split by different age groups, it shows that the 20-29-year-old group is the ones agreeing the most with the statement, whereas the other groups are more divided. However, one interesting thing to note is that the 30-39-year-old age group seem to be the ones disagreeing the most. Looking at males versus females, it shows that the male group is much more in agreement with the statement compared to the female group. In terms of education, the group with the highest education seem to be more in disagreement than the group with a slightly lower level of education. Finally, looking at students versus full-time employed, the student group seem to be more in agreement.

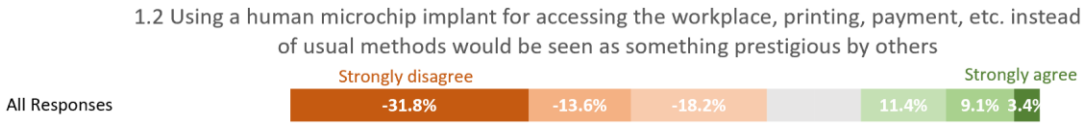

Figure 7.7: Part of diverging stacked bar chart showing all responses for statement 1.2 (own figure).

Let us now consider statement 1.2. As seen above (*Figure 7.7)*, regarding the perceived prestigiousness, the distribution is strongly skewed towards disagreeing with the statement. Looking at central tendency or the center of the distribution, the median is 3, meaning that the tendency is towards disagreement. Scrutinizing specific demographic groups, some of the same trends are evident as were presented in connection with statement 1.1. Specifically, the 20-29-year-old age group was the most in agreement similar to the previous statement. Also, the 30-39-year-old group is once more the ones mostly in disagreement. Furthermore, males were more in agreement compared to females, also similar to the previous statement.

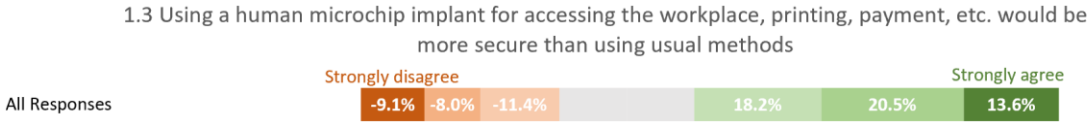

Figure 7.8: Part of diverging stacked bar chart showing all responses for statement 1.3 (own figure).

Regarding perceived security in relation to relative advantage, there is a heavy overweight of respondents agreeing with the statement, as shown in the above figure (*Figure 7.8)*. Here, the median is 5, as such, the central tendency of the distribution is leaning towards an agreement. In relation to individual demographic groups, interestingly, the 50-59-year-old age group are the ones mostly agreeing with the statement of it being more secure.

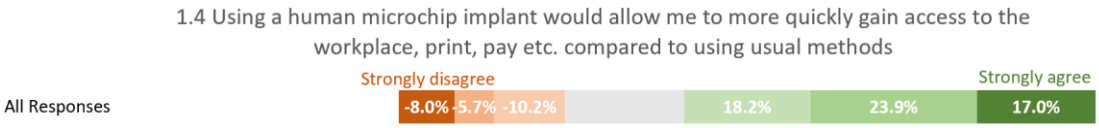

Figure 7.9: Part of diverging stacked bar chart showing all responses for statement 1.4 (own figure).

For the final statement associated with perceived relative advantage, considering the aspect of it being quicker, there is also an overweight of respondents leaning towards agreeing with the statement. The responses can be seen in the above (*Figure 7.9)* diverging stacked bar chart. Looking at the central tendency, a median of 5 can be determined, similarly to the previous statement. As such, there is a tendency towards agreement on this aspect. For this statement, the 50-59-year-old age group is the one agreeing the most, similarly to the previous one. Furthermore, the males are once again more in agreement.

To summarize the above results, generally, the respondents were able to see and agree with the perceived relative advantages of using human microchip implants. The majority did,

however, not see it as something prestigious. The aspects of security and quickness were all perceived as advantageous by the majority, while the view on convenience was more neutral, yet with a slight tendency towards an agreement. As put by Rogers (2003), the perceived relative advantage is one of the more important attributes when looking at adoption, as the degree to which an innovation is perceived as advantageous will largely determine its rate of adoption.

7.1.4.2 Compatibility

Another important attribute as mentioned by Rogers (2003) is that of compatibility. In other words, the perceived degree of consistency of the innovation with the values and norms of a social system. The greater the incompatibility, the slower the rate of adoption will be. The statements associated with this attribute were related to how using the innovation would fit into their lifestyle and how they would want to access the office etc. Let us first consider statement 2.1.

Figure 7.10: Part of diverging stacked bar chart showing all responses for statement 2.1 (own figure).

As shown in the figure above (*Figure 7.10)*, the majority of respondents did not agree with the statement regarding the microchip fitting into the way they would like to access the workplace, etc. Considering the median, a score of 2 can be determined, which corresponds with the strong tendency towards disagreement. Let us now consider different demographic groups. Once again, the age group of 20-29-year-olds, as well as males, are ones agreeing the most. That being said, the majority of these groups still lean towards disagreement.

Figure 7.11: Part of diverging stacked bar chart showing all responses for statement 2.2 (own figure).

Looking at statement 2.2, in the above figure (*Figure 7.11)*, regarding how it would fit into the lifestyle of respondents, a strong skew towards disagreement is also noticeable. For this statement, the median is also 2, similarly to the previous statement. Looking at demographics, once more the age group of 20-29-year-olds and males are more inclined to agree. However, they still have a majority of respondents of those groups disagreeing.

In summary, respondents did not seem to perceive the innovation as being compatible with their existing social norms and values. As a result, this may slow down the rate of adoption of human microchip implants drastically. In particular, as mentioned in *Chapter 4.2*, religious beliefs could play a role here, as certain religious groups may see this implantable technology as something resembling things in a religious context. This was also mentioned during an interview with three implanted employees from the travel company TUI, where many religious people had contacted one of the implanted employees regarding these issues.

7.1.4.3 Complexity

Another important perceived attribute to consider is that of complexity. However, it is not as important as relative advantage and compatibility as a factor when looking at the rate of adoption according to Rogers (2003). Complexity is the degree to which the innovation is perceived as easy to use and easy to understand.

Figure 7.12: Part of diverging stacked bar chart showing all responses for statement 3.1 (own figure).

As seen in the above figure (*Figure 7.12*), the majority of respondents agreed with the statement of perceived simplicity and ease of use. Here, the median is at 6, showing a central tendency towards an agreement. In regards to individual demographic groups, once again 20-29 year olds and males are generally more in agreement compared to their counterparts.

All in all, the perceived complexity of the innovation is quite small. Even though this particular attribute is not as important as the former two presented, it is still an important factor. According to the data, it appears that this attribute will not have much of a negative impact on the rate of adoption.

7.1.4.4 Trialability

The fourth perceived attribute is that of trialability. Trialability is the degree to which an innovation may be experimented with and tried out on a limited basis. This is quite an interesting attribute to survey, as this will arguably say something about the willingness of potential adopters to try out the innovation on a limited basis prior to deciding on adopting the technology or not. Let us look at the spread of the data.

Figure 7.13: Part of diverging stacked bar chart showing all responses for statement 4.1 (own figure).

As seen in *Figure 7.13 above*, the majority of respondents were in disagreement, with the majority being in strong disagreement. This is also evident by having a median of 2. Another interesting thing to consider is the fact that only a tiny portion selected the neutral score for this statement, which could mean that respondents had a strong opinion on this matter. Let us now consider demographics. For this statement, once again the younger generation, as well as males, were more in agreement compared to their counterparts. However, the majority were still in disagreement. Another interesting thing to note is that the female group was the group disagreeing with this statement the most.

In summary, the perceived trialability of the human microchip implants may reduce the rate of adoption according to the data from this survey. It is understandable that respondents answered in a negative fashion, as many people will arguably find it quite invasive to have something implanted underneath their skin, even if it is only as a part of a limited trial. However, it appears that there are still a substantial amount of people out there who are willing to try out the technology as a part of a trial, according to the survey. As such, it is not entirely skewed towards one side.

7.1.4.5 Observability

The final perceived attribute to be considered is the observability. The attribute is concerned with the degree to which the results of using a particular innovation is perceived as something that is visible to others. In addition to the four other attributes, this one is also affecting the rate of adoption of an innovation. In the survey, the statements were focused around being able to explain the benefits to others and the visibility of the results to others.

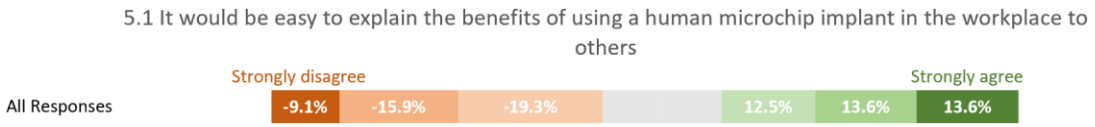

Figure 7.14: Part of diverging stacked bar chart showing all responses for statement 5.1 (own figure).

Looking at the above figure (*Figure 7.14)*, which shows the responses for statement 5.1, the results show that there is a slight overweight of respondents disagreeing with the statement. However, the scores are spread out relatively evenly and the median is 4. As was seen with the other attributes, there is once again a trend of 20-29-year-olds and males being more in agreement with the statement.

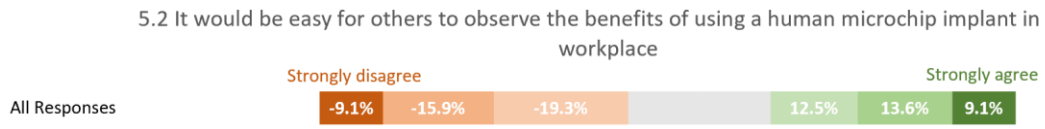

Figure 7.15: Part of diverging stacked bar chart showing all responses for statement 5.2 (own figure).

Considering the second statement associated with the observability, shown in the above figure (*Figure 7.15)*, there is a slight tendency towards disagreement. The data from this statement also has a median of 4. Looking at the demographics, the same trends are evident of males and 20-29-year-olds being more inclined to agree and females being more inclined to disagree.

The aspect of observability is quite peculiar in relation to the human microchip implants. The technology itself will be hidden underneath the skin, which could potentially make it less observable by others. On the other hand, which was also brought up during the interview with TUI, it may also make observers become curious and think about what they just witnessed, e.g. someone accessing an office using their hand.

So, in summary, the survey shows that in terms of perceived observability, the respondents are slightly in disagreement. Therefore, the rate of adoption may be slower as a consequence. However, the extent to which the respondents disagreed may also prove to be insignificant in the long run, as several also agreed with the statement.

7.1.4.6 Rate of adoption

Based on the data acquired from the survey, one may get an idea of how potential adopters perceive different attributes of human microchip implants for use in the workplace, and as a result, see in which areas potential barriers impeding the rate of adoption are. In terms of the relative advantage, the respondents seemed to have a quite positive perception, apart from seeing it as something prestigious. So, the advantages of switching to such a technology are evident to a lot of people, and will as a result, likely speed up the rate of adoption.

The second perceived attribute of compatibility, however, may be turn out to be a big barrier for a lot of people. As was presented previously, the majority of respondents responded in a negative manner to the statements associated with compatibility. As such, it appears that a lot of people do not find the technology as something that would fit into their lifestyle nor their social norms and values. However, this aspect may vary a lot from country to country or community to community. But, based on this survey, it seems that people in Denmark do not perceive it as compatible at this stage, meaning that the rate of adoption will likely be slower as a result. The incompatibility could be due to many reasons, one of them being religion, as mentioned previously. As for the perceived complexity, it appears that the respondents see the technology as something that is easy to use and understand, and as a result, could speed up the rate of adoption.

Considering the perceived trialability, many respondents seemed to have a very negative attitude towards this. However, there were also a substantial amount of people open to the idea. As mentioned, this could likely be due to people viewing the implantation process as something too extreme or invasive, even if it was merely for trial purposes. So, arguably, this could also play a significant role in the rate of adoption, as a lower degree of perceived trialability could mean that fewer people are willing to try out the technology and thus potentially be persuaded to adopt.

As for the attribute of observability, this was also an interesting aspect. Respondents seemed to be quite spread out in their opinion on this. As was mentioned, the microchip technology itself will not be visible to others once it has been implanted, which could impede the rate of adoption. However, an argument can also be made that the benefits it provides could be visible to others and act as a way to persuade people and inform people about the solution, as was pointed out during the interview with TUI, which could positively affect the rate of adoption.

Another trend which revealed itself was that the younger generation, specifically the 20-29-year-old group, was always more inclined to agree to the statements. As such, this seems to correlate with the study presented by Czaja et al. (2006), where data indicated that older adults had more difficulty in operating and using current technologies in comparison to younger people. It was also evident from the survey that the male group was more inclined to agree compared to their counterpart of females. This ties in with Kotze, Anderson, and Summerfield (2016), who argued that females tend to be less optimistic when it comes to high-technology consumer products, compared to males. So, the data indicates that the rate of adoption of human microchip implant technology will be more rapid among the younger generation and among men.

Having established the perception of these five different attributes, one may argue that compatibility will be one of the biggest barriers for hastening the rate of adoption. Certain social systems simply may not be compatible with new innovations. As Rogers (2003) argues, the social system can either facilitate or impede the diffusion of innovations depending on their values and needs.

There may be other barriers or uncertainties impeding the rate of adoption which were not included in the survey. For example, as mentioned, several people provided feedback to the questionnaire stating that they would have liked to voice their concerns about privacy, surveillance, ethics and so on.

7.2 Interviews

In this section, the summaries of the interviews which were conducted will be presented. The first interview was conducted with three implanted employees from the travel and tourism company TUI. This interview was conducted in their office in Copenhagen, and the objective was to find out about their reasons behind adopting the technology, how their nearest relatives responded to it, use cases in the workplace and so forth. The second interview was conducted with the founder of Dangerous Things and Vivokey Technologies. Dangerous Things is a web store selling various implants and accessories for users to play with on their own. Vivokey Technologies, on the other hand, sells chips which can be used in an ecosystem of services, meaning the user does not have to play with all of the components themselves. The purpose of the second interview was to determine what a service provider and manufacturer of these components thinks of the potential of the technology and its potential drawbacks. This interview was conducted online, as the founder and his businesses are based in the United States. The transcripts of the interviews can be found in the appendix (*Appendices B and C)*.

7.2.1 TUI

In TUI, employees are offered to have a microchip implanted for free. They can then use this chip for whatever they want, as they own the chips themselves. In their office in Sweden, around 100 employees are chipped, whereas, in Denmark, there are around 7. They can use them to enter the offices, use the printers and the vending machines. Furthermore, in Sweden, they can also use them as a ticket when traveling by train.

For the interview, three implanted people from the Copenhagen office participated. These individuals had recently been implanted by their partner Biohax International which is based in Sweden.

The reason why they adopted the technology was for the fun of it, but also because they want to see the services and use cases expand so that they can use it for other things besides printing and accessing the office in the near future. They want to help the technology spread more rapidly. Also, they hope for a future where the technology can ease their daily lives, and also, reduce the management of all of the different cards and keys that they have.

They stated that a common misconception they heard was that the provider of the chip would now be able to track their location with GPS. However, prior to being chipped, they had been assured of the chip’s capabilities, and that a much bigger chip would be needed in such a case. Also, in terms of security, they seemed certain that the chips were quite safe since a person would need to get really close to scan the chip. However, one of them was concerned

with potentially using the chip for payment, as there is no authentication process aside from the ID being read.

In terms of issues, they stated that the signal strength of it is quite low. As a result, when trying to access their lockers, sometimes they would have to stand there for a while to make it register the chip within the reader field. However, they also mentioned that the lockers were not built with microchips taken into account and were optimistic that it will improve in the future.

Medically, they observed no issues or pain, whatsoever, aside from a little soreness initially. They compared the process of the injection to that of having a blood sample taken at a hospital.

The reactions that they had received by others were a mixture of negative and positive comments. Some were extremely upset and worried about surveillance, religious issues (‘mark of the beast’) and so on. Others found it exciting, but would not want to get the implants themselves.

They also see the potential for the chips in connection with their business. For example, they would love to see people being able to check-in at the airport using a chip or using them as keys at a hotel. So, they also do it to prepare for and potentially be ahead of competitors in the future.

Overall, they were not too worried about the technology not taking off, as the injection has not cost them anything and they can just have it removed if they want to.

They saw the biggest potential usage of the chips outside of the workplace, where the chips could be used for a variety of different things in the future. In the workplace, it is more limited.

They used an Android app to write in gimmicks and links (such as LinkedIn) to the reader. It is the same in case they wanted it to be used as a key to access stuff. As such, it is quite easy to write code to the chip. However, the services are quite limited right now. But overall, they found it quite easy to use.

In terms of costs, they stated that the injector told them that it would cost a person around 1,400 DKK to get an implant injected. However, usually, his customers are not private individuals.

In Sweden, the technology is a lot more accepted. They stated that this could be due to their openness to digitization and the way they explain technologies to people. But also, it is where Biohax International is located, which is a big provider of these implants.

Lastly, they were not optimistic about everyone having adopted the technology in the future, as some people will always be opposed to it, like with all technology.

7.2.2 Dangerous Things and VivoKey Technologies

The founder of Dangerous Things and Vivokey Technologies adopted the microchip technology back in 2005, and used for getting into the office, unlocking the computer and so on. As he saw an increased interest in the RFID hobby market, he started the Dangerous Things web store, in 2013, selling components which people could play with. In 2018, he started a new business called Vivokey Technologies. The aim of this company was to bring implants beyond the personal scope. Specifically, proving your identity, cryptographically, which can be used within their ecosystem for different services.

The Dangerous Things customers consisted mostly of people with a programming background or developers, who wanted to build their own thing using the components. On the other hand, Vivokey Technologies is for the people who do not want to build their own thing, and instead, just want it to be plug and play.

He saw a lot of negative attention early on, but as time passed the reactions became more positive. He thought that the negative attention was due to people having the wrong assumptions about the technology, such as being able to be GPS tracked, surveillance and those kinds of things. Also concerns with religious beliefs.

He sees the main selling point of the products as getting rid of the management burden. Having phone, wallet, keys and other wearables become a management nightmare. This is where he sees potential using microchips, which can drastically reduce this aspect.

In terms of security, he stated that the chips on their own are not secure. Basically, the RFID chips send a serial number to the reader and that is it. There is no encryption. Therefore, he argues that one should not use these for anything business related, payment and so on. However, with the Vivokey, one’s identity can be cryptographically validated, making it suitable for more critical services beyond the personal scope.

They buy all of their components themselves and have them assembled at a factory. This is to ensure that everything works and is quality assured, even though it is a bit more expensive.

He mentioned that he had not experienced any medical issues with his products, however, he had heard about products made by competitors breaking. This can be a big issue, especially if the people are using cheaper knock-offs, which have not been tested properly. Breakage could result in the leakage of hazardous substances and other concerns. Furthermore, he argued that the cancer research which had been linked to tumor growth due to implants had

several problems and biases, thus rendering it unscientific. So he is certain that his products are safe.

The reason he started Dangerous Things in the first place was to ensure that users could be injected safely by professional partners and be assured of the quality of the chips. However, many knock-offs are available now, which can be dangerous if people inject these. Especially if they inject them in the wrong way, without the assistance of professionals.

7.3 Subconclusion

This chapter investigated the rate of adoption of human microchip implants through the lens of Rogers' DOI theory. Based on survey data, several key points were identified based on potential adopters' perceived attributes of the innovation. The results showed that many respondents were able to identify the relative advantages of the technology, however, not so much for the aspect of seeing it as something prestigious. In terms of compatibility, this appeared to be the biggest barrier, as many people did not find it as something that would fit into their lifestyle and current social norms and values. Complexity, however, did not seem to be a factor which could impede the rate of adoption. Trialability statements showed that a significant portion of respondents was opposed to the idea of trying out the innovation on a limited basis, which may also affect the rate of adoption in a negative manner. In terms of observability, respondents were evenly spread out between positive and negative attitudes. As such, compatibility and trialability seem to be the biggest factors which could reduce the rate of adoption based on the survey data. It was also found that males and younger generations were more inclined to show a positive attitude towards the statements, which could mean that these groups would adopt the technology before the other groups.

Two interviews were also summarized. Here, it was found that the interviewees had gotten their microchip implants for the fun of it and because they saw potential with the technology in the future, which they wanted to help diffuse. The interviewees had also received a lot of negative responses on adopting the technology, especially from fundamental religious groups. Concerns with surveillance and tracking seem to be the main assumptions that people make about the technology. And while the chips seem unable to do GPS tracking, some security issues were identified, since the RFID technology uses no encryption. Also, it was found that they saw the most potential for the technology outside of the workplace, and thus, saw no scenario in which the employer would be the owner of provided implants. Lastly, right now, the services which can be used with the chips are quite limited.

This concludes the first part of the project. In the second part, the development of the prototype will be presented. This includes a framework to ensure security by design throughout the development process.

8 Security Development Framework

This chapter's aim is to introduce a security development framework used in order to induce security controls and security consideration into every phase of the development lifecycle. This ensures that the microchip web solution that is proposed in chapter 9 is secured by design. All the security and privacy aspects of the RFID microchip, that have been identified in relation to RFID and microchips are described in *Chapter 4.3*.

The importance of implementing a development framework that put security on the highest priority relies on the fact that, in these days, privacy and security is a hugely critical factor that must be taken into consideration, this is as mentioned also something that has been taken into law in the form of the GDPR, where it is required that companies operating in the EU must comply with this regulation (*Chapter 6)*. Failing to comply leads to big legal repercussions especially when developing and implementing web solutions that are storing and handling personal data and information from individuals.

There exist many concerns regarding security and privacy in implanting a microchip, and as mentioned in *Chapter 7.2*, the interviewees from TUI who had implanted microchips, mentioned that they usually were met with concern from friends and family due to privacy and security misconceptions. some of these misconceptions were that nefarious governments and company entities could track their location. Another concern had a religious connotation. The interviewees were even aware of the name of the passage that mentions, that in the end days people will be forced to wear a mark on the right hand or forehead, all 3 interviewees had the microchip implanted on the left hand (*Appendix B)*.

However, this thesis is not trying to advocate that, implanting a microchip and implementing it into a company is 100% secure. The belief that it is completely secure is largely misleading. This chapter will, therefore, analyze and describe the Security framework processes on the development phases (SDLC). The security processes and its underlying activities, presented in this chapter will be used on every aspect in the development of the microchip web solution. The microchip web solution is presented and designed in *Chapter 9*. A proof of concept of the solution is presented in *Chapter 10*.

The Security by design Framework that is introduced in this chapter will be used for developing and designing the microchip solution while ensuring that the issues and vulnerabilities that are mentioned in *Chapter 4.4.1* and *Chapter 4.4.2* can be avoided by applying security controls and considerations into every part of the development phase.

The security framework chosen for the development is the Security By Design framework (SBD). The principles behind this framework is introduced by OWASP (OWASP, 2016), with the aim to provide security principles to system designers. This assist in developing secure and robust systems that have security implemented into every phase of the development, so that it is secure by design. The use and implementation of SBD framework are clearly presented and documented by the ministry of CSA, Singapore (CSA Singapore, n.d.), the SCA report guides organizations in applying SBD framework in order to build security into the system development life cycle, in order to produce more cost-effective IT security measurements (CSA Singapore, n.d.). Furthermore, the report's SBD framework guideline is described in details and is used as the main source on how to implement such a framework into the development of the microchip web solution. The microchip web solution is designed/developed in *Chapter 9* and presented, implemented and assessed in *Chapter 10*.

8.1 System Development Lifecycle

Before describing the aspects of the framework, it is important to understand the general development life cycle normally used, namely the System Development Life Cycle (SDLC). The development lifecycles under the SDLC mostly mentioned are the waterfall and agile development model. Waterfall model has six phases that go from initiation to disposal, and the agile version of the SDLC is a set of principles for system development under which requirements and solution changes are possible. This is the collaborative effort which makes it possible to develop quick iteration of a working system to users who have changing requirements and priorities (CSA Singapore, n.d.).

The key principle here is the iteration part of the agile development lifecycle which means that the stakeholders that are responsible for the different phases are able to collaborate and update status through frequent meetings. This provides the possibility to go back and forth the phases and discover and resolve any unplanned issues or errors when needed.

8.1.1 Phases

The figure below (*Figure 8.2)* represents the six phases of an SDLC, namely initiation, acquisition, design/ development, implementation/assessment, operations/maintenance and finally disposal. These phases are usually the basis for any type of SDLC out there. The security by design (SBD) is applied to these 6 phases. The SBD will be described and presented in *Chapter 8.1.2*.

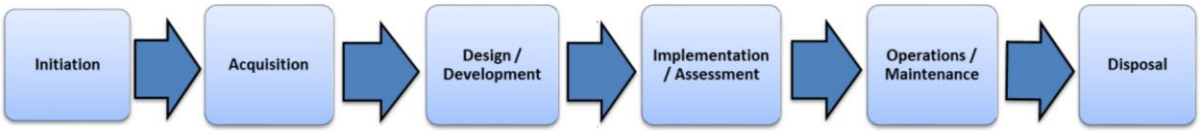

Figure 8.1: Phases of the Systems Development Lifecycle (CSA Singapore, n.d.)

8.1.1.1 Initiation

In the initial phase, presents the functional requirements and specifications of the web solution being documented (CSA Singapore, n.d.). The methodology behind gathering and specifying requirements can be done through different means, and the ones used for this microchip web solution were gathered through research, brainstorming, workshop meetings and interview with stakeholders such as employees or employer, etc. The functional requirements related to the solution proposed in this thesis are described in *Chapter 9* concerning the conceptual design.

8.1.1.2 Acquisition

When the functional requirements have been specified, the evaluation and preparation of the purchasing/procuring will be conducted in order to determine how to acquire the right elements needed for the system through a procurement process (CSA Singapore, n.d.). This phase is important in order for the acquirer to determine the cost factors and entities and if the cost of the solution outweighs the benefits, which is revealed after the end of the lifeline.

8.1.1.3 Design/development

The third phase is design/development, where the requirements and specifications are designed, coded and developed into the proposed solution (CSA Singapore, n.d.)

8.1.1.4 Implementation/assessment

The next phase is implementation/assessment. This phase is initiated when the solution is accepted, commissioned and in the process of being implemented (CSA Singapore, n.d.). An important aspect of the implementation/assessment phase is the need for various types of testing.

The first type is the testing of components installed as a part of a system (CSA Singapore, n.d.). This could in the case of microchipping be components such as the RFID reader module proposed in *Chapter 10*.

This then leads to the second part, system/solution integration testing. This part is conducted in order to test how all the elements that are a part of the solution works and communicate flawlessly together (CSA Singapore, n.d.).

The solution is then finally ready for deployment when all the testing are conducted and their results have been assessed and corrected.

The final step in the implementation/assessment phase, namely the deployment of the solution, is conducted when the solution has been approved by system designers and stakeholders such as relevant employer and employees (CSA Singapore, n.d.).

8.1.1.5 Operations/maintenance

The fifth phase, operations/maintenance is applied after the solution has been implemented, assessed and deployed (CSA Singapore, n.d.) So, when the system is operational and providing the results that were specified. In this phase, the system is assessed for modification needs, required enhancements, maintenance of hardware, software and system upgrades (CSA Singapore, n.d.). This means that the system designers must make frequent status updates on how everything is operating and if it is operating correctly or not. The system designer must also be ready to provide maintenance and support if something critical unexpectedly appears (CSA Singapore, n.d.).

8.1.1.6 Disposal

The final phase of the system development life cycle is the disposal phase, This phase appears at the end of the lifecycle when the system is no longer up to date and is therefore redundant or obsolete (CSA Singapore, n.d.). So, it is essential that the system must be disposed of by correctly terminating the system while safeguarding vital information when deleting or migrating data to a new system so that any existing information is preserved in accordance with regulations and policies (CSA Singapore, n.d.).

8.2 Security-By-Design Framework

The SDLC described earlier is an effective development methodology which is used by different companies and organizations. However, when developing these systems, security often is not prioritized and is sometimes it is not considered at all and it can, therefore, be costly if there are vulnerabilities or threats inherited from the solution, due to the lack of security measurements being taken in the development process (CSA Singapore, n.d.).

By applying Security-by-Design (SBD) lifecycle, the system designer is able to incorporate security considerations into the processes at every phase which is mentioned in the CSA article (CSA Singapore, n.d.). The importance of SBD and the practice of incorporating security consideration can help identify security risk early on in the development phase which consequently will result in a huge advantage in terms of more cost-efficient actions to counter

the security issues. The way to address and mitigate the identified security risk is to change the requirements of deployment to avoid identified security consequences while adding alternative and mitigating controls that would assist in reducing the risk factor (CSA Singapore, n.d.). If security risks that are too costly to avoid are discovered, then the security advisors can undergo a risk management process, in order to see if it would be acceptable to ignore the risk (CSA Singapore, n.d.). The security process of SBD means that security is evaluated at each phase and determined whether the security processes are required to mitigate the security risk. This provides understanding, security transparency together with appropriate decisions taken in a timely manner to reduce risk to an acceptable level (CSA Singapore, n.d.). The SBD framework is applicable to all computer system development projects which include ICT system, network technologies, and IoT (CSA Singapore, n.d.).

8.2.1 Security-by-design framework phases and its processes

Figure 8.2 shows the SBD framework applied to an SDLC. The six phases can be seen on the top of the diagram, these are presented vertically, starting from left to right.

The development phases are, as mentioned in *Chapter 8.1*, initiation, acquisition, design/development, implementation and assessment, operations/maintenance and disposal.

The Security by design processes are stated in the diagram below, named in the yellow boxes. These security processes are applied to each individual phase.

The activities are named in red boxes below its corresponding processes. The activities have the function of defining the expected outputs of the security processes (CSA Singapore, n.d.).

The SBD life cycles processes in each of the development phases run in parallel to the SDLC, which were described in *Chapter 8.1*.

Another important aspect of the SBD framework is Control gates this is where the activity result is validated and reviewed in order to assess the risk and vulnerabilities when important milestones have been reached (CSA Singapore, n.d.). The control gates appear on the diagram as a recycle logo seen in between the phases.

The Security-by-Design lifecycle (SBD) processes and activities that go into each phase are described below the figure (*Figure 8.2)*.

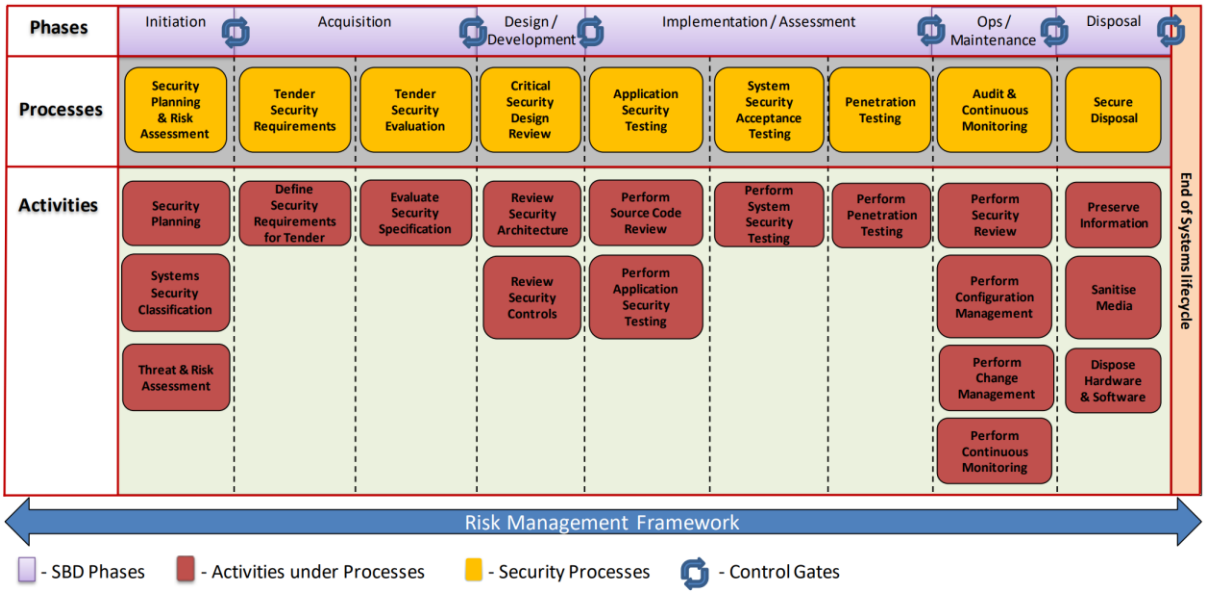

Figure 8.2: Security-by-Design framework (CSA Singapore, n.d.).

The description of the SBD processes mentioned below, contains a subpart that describes how and when these processes and activities relate to the microchip web solution are proposed in this report.

8.2.1.1 Initiation

Processes: *Security planning and risk assessment*

The two security processes in the initiation phase; security planning and risk assessment. which is where security considerations are integrated in terms of threats, security requirements, together with potential constraints of functionality and integration (CSA Singapore, n.d.)

The security planning and risk assessment consist of the activities; security planning system, security classification, and threat and risk assessment. These activities aim to integrate security at the early phase of the development (ref.). The security plannings aim is to understand security goals and objectives, and most importantly identify key actors of security roles (CSA Singapore, n.d.).

Security planning is, therefore, to be conducted as part of the initiation and planning phase, which also includes the outlining of key security milestones and activities for system development and assists in identifying the use of security in the design, architecture, and coding (CSA Singapore, n.d.).

The security planning is important since it identifies the key stakeholders. The key stakeholders, in this case, are the system actors that are involved with the development

progress, and whose decisions will have security implications for the system (CSA Singapore, n.d.).

The goal of the risk assessment processes together with the system security classification activities is to determine the security classifications of the proposed system (CSA Singapore, n.d.).
The findings from the security classifications will then be used for the threat and risk assessment to ensure that threats, risks, and security decisions are probably documented, assessed and approved (CSA Singapore, n.d.).

To summarize, the SBD phase 1 processes and reviews the functional requirement specifications, in order to identify the threats and vulnerabilities. This is done through risk identification analysis and evaluation, which is complemented by recommendations of appropriate security controls that are needed to mitigate and control the risks and vulnerabilities (CSA Singapore, n.d.). Threat and risk assessments must also take relevant standards and regulatory legal aspects into the system development considerations (CSA Singapore, n.d.)

Security-by-design for the proposed solution in phase 1

This subsection will describe the SBD security process and its underlying activities, in phase 1. Initiation of the system development life cycle. Phase 1 on the SDLC is presented in *Chapter 9.1*, functional requirements and specifications, this is where all the given requirements are specified and presented to the reader.

As mentioned in the previous section (*Chapter 8.2.1.1*), the SBD process conducts security planning to identify key security roles and assigning appropriate security classifications for the system.

The roles in the case of the microchip web solution are the; employee, system designer/developer, security administrator, and system administrator. These actors and their roles are described in the conceptual design (*Chapter 9.1*).

The security classification is determined in this solution in terms of critical information, entry, access, and otherwise elements of the microchip solution that if violated will degrade the confidentiality, integrity, and availability of the system. The specific system parts and their security classifications are mentioned in the conceptual design (*Chapter 9.1.1*).

The Microchip solution system and its underlying components are classified to the proper security classifications (i.e. low - critical). A vulnerability and risk assessment is conducted on the system requirements and this is done by reviewing the functional requirements specified

in the conceptual design (*Chapter 9.2*). This will be followed by recommendations for security controls that will mitigate the identified vulnerabilities and their risk to the system (*Chapters 4.4.1* and *4.4.2*), which can be implemented in later phases.

The risks and vulnerabilities are identified, described and complemented with recommendations for security controls, under each specified requirement in the conceptual design (*Chapter 9.1*).

8.2.1.2 Acquisition

SBD Security Process A: *Tender security requirements.*
Process A Activities: *Define security requirement for Tender.*

SBD Security process B*:* *Tender security evaluation.*
Process B Activities: *Evaluate security specification.*

The next phase of the SDLC development life cycle is concerned primarily with the identification of the security requirements, that is required from a component such as software and hardware, alongside an evaluating of the proposed security controls that would be needed in order to add security measures to the components. i.e. requirement to adhere to a minimum ISO security standard 27000, etc (CSA Singapore, n.d.).

So the first SBD security processes in the acquisition phase are; the tender security requirements, which is about defining and refining the security requirements as a part of a hardware and software components requirements submission (CSA Singapore, n.d.).

Security requirements should be clearly articulated, as mentioned in the article CSA (CSA Singapore, n.d.), its overall purpose and objectives should also be clearly stated, so that it is desirable to provide adequate measures and controls to meet the requirements, in order to protect the system in the area of confidentiality, integrity, and availability (CSA Singapore, n.d.).

Following this is the next SBD security process, namely the tender security evaluation which is the process that occurs after the components have been procured through a procurement process (CSA Singapore, n.d.). Here, it should be provided as an integral part of the overall evaluation of the tender submissions, meaning that it focuses on assessing security controls specifications proposed by the vendors (CSA Singapore, n.d.).

The activity includes a series of documentation review proposals for evaluations and clarifications on how the security controls would comply with ISO security standards. This proposal can be in the form of software hardware testing and demonstration and then documented in a tender evaluation report for recommendations (CSA Singapore, n.d.).

The activity requires documentation reviews, clarification, evaluation of proposals with the addition of some live demonstrations of the proposed components (CSA Singapore, n.d.).

Security-by-design for the proposed solution in phase 2

As mentioned earlier in this chapter (*Chapter 8.2*), the SDLC Phase 2: Acquisitions, is where requirements for components such as software, hardware, and vendors are defined, assessed and identified to determine if they can be used to provide the proposed functionalities (CSA Singapore, n.d.) i.e. the microchip web solution.

Whereas, the SBD Security process and underlining activities aim to define the security requirements for the software and hardware components that make up the system. The security requirements for the technology, hardware, and software needed for the Microchip web solution is carefully examined and reviewed in order to make sure that known risk and vulnerabilities are identified, the components and vendors security efficacy will be reviewed and documented. These reviews are described under each tech. description in the conceptual design (*Chapter 9.2*).

8.2.1.3 Design/development

SBD Security Processes: *Critical security design review*
Process Activities: *Review Security architecture, Review security controls*

The next phase of the system development life cycle is Phase 3 namely the design/ development as mentioned earlier in this chapter (*Chapter 8.2*), This phase begins after the acquisition phase has been finalized, so now the tenders have been approved and are ready to be integrated into the System design (CSA Singapore, n.d.).

The security by design process; Critical security design review shall be conducted to check that the system architecture is secure and if not, then appropriate security controls are put in place in the design (CSA Singapore, n.d.).

Critical security design review is where the review of Security Systems architecture and controls is initiated. This process ensures that those security requirements are correctly incorporated into the system design and can be implemented to meet security requirements (CSA Singapore, n.d.).

The underlying activity is the review of security architecture. The system is composed into smaller components so that its inner workings can be identified to identify trust boundaries, information entry, access points and data flows sorted, meaning that the Architecture documentation of the proposed solution is reviewed in terms of vulnerability assessment and security recommendations (CSA Singapore, n.d.).

The next activity in the security process of critical security design review is reviewing security controls. This activity is primarily about reviewing the security of the system architecture to scrutinize the security controls put in place as part of the system design. This can be complemented with an additional analysis of the cost of implementing operations security control (CSA Singapore, n.d.).

Security-by-design for the proposed solution in phase 3

As mentioned earlier in this chapter (*Chapter 8.2*), the SDLC phase 3. design/development, is where the proposed solution is designed and developed. Here, the system is described and fragmented into separate components, in order to clarify the exact parts and inner workings of the proposed solution and define the information and process flow of the user interaction with the microchip web solution.

The SBD security process, in this case, is to make a critical security design review to validate that the system is secured and that the appropriate security controls are put in place. This is to ensure that, the system designs security requirements and controls are met and can be implemented while still meeting the microchip web solution system.

The two process activities that will be made in the conceptual design (*Chapter 9.3*) is the review of the security architecture and security controls. The review of the security architecture will be made on the overall microchip architecture described in the design chapter (*Chapter 9*) and the proof of concept in *Chapter 10*. The security consideration and requirements will be assessed and aligned with the design and flow of the microchip system architecture and its underlying components.

Security controls are added to the system design in order to mitigate the identified security risk and vulnerabilities. These controls are being reviewed and documented in the conceptual design (*Chapter 10*).

8.2.1.4 Implementation/assessment

SBD Security Process A: *Application security testing*
Process A Activities: *Perform source code review, Perform application security testing*

SBD Security Process B: *System security acceptance testing*
Process B Activities: *Perform system security testing*

SBD Security Process C*:* *Penetration testing*
Process C Activities: *Perform penetration testing*

The fourth phase of the SDLC is the implementation/assessment phase which as mentioned earlier in this chapter (*Chapter 8.2*) begins after the architecture of the system design has been approved.

As the system is being implemented, security source code review and application testing should be conducted to ensure that the solution has been probably built from a bottom-up perspective to identify if there is any real liabilities or threats in the code or in the application provided to the customer (CSA Singapore, n.d.)

The application security testing is to ensure that, vulnerabilities are surfaced, addressed and detected early on during the development of the solution (CSA Singapore, n.d.). The first activity of the application security testing is the security source code review. Here, a systematic Source Code examination of the application is conducted in order to find security issues that have appeared due to insecure coding practices, malicious intent or coding errors (CSA Singapore, n.d.). This review should examine the codes for common issues like input validation, authentication, and access control implementation of security functions, encryption access controls as well as backdoors logic bombs, unnecessary functions, known language-specific vulnerabilities (CSA Singapore, n.d.).

This lead to the necessity of making mitigation plans to address all the vulnerabilities and risks that were found, which is followed by validation on the effectiveness of the mitigations (CSA Singapore, n.d.).

The next activity in the first SBD process, namely Application security testing, is a process where a test on the system is conducted to determine if the corresponding modules are fit for use (CSA Singapore, n.d.). The combination of these modules make up the system, so the aim is to isolate each part of the system and show that individual parts are correct. this is to ensure that, problems are identified, assessed and mitigated early in the development lifecycle and prior to integration, by testing the parts of the system first and then testing the sum of its parts (CSA Singapore, n.d.). After this test, a mitigation plan has to be put in place in order to correct all the vulnerabilities found. This could be followed by a regression test to validate the effectiveness of the mitigation actions which also needs to be proved or risk accepted prior to performing security acceptance testing (CSA Singapore, n.d.).

The security acceptance testing is when the system is being tested as a whole against a set of security test cases, which means that prior to the development of the system it can be necessary to conduct penetration testing to check for any vulnerabilities and risks that were not identified or addressed adequately during the previous phases (CSA Singapore, n.d.).

The security acceptance testing is conducted to verify that, the complete system satisfies the specified requirements. It verifies that the security requirements and controls have been improved as part of the system design and is acceptable to be deployed so that they can identify the system configuration against security specifications (CSA Singapore, n.d.).

Penetration testing is made on the overall system and components in order to see the system security defenses in different use cases, meaning that it evaluates the security of the system and the efficacy of the implemented security controls and policies (CSA Singapore, n.d.).

Penetration testing also called pen testing, is the practice of testing a computer system network application and identify vulnerabilities that an attacker could exploit, these may exist in the operating system, service application, configurations, risky user behavior (CSA Singapore, n.d.) Conducting a pen test provides information about the target to identify actions to encounter the vulnerabilities (CSA Singapore, n.d.).

Security-by-design for the proposed solution in phase 4

Phase 4 of the SDLC implementation and assessment is as mentioned earlier in this chapter (*Chapter 8.2*) initiated when the system architecture design has been approved. There are 3 SBD security process all with corresponding activities, the 3 processes are application security testing, system acceptance testing and penetration testing.

The system architecture of the microchip has been presented and proposed in the conceptual design (*Chapter 9*), while the solution chapter (*Chapter 10*) will present the final solution through documentation and visual images. Here, the SBD security processes are applied in order to test and assess the microchip web solution. However not all testing seem relevant to this particular proposed solution since it has not yet been implemented in a real-life scenario.

The first security testing process that is relevant to conduct is application security testing. The underlying activities in the SBD are; source code review, here the source code behind the authentication access control system will be reviewed, this is then followed by an application security and system acceptance testing/assessment on the whole conceptual system against some security related use cases. This will be reviewed and described in the proposed solution chapter (*Chapter 10*).

Penetration testing will be made on the Authorization access control module which is coded, developed and described in the proposed solution chapter (*Chapter 10*).

8.2.1.5 Operations/maintenance

SBD Security Processes: *Audit and continuous monitoring*
Process Activities: *Perform security review, perform change management, Perform configuration management, Perform Continuous Monitoring*

As mentioned earlier in this chapter (*Chapter 8.2*), the SDLC operations/maintaining phase is set in motion when the system is running and in place. The operations are performed when enhancements and modifications are introduced to the system and tested from a software and hardware perspective (CSA Singapore, n.d.).

From the security by Design framework perspective, the security process of auditing and continuous monitoring takes place. This process has four activities which are to; perform security review, perform change management, perform configuration management and perform continuous monitoring (CSA Singapore, n.d.).

The process of continuous auditing and monitoring is to ensure that the operational system is running while addressing the system security against current risks (CSA Singapore, n.d.). Activities of this process include the need to perform regular general and technical security control reviews, in order to determine if the security controls are in place and continuously effective over time (CSA Singapore, n.d.).

Furthermore, it is necessary to perform proper change management. Change management is to identify significant changes an impact that alters the system security posture (CSA Singapore, n.d.)

The third activity performed in this process is the configuration management. The reason for performing configuration management is to ensure that the security after system changes remains effective and negative effects on the security requirements are minimal (CSA Singapore, n.d.).

Continuously monitoring the current state of the system is to frequently review and monitor the system security vulnerabilities. This is essential in order to determine if security controls continue to be effective over time during system changes, environmental changes and additions of technology and security policies issues, since inadequate control of changes in over time can result in late discovery of issues and vulnerabilities, which can affect the mitigation cost (CSA Singapore, n.d.).

Security-by-design for the proposed solution in phase 5

As mentioned earlier in this chapter (*Chapter 8.2.1.5*), Phase 5, operations and maintenance is conducted after the system has been implemented and integrated into the company that has adopted the microchip solution.

The SBD security process in this instance is concerned with audit and continuous monitoring which have some underlying activities that provide the result.

The fact that the SBD framework offers this element is one of the reasons why SBD has been added to the SDLC of the microchip web solution. This solution is flexible and dynamic, meaning that new IoT, RFID components can be added to chip and reader technology, etc. constantly improves and gets more accessible and therefore it is necessary to audit and monitor these aforementioned changes and adapt as quickly as possible, so that these changes are not negatively impacting the overall security posture of the company that has adopted the Microchip web solution.

The conceptual solution and proof of concept are not implemented by any companies yet, so the SBD process in phase 5 is not conducted in the thesis report. The aforementioned is simply a guideline for the later phases of the SDLC and SBD.

8.2.1.6 Disposal

SBD Security Processes: *Secure disposal*
Process Activities: *Preserve information, Sanitise media, Dispose hardware and software*

As mentioned earlier in this chapter (*Chapter 8.2.1.6*), the final phase of the SDLC, is Disposal. The Disposal phase is set in motion whenever the system is obsolete and no longer in service, and therefore termination, migration, deletion, and disposal of hardware and software is set in place (CSA Singapore, n.d.).

The SBD security process in this phase is the Secure disposal. The underlying activity in this process is preserving information, where sensitive data is to be archived, or migrated to another system (upgraded system) and facilitated for later use (CSA Singapore, n.d.). The archival and preserving of sensitive information must be done in compliance with the GDPR (*Chapter 6.3*) in order to ensure that, the employee can determine what should be done with the information.

The second activity in the secure disposal process is the sanitation of media, where all information, images, video, etc are properly sanitized from media storages and devices (CSA Singapore, n.d.). The aim is to assess the medium that the media was recorded on and make risk assessments on confidentiality.

The third and final activity of the Security by design framework is Dispose of Hardware and software. This is where hardware, software and other equipment related to the system can be sold, discarded, recycled or given away in a secure manner without loss of valuable data and information means that it is applied in order to ensure that the disposal is done correctly and under compliance of recycle/waste regulations (CSA Singapore, n.d.).

Security-by-design for the proposed solution in phase 6

The final activity of the SDLC is phase 6: Disposal (*Chapter 8.2*). This phase is to be conducted when the microchip solution has been obsolete, and need to be replaced by a new solution. It can also be whenever individual components of the system are obsolete or not working anymore etc.

The system development life cycle of the conceptual solution has not yet reached this phase, however, the aforementioned is used for a guideline when the SDLC has reached this phase in the future.

8.3 Subconclusion

This chapter began by introducing the SDLC development phases, where each phase was defined and described in terms of the processes that occur in these development phases. This was then followed by an introduction into the Security-by-design framework, processes and activities related to applying security into each of these development phases.

The processes together with the expected output of the security activities of the SBD framework, was presented and described. Finally, guidelines were detailed on how to apply the SBD framework in the case of the proposed solution.

The purpose of this chapter is to provide a secure development framework to the development of the microchip solution which is designed in the next *Chapter 9*.

9 Conceptual Design

The design features and requirements of the proposed solution are specified, described, presented and then visualize and documented using Unified Modelling Language (UML). This solution is aiming at developing a human microchipping system suitable for companies. The system enables unique services and applications for companies and its employees, that would ensure a convenient and user-friendly interaction and access to the company facilities and IT infrastructures.

A Solution overview with a visual depiction of the architectural design of the Microchip web solution will be described in *Chapter 9.3.3*. This entails graphical interpretations of the conceptual company that has adopted the proposed microchip web solution. The solution overview is presented to the reader with the aim of providing a high-level, conceptual understanding of how the Microchip web solution would operate in a company.

It is important that the microchip web service is secured and private. This is to ensure that the adoption of the solution will not result in the risk and vulnerabilities that are mentioned in the *State of the Art* (*Chapter 4.3*), since this would endanger the confidentiality, integrity, and availability of the microchip web solution and by that the company in itself i.e. theft of physical and intellectual property, classified information, unauthorized access, etc. Therefore, offering a solution to a company where employees can implement a microchip in their hand, and through that interact with authorization required functionalities, is inherently something that must be designed and developed with security considerations and mitigations in every phase of the development. So, as mentioned in the security framework chapter (*Chapter 8.1*), the development methodology used for the development of the microchip web solution will be the integration of Security-by-Design framework into an Agile system development life cycle.

There exists 6 different phases of the SDLC, the 1. Initiation, 2. Acquisition, 3. Design/ development, 4. Implementation/assessment, 5. operations/maintenance and 6. Disposal. (*Chapter 8.1*). This chapter is concerned with Phase 1, 2 and 3, whereas *Chapter 10* on the proof of concept will be concerned with parts of phase 4 (testing, implementation).

Phase 5 and 6 is not documented in this report, since Phase 5 and 6, are not initiated before the solution is completely integrated into the company (*Chapter 8*).

The SBD security processes and its underlying activities defined in the security chapter (*Chapter 9*), will be conducted in the corresponding SDLC Phases. The SBD processes and activities will be presented, discussed and highlighted, in this chapter in a subsection under each subchapter.

9.1 Phase 1: Initiation - Requirements and Functionality

This subchapter will present and explain the functional requirements for the microchip web solution, designed in this chapter. The functional requirements have been specified through research of microchip and RFID technology, together with research of existing access control through RFID (Smartcard) solutions. Additionally, the interviews described and presented in *Chapter 7.2*, provided some insight into the usual functionalities offered/experienced, as well as acceptance feedback on a microchip web solution that could provide personalization. The reasoning behind each individual functionalities that are provided with the microchip web solution, is explained under their respective section below.

The functional requirements of the microchip web solution are divided into two categories; Access control and Personalization. The access control feature whereby employees, implanted with a microchip can get authorized access to company facilities and RFID enabled components, is a common service that is already provided in different varieties by i.e. companies mentioned in the *State of the Art* (*Chapter 4.1*). whereas the Personalization aspect of the microchip web solution is unique in terms of combining implanted microchip authorization and IoT.

The Security by Design (SBD) process in Phase 1: initiation, is Security planning and risk assessment. This process has 3 underlying activities: Security planning, system security classification, and Risk assessment. These activities have the aim to ensure that the system in development is secured and threats and vulnerabilities are identified and mitigated if possible (*Chapter 8*). The SBD processes and activities output/outcome will be defined and described in a subchapter at the end of each development phase.

9.1.1 Access control requirements and features

The Features related to the Access control category is an important aspect of the microchip web solution. This aspect of access control makes it possible for the employee to interact with RFID enabled access control devices, these devices are installed in the company and integrated to the microchip web solution. This aspect provides convenience to the employee since the proposed solution enables fast access, without the need to use a physical card (which can be lost or stolen.), or manually sign in, etc.

The features that are listed below all have one thing in common namely that they are offering access to various RFID enabled access control units through the authorization of the employee with a microchip, who is uniquely identified by Unique ID (UID) information stored on the microchip, this inherent some risks and vulnerabilities. The risk and vulnerabilities

identified in the specified requirements will be explained in the SBD processes' subsection of this subchapter (*Chapter 9.1.3*).

Access control features enabled with the microchip web solution:

- *Authorized access to the facility*
- *Role-based access within the facility*
- *Authorized and personal access to IT equipment* (Such as pc, printers, projectors conference room booking)
- *Enable purchases using microchips* (canteen, coffee, vending machine, etc)

9.1.1.1 Authorized access to facilities

One of the features that the proposed solution offer is easy authorized access to enter the company building along with user and role-based authorized access within the facility (more about role-based access to the facility will be mentioned below in *Chapter 9.1.1.2*) etc. With reference to *Chapter 4* where it is presented that the access was authorized via smart cards equipped with an RFID chip. But, this method has some well-known security threat and implications (*Chapter 4.4*). e.g., if the card is lost and stolen. This solution proposes a way for employees to enjoy secure and convenient access to company buildings using their implanted RFID chip on the same or similar RFID reader devices (*Chapter 5.2*). This means that the employee can walk right over and wave their hand in front of the RFID reader device which will then open the door/lock because of the implanted (in whatever hand the employee prefers).

It prevents a person in danger of losing the chip and make the password requirement useless. Since the implanted chip operates as a near field passive RFID chip, it implies, cloning (*Chapter 4.4.1*) or tracking is not really possible since the chip is powered by the reader and have to be quite close to read the chip (*Chapter 5.4*). Authorized access to buildings via an implanted RFID chip is in itself not something unique. But, it is an important requirement for our solutions as a whole since it will be used together with a combination of useful existing microchip RFID services and RFID compatible IoT devices for convenience and personalization.

9.1.1.2 Role-based user access within the facility

This feature which will be a part of the proposed bundled solution is enabled through the same techniques mentioned above. However, this solution will provide role-based user authorization, means, all employees have at least standard access (i.e to access company

building) but since the employees also can have unique access to their own personal office and possibly, the employees can be assigned to different levels depending on their roles. Again, this solution would enable the possibility for the RFID system installed in restricted areas which require specific permission, etc. It can differentiate between employees and their roles, and provide access accordingly based on authorization and user identification.

9.1.1.3 Authorize and personal access to IT equipment

The Implanted RFID chip solution will enable convenient user access to IT equipment such as PC, laptops, and printers by waving the hand at the reading device. This will then initialize the identified employee's pre-selected configuration. It is an interesting feature but before delving into that, one must understand the meaning of enabling convenient user access to pc, laptop, and printers. Convenient access to pc and laptop means, that the employee can log into their PC and laptops by their implanted chip. This removes the tedious well-known task of entering a username and password every time an employee has to log in. Again, it works in the same way as discussed in the previous section where the employee waves his or her hand at the RFID reader. The reader could be installed on the laptop or at the entrance of the office or room. The convenience here lies in the fact that an employee can have multiple logins for different systems or departments and it could waste valuable office hours if the employee has to input different user login credentials multiple times a day.

The security aspect here is also overwhelming due to the fact that it is more difficult for other people to actually hack one's password, especially now that, the password can be much longer than anyone can remember. The other enabling factor of the RFID solution is the aforementioned feature is accessing the printer without typing in any user access information. Again, here the user only has to wave their hand at the reader to get access to the printer. This is also convenient because it can be a lengthy and tedious task when having to write username and password credentials into a printer. The reason for this is obviously the lack of user interaction capabilities on a printer terminal. Generally, it is a small compressed screen with a poor touch function which is really difficult to press the right letters and can be demotivating for the employees. So, having the capability of accessing the printer just by waving your hand at a reader, is a helpful aspect that will optimize and make the whole process of accessing IT equipment in a company more convenient.

9.1.1.4 Purchase using microchips

This feature grants the possibility for the employee to buy food in the canteen, coffee, and snacks using vending machines, etc. Using implanted microchip is a helpful, convenient way to make purchases in an environment such as in a company. Now, the employees do not have

to use a credit card or cash, which can be quite good to counter the vulnerability of theft, losses, etc.

This feature can be implemented in two ways. Firstly, by adding credit card information on the implanted microchip. This will enable the employee to use it outside the company in shops and stores as long as their credit card payment device has an RFID reader, as many shops and stores in Denmark have.

The second method is to log every purchase to the employee's user account, which means, when an employee buys something in the canteen or vending/coffee machines, he or she will swipe their hand at an RFID/smart card reader. The amount of money the employee has to pay will then be registered in the user account. The total amount can then be withdrawn from their salary at the end of the month. This feature is optional and is something that can be selected if the company requests it. This includes companies where employees get coffee, snacks, and food for free.

9.1.2 Personalization

The IoT and Personalisation functionalities offered by the microchip web solution is the second aspect of the proposed solution. The personalization is provided by IoT components installed in the company and integrated with the Microchip web solution, which basically means that the employee can choose their preferences regarding the IT and IoT company components, which will be remembered and initiated automatically upon microchip authorization. So consequently, the Access control units can communicate with the IoT devices, through the microchip web service. The addition of the personalization aspect leads to some security risks and vulnerabilities which is addressed by applying the SBD processes.

Below is a list of the standard company devices, where the setup of preferences can be applied to. However, it's important to mention that other devices could be integrated into the solution, as long as they have a wireless/wired connection to the internet, where it’s settings can be configured. This will allow for communication to the microchip web solution. The first part will describe each feature under the “Personalization” category. This will be followed by the documentation of the Security by design processes related to the Initial Phase 1.

- *Room temperature/Ventilation/Air-conditioner*
- *Lights Settings*
- *Allergic and food preferences notification from the canteen, vending machine, etc.*

- *Seamless access and interactions between different components of the system* (pre preparations, readiness, etc)
- *Microchip Web app, where employees can set up account settings and preferences.*

Using personalization and customization is something that can bring ease and enjoyment as well as boosting workplace morale. The personalization in this solution is expressed by having a user interface where employees can adjust their different preferences in the employee preferences interface. These features touch everything from room temperature, lights, food preferences as well as initialization of making office spaces “ready” for accommodating the employees' personal preferences.

9.1.2.1 Room temperature, ventilation, and air-conditioner

Room temperature preferences vary from person to person, therefore this solution provides the possibility for employees to set their preferred temperature and air-conditioner. If the employee has their own office or they are booking a conference room and they are swiping their hand at the entrance, then the installed smart heater/air-condition will set the temperature to the employees preferred settings. This can be changed on command through the employee preferences interface which is described in *Chapter 9.3.1*.

Incorporating IoT in this solution provides endless possibilities. This is due to the fact that more and more smart IoT devices are developed and connected to systems in places such as companies. These devices can be implemented into the preferences user interface system, where the employees can choose their preferred outcome upon interaction.

Another example that has been added to this solution is light settings.

9.1.2.2 Light settings

Using the same techniques as with the installed smart heater and ventilator air conditioner, the employee can choose their preferred settings of light, color, and dimness. With a smart bulb connected to the RFID system, this can be activated upon an employee’s interaction with the reader.

9.1.2.3 Allergy and food preferences notification

Another feature that this solution offers is making it possible for the employees to notify the system about food allergies, religious and food ideologies preferences, etc. So, if the employees have any food allergies or if their religion forbids certain foods or if they are vegan or vegetarian, they can notify the system via the employee preferences interface (*Chapter 9.3.1*), which will alert the employee if they are about to buy something that goes against what

they preferred. The use cases and scenarios of the above-mentioned features will be presented in *Chapter 9.3.2.3*.

9.1.2.4 Seamless access and interaction between different components of the system

The final feature in this proposed solution is seamless interaction between different parts of the system. To elaborate it further, the proposed solutions can preset heating ventilation, smart bulbs as well as sign in to a PC with the microchip. These functions can be called automatically whenever, the system has detected that employee has entered the building or the office room or the conference room, etc. Then the IoT smart devices along with the PC turns on to the preferred settings. As mentioned before, this can be enabled on the employees prefer interfaces, here there will be different settings which will be explained in *Chapter 9.3.1*.

9.1.2.5 Microchip web app for account settings and preferences

The personalization features of the microchip solution, requires a graphical user interface, in order for the employee to be able to log in and set up their account and user preferences. The microchip web solution offers exactly that, a web app where company employees can log in and view/setup various settings and configurations. The microchip GUI (Graphical User Interface) and its functionalities will be presented and described in *Chapter 9.3.1*.

9.1.3 Security-by-design process in phase 1: security planning and risk assessment

The security planning and risk assessment process aims at integrating security at the Initial development phase (*Chapter 8.2*). The first activity in this process is the security planning, this activity presents 4 different expected outputs.

9.1.3.1 Security planning

The first expected output is the identification of key security roles. The second expected output is setting common goals for the security requirements of the system. The third part of the security planning activity is to outline key security-related milestones and activities for the development of the solution. The Final part of the security planning is to identify secure design, coding and architecture practices (*Chapter 8.2.1.1*).

Security roles

The Stakeholders in the SDLC is the Employee with the implanted microchip (employees can have different roles and access authorizations in the company), company representatives/company system administrators and finally the system designers.

These actors also have security roles, i.e. the employee and company representative role is to provide input to the Threat and Risk Assessment (TRA) on risk and threats pertaining to their business operations/interactions, whereas the system designer needs to provide input to the TRA on risk and vulnerabilities pertaining to the system development (*Chapter 8.2.1.1*). The final security role needed in the case of microchip web solution is a security consultant/officer who preferably is the one performing the Threat and Risk assessment, in order to determine the level of risk that the system is exposed to, and recommending the appropriate level of protection relative to the system classifications.

The security activities of the security consultant/officers will be conducted by the authors of this report.

Common goal for security requirements of the system

The microchip web solution is offering the employees easy and convenient all-in-one access opportunity within a company who has adopted the solution. This means that the common understanding of the security requirements should be as such;

1. All microchip/employee related data should be protected i.e. from hackers with malicious intent to steal or change the data, such as user info and intellectual property.
2. All Information related to the employee/company's privacy should be stored and handled under compliance with privacy regulations such as the GDPR.
3. The integration of the microchip web solution should not negatively impact, the overall security posture of the company and this is also true when installing the RFID enabled IoT devices that are used with the microchip web solution.

Security-related milestones and activities for the solution development

The key security milestones of the microchip web solution are placed in between the SDLC dev. phases.

First security milestone is when the security classifications of the system have been identified, determined, and the TRA has been conducted, which is occurring in the initial SDLC phase 1.

The second milestone is when the security requirements for the components and device that makes up the microchip system, has been reviewed and evaluated, this milestone appears at the end of the Acquisition phase 2.

The third milestone is when the security of the system together with the proposed security controls are applied to the design, assessed and approved. This occurs at the end of design phase 3 of the SDLC.

The fourth milestone is when these security controls and mitigations have been implemented and assessed, through various types of Security Tests, this appears at the end of phase 4 of the SDLC life cycle. The same logic goes for phase 5 and 6 of the SDLC Namely that the milestones a placed at the end of the phases.

Secure design, coding, and architecture practices

The fourth output from the security planning activity is to determine the right choices of secure design, coding and architecture practices, so the design and architecture of the microchip web solution must not become an unintended weak link to the security of the company and by that negatively impact the overall security posture. This is done by ensuring that the communication between the different subparts of the system is encrypted and by security activities, which increases the confidentiality, integrity, and availability of not only the Microchip web solution but also the company in itself.

Furthermore, it entails that the code, is secured from malicious code, logic bombs, bad coding practices, this is described in the proof of concept part (*Chapter 10*).

9.1.3.2 System security classification

The next activity in this SBD security process is the System security classification, where the different parts of the system are examined in order to determine the security classifications of the system (*Chapter 8.2*). This activity has two expected outputs, the first expected output is the different security classifications of the system, meaning that different subparts of the system may not all be equally classified and therefore have different security classifications. The second expected output in this activity is the definition of high-level security requirements that needs to be fulfilled for each security classification.

Security classifications of the system

The system subparts of the solution will be presented and classified according to its security implications towards the system. The different parts are described in phase 2 acquisition (*Chapter 9.2*). However, it will be presented here for security classification purposes.

1. The first subpart of the system is the microchip. This is the microchip that is implanted in the employee. The information stored on the chip is the Unique ID (UID). This UID is related to a table in a database containing the employee info and preferences, which means that the microchip part of the system is a highly classified entity, which would need to be secured through proper security requirements.

2. This leads to the second part of the system, namely the Database (DB)/Server, where all the microchip related information is stored and the DB/Server is categorized as a highly classified part of the system.

3. The third part of the system that needs security classification is the Microchip web app, where the employee can set up their account and preferences. This means that this web app gives the employee (or nefarious person) read and write permissions, making it possible to set up and modify account setting and preference info. which is related to that employee. This leads to the conclusion that the Microchip web app is a highly classified part of the microchip system. The microchip web app is presented and described in (*Chapter 9.3)*.

4. The next part of the system is the RFID enabled access control units. These readers scan the microchip in order to check for authorization and the devices enable easy access to the company facilities and are therefore a highly classified part of the system. Same goes for the IoT devices that are installed in the company and integrated with the solution. Since the RFID reader and IoT devices communicate with the microchip system it means that they present point of entry vulnerabilities to the overall system which concludes that the RFID and IoT devices are highly classified aspects of the system.

High-level security requirements for security classifications

The Final activity of the system security classification is the “high-level security requirements for the security classifications”. The expected output here is the specification of the security requirements that are needed in order to provide a robust and secure system, on a high level. The requirements here are defined through analysis of existing solutions, security risks and vulnerabilities that are mentioned in *State of the Art* (*Chapters 4.3* and *4.4*) and *Technology Background* (*Chapter 5*), together with security considerations, that was received through interviews with individuals who had first-hand experience with implanted microchips as well as internal discussions amongst the group members behind this thesis.

The Security requirements for each security classification are listed below.

1. *Microchip*

    a. Personal information that can be used to identify employees is not to be stored on the microchip.

    b. It must not be possible to track, the employee/microchip

    c. The read antenna distance of the microchip must be sufficiently low.

d. Data on microchip should be secured

2. *Database*

    a. The database must be secured from unauthorized access.

    b. Information stored and handled on the DB/server must be encrypted, and certified with SSL certificates.

    c. The information must be backed up on other servers in case of loss of data and/or availability

3. *Microchip web app*

    a. Users must log in with not only username and password but with two-factor authentication, this is in order to prevent unauthorized access from malicious hackers.

    b. The information and data that is traveling to and from the DB, must be secured through SSL certificates.

    c. The app must be a standalone app with functionalities limited to the absolute minimum. This is to ensure that the app is not vulnerable to the security issues, such as logic bombs, etc. that may come to life due to the app being over complexed.

    d. The code behind the microchip web solution must be written in a way that it avoids bad coding practices, back doors, logic bombs, etc.

4. *RFID reader enabled devices*

    a. Devices must only have Read capabilities, meaning that it is not allowed to write anything on the chip

    b. The data transmitted between the RFID reader and the web service must be encrypted, and secured from man-in-the-middle attacks.

    c. The RFID reader access control units must only grant access to Authorized personnel

5. *IoT devices for personalization*

    a. The data transmitted between the IoT device and microchip web service must be encrypted so that it protects against malicious attacks such as man-in-the-middle attacks.

b. The Integration of the IoT devices must not negatively impact the overall security posture of the system and the company. i.e. becoming a weak entry point-of-access to the entire system.

9.1.3.3 Threat and risk assessment

The third and final activity in the Initial development SBD process is the Threat and risk assessment (TRA). The aim of the TRA is as mentioned and described in *Chapter 8.2.1.1*, to systematically process and identify various risk and threats to the system while determining the level of risk that the system is exposed to. This is followed by recommendations for appropriate levels of system protection (*Chapter 8.2.1.1*).

This means that the expected output in the TRA activity is the TRA report/document. This report identifies and details the potential risk and vulnerabilities that could negatively impact the company business and employees privacy (*Chapter 8.2.1.1*). This is complemented with recommended security controls that need to be implemented to reduce the risk to an acceptable level.

TRA report/document

The Potential security risks behind the functional requirements that were specified in *Chapter 9.1.1* are identified and described. In addition to that, the security controls required to mitigate the risks are proposed.

Risk assessment of the functional requirements in the microchip solution is detailed below.

Access control category features and defined requirements

The functionalities and features presented in *Chapter 9.1.1* are divided into two parts namely the access control and the personalization. The first part to be assessed is the features in the access control category:

A. *Authorized access to facility:* The risks and vulnerabilities that are associated with the specified requirement of when the employee is able to access the facility through their implanted microchip. The microchip in itself is relatively limited in terms of memory and processing power/speed, which means that elaborate encryption algorithms and other security mechanism is difficult or impossible to implement, meaning that extra security measures should be added in order to completely secure the feature.

    1. *Proposed security control for requirement A*: The information to be stored on the microchip only have to be the unique ID (UID). This UID references to a table pertaining to the employee information which could include an encrypted

4-digit pin. This means that when the employee swipes their hand at the RFID enabled access control unit, will lead to the RFID access control reader prompting the user to insert a 4-digit pin. This data is then encrypted from the reader module to the microchip web service. Finally, the pin code that is inserted into the access control unit is verified against the encrypted pin code. The lock/door will open if there is a match (if the pin number is correct).

2. *Proposed security control for requirement A***:** Another security control that could be applied would be to only allow specific microchips to be allowed in the solution. The microchip that is to be allowed is a near field, passive microchip with a maximum reading distance of 30 cm. This would ensure that malicious hackers will have difficulties in cloning the data that is stored on the chip. Furthermore, the microchip is implanted and therefore not stealable, automatically mitigates a huge risk, namely the theft factor.

B. *Role-based access within the facility:* The feature of role-based access within the facility is in itself a security feature, that only provides access to specific employees that have been given permission and authorization. However, the limitation issues of the microchip are also relevant for this feature. Namely the need to provide extra security measures to ensure the privacy and security of the implanted microchip. This means that the security controls regarding the addition of a 4 digit pin are also relevant here.

C. *Authorized and personal access to IT equipment:* This functional requirement enables the use and sign in of IT components installed at the company through an RFID reader access control unit installed on the device. The microchip web solution enables the customer to quickly and with convenience sign-in with only a swipe with their hand on the reader. This feature is in itself a security requirement. This is especially true when considering the fact that, the microchip cannot be stolen or lost, meaning that the system can be confident that it is authorizing the correct employee. Additionally, the overall security level of the system will be enhanced thanks to the security controls. With regards to pin code and short antenna reading distance, these security controls were mentioned in feature a.

D. *Enable purchases using microchips:* This functional requirement is allowing the employee implanted with a microchip to purchase food/drinks and snacks at the company canteen and/or vending machine. The risk that appears is that it won't be smart or even possible to clone a credit card information into the microchip. Even if this cloning took place, then it can only be read by a reader with specific software.

1. *Proposed security control for D*: A way to mitigate that risk and still be able to allow such functionality is if the employee is able to deposit money to a bank account through the microchip web app. The funds deposited would then be registered and stored in the DB. So, when the employee purchases something, then the microchip web solution will check the employee data in the DB for sufficient funds.

Additionally, the pin code requirement mentioned in the security control for the functional requirement regarding “access to facilities”, will heavily increase the security and privacy of the specified “purchase with microchip” functionality. Since adding extra security measures such as the pin code requirement will reduce the risk of anyone cloning your chip.

Personalization features and requirements

A. *Room temperature/ventilation/air-conditioner/lights settings:* The IoT devices in itself does not constitute a high-level risk or vulnerability to the overall security posture of the system since the communication goes one way, namely from the microchip web service to the IoT device, and not vice versa.

B. *Allergic and food preferences notification:* This feature allows the employee to get notifications if they are about to purchase something that they have opted out as food they wish to congest. i.e. allergies. The risk associated with this feature is that this functionality must be totally secured. One major risk is if somebody with malicious intent modifies an employees’ preferences regarding allergies, this could potentially lead to severe outcomes. Also, it is a risk, if somehow the transmitted information changes along the way from the DB to the web service and then finally to the payment RFID reader. It would cause a disaster if suddenly the information regarding allergies integrity is lost in any way, which could appear quite easy especially if the value for preferences is transmitted and stored as a single boolean value (0 or 1).

    1. *Proposed security controls for B:* Employee information is to be hidden from unauthorized persons and securely stored. The data regarding the preferences and allergies should be defined through larger values so that the error corrections can work properly and missed packages can be retransmitted. The data transmitted to and from, the web service and payment RFID reader should be encrypted. And finally, access to the settings configurations should be restricted and only accessible by the employee.

C. *Seamless access and interactions between different components of the system:* As mentioned in *Chapter 9.1*. the feature of providing automatic personalization is done

by retrieving the preferences and employee info from the database. The microchip web service is then set up and readies the IoT devices and PC to the employee's preferred settings. This is achieved whenever the employee has been authorized to access an office or conference room. The risk pertaining to this feature is if someone else is able to pretend to be the legitimate person, i.e. employee in the company. This could again be done by cloning the information on the microchip. However, the security control regarding the pin code requirement will reduce this risk. However, if the employee forgets their pin code, then it should be possible to reset/retrieve forgotten password through secure means.

D. *Microchip web app, where employees can set up account settings and preferences:* The Risk behind the Microchip web app relies upon the fact that, if a hacker with malicious intent gets access to the employee's microchip preferences setup, then he/she could potentially learn a lot about the employee account, purchase funds and their role in the company. Furthermore, the hacker may able to change and modify settings and preferences such as allergies, etc. which could leave to devastating outcomes.

    1. *Proposed security controls for D:*

        i. The employee has to login in order to be able to access their account,

        ii. The password of the account should be complex and changed regularly,

        iii. 2-factor authentication for every login to enhance account security

9.2 Phase 2: Acquisition - Required Components for Solution

This subchapter will present and describe the second phase of the SDLC. This is where the needed subparts and components, that makes up the entire microchip solution system, are identified and reviewed. These parts have been defined and assessed through research, in order to understand, what it would take to provide the offered requirements.

The SBD security process in Phase 2: Acquisition, is Tender security requirements and Tender security evaluation. These 2 processes underlying activities are: Define Security requirements for Tender which then leads to the evaluation of security specifications. These activities have the aim to ensure that the security requirements for the system components are defined and secured and that known vulnerabilities are identified and reviewed (*Chapter 8*). Finally, these defined security requirements are evaluated, if the components are approved to be used as a

part of the system. The SBD processes and activities output/outcome will be defined and described in a subchapter at the end of each development phase.

9.2.1 Microchip solution components

This section will present the required components of the microchip web solution. The components presented is the microchip implanted in the employee. the second needed component is the database & server required to store and handle the data and information from the microchip web solution. The two final subparts needed are the RFID and IoT enabled devices that are installed at the company and integrated with the microchip system, These are the external/ procured components that enable access control authorization and personalized IoT experiences. These components all have their own security issues, risks, and vulnerabilities, so if it is implemented without security considerations it can become the weak link in the overall security posture of the company, so this means that there must be some security requirements for these components. The security requirements are defined and evaluated in *Chapter 9.2.1*.

The system subparts and components required for the microchip web solution is listed and described below.

9.2.1.1 Microchip implanted in employee

The only real actor in this solution is the employee who is in control of their implanted microchip and the user of it. No employer or other has access, which ensures privacy to the individual employee who has adopted this solution. However, it is important to note that the company must agree to allow such implementation, and review if it is complying with the company security policies, furthermore the integration of the microchip solution and the company is done together with company representatives.

The microchip that is to be used for implant only has to store limited amounts of data, namely the unique user identification tag. this is due to the fact that this solution proposes to store all other employee-related data on a database which is the next component described in this chapter.

9.2.1.2. Database external storage

The solution differs from others by enabling logic and functionality behind the implanted microchip innovations which are, as mentioned, extremely limited in actual data storing and processing, and is merely used for identification in terms of access to the door or other RFID

reader accessible technologies. Therefore, this solution is dependent on storing info in order to provide features such as personalization and notifications (food and allergies).

Another important aspect of DB is the privacy issues that exist when storing personal information, which in this design could range from less critical personal information such as light and other IoT setting preferences to more critical personal information such as employees food preferences based on religious beliefs.

When looking at these extra precautions that need to be made in regards of ensuring a secure and private interaction and adoption, one must keep in mind that the web app and database is made available by the system designer and controlled by the employees, and set up in cooperation with the system designers and the company. In order to ensure that the solutions are tailored and implemented to the company in question, it means that this solution will not be ready out of the box solution.

This is due to the fact that companies have different needs and requirements, which translates to parts of the solution may not equally relevant for all companies and this applies to all parts of the solution.

An example of this can be seen when looking at access control feature. Some companies requires the employees to use Unique ID (UID) smartcard to access the building externally and also access different departments internally, whereas other companies have no authorized access requirements which means that the employee is not restricted to specific departments and can access the company building and freely roam around without having to be authenticated by the UID smartcard.

The proposed solutions security and privacy measurements from the SBD will ensure that the user is able to delete all information and deleted data is never stored. This solution i.e. employee microchip information is stored on a cloud-based database. The pros of using cloud over traditional centralized physically stored DB are numerous, but in this solution, the most particular reasons are the support and maintenance aspects (handled by the cloud provider), fast data transmission (since there usually is more processing power behind the cloud DB), secure DB and the availability aspects of cloud database since the information on cloud databases is backed up on different databases at different locations (Rackspace Support, 2018). It implies, if something happens such as breakdown, loss of information or theft, etc. then the data will still be available, avoiding critical issues that would otherwise prevent the employee's access to the company, disable purchase, delete employee preferences in IoT settings and so on.

9.2.1.3 RFID readers

The next block that is a part or at least enabling the RFID microchip solution is the RFID reader enabled technology components ranging from printers, vending machines, point of sale (POS), PC to company and office door locks. The components in itself do not have to come from a specific manufacturer or model. It can be applied to the overall solution as long as it is compatible with NFC type 2 devices, which leaves room for a variety of RFID enabled technology components to be implemented and all are based on the reality and requirements of the company adopting this solution. The RFID devices will not be provided by the solution but a system designer together with company representatives which would have to agree on what technologies that are already existing and which are relevant and can be applied to the RFID microchip solution. Furthermore, the system designer can propose the RFID device that is lacking and which they should purchase in order to fulfill the companies needs. These components are owned and managed by the company and its employees. These components are then implemented into the RFID microchip solution in order to provide more convenience to the employees since it is arguably easier to swipe your hand to open doors and access printers and make purchases and be completely independent on having to use keys or store numerous cards in a wallet. Additionally, the microchip security and confidentiality aspects of this solution also trump smartcard solutions due to a couple of other factors. This includes the fact that losing an implanted microchip is far less likely than losing a smartcard, and can, therefore, be more trusted, leaving the possibility to remove requested input for pin codes or similar, if needed.

9.2.1.4 Smart IoT devices

Smart IoT devices attached to offices and conference rooms are, similar to the RFID reader enabled technologies, something that can be added on a per company or employee basis, meaning that the system designer together with company representatives will make an assessment of the IoT devices already installed in the company and implement the ones deemed relevant,. Furthermore, the system designer can make proposals to the company regarding the choice of IoT devices, to fully able to embrace the solution. These devices will then be integrated into the web app and database so that the employee can choose their own preferences in the IoT devices attached to the office or conference room that they are in.

The technologies that could be proposed for the microchip web solution is mentioned in *Chapter 9.2.1*.

The reason for allowing the employee to conveniently set up their preferences in regards of the IoT devices is namely to introduce customization and allow the employee to personally set

up the IoT devices in accordance to their preferences. This will arguably provide a more welcoming personal environment at the company, which will hopefully increase the employees overall work morale.

9.2.1 Security-by-design processes in phase 2: tender security requirements and tender security evaluation

The two SBD processes that occur in the second phase of the SLDC are the Tender security requirements and the tender security evaluation. The tender security requirement is where the security requirement for the procured components that are required by the system. The purpose and requirement should be clearly stated so that the tenders are able to provide adequate measures to meet the security requirements that were defined (*Chapter 8.2.1.2*).

The Second process namely the tender security Evaluation is a process that occurs after the tender security requirement has been submitted. The activity of the second process is to assess the security efficacy and the security control specifications proposed by the vendors. This includes an assessment of the security controls, followed by a series of documentation reviews, proposal, evaluation, clarifications and Hardware and software demonstrations (*Chapter 8.2.1.2*).

9.2.1.1 Tender security requirements

The microchip web solution is conceptual, so submissions for security requirements to the tender will not be provided. However, the subparts of the system and its classifications and high-level security requirements are mentioned in *Chapter 9.1.3.2*. Some of these security requirements could be submitted to the tender, e.g. the security requirements for the Microchip.

Below, is a list of general security requirements for the hardware and software that is integrated into the microchip web solution:

1. Hardware and software should have the minimum security controls required by international standards organizations e.g. ISO 2700x standard (CSA Singapore, n.d.).
2. Hardware and software should be resistant against various cyber attacks, such as penetration, etc. and should not negatively impact the overall security posture of the system.
3. The hardware and software should comply with the GDPR, in terms of storing and handling private and classified information.

9.2.1.2 Tender security evaluation

As mentioned above, security requirements to the tender have not been submitted, due to the fact that the proposed solution is conceptual in nature. This means that there is not any proposed hardware or software from the vendors, so no review, proposals, evaluation clarification or demonstrations have or can occur. However, there are procured components used, described and demonstrated in the proof of concept part (*Chapter 10)*. The microchip component used for the proof of concept is relevant and could be used in a real-life scenario. This microchip NTAG216 from xNT is as mentioned in the *State of the Art* (*Chapter 4.1.6*), a near field passive RFID tag, which means that the microchip is not actively transmitting. Furthermore, it is not possible to read the tag info from a distance over 30 cm, leading to security in terms of making cloning of the chip way more difficult.

The RFID tag (NTAG216) is limited in terms of processing and memory meaning that it does not support encryption/decryption. The consequence of this is that the data stored on the chip is in clear text, making it possible for a hacker with malicious intent to perform a man in the middle attack.

A mitigation plan for this could be the previously mentioned security control for pin code requirement.

Another way to solve this could be to use another Microchip solution named VivoKey (*Chapter 4.1.7*). VivoKey is still early in the development phase. The Vivokey solution proposes certification and encryption possibilities in a solution coined as Cryptobiotic identity. Cryptobiotic identity aims at counteracting the security issues with the NTAG216. The proposal to solve these security issues is by having some authority to certify through cryptography and trust that the “vivokey”, is used by the real owner of the microchip. VivoKey is mentioned in *State of the Art* (*Chapter 4.1.7*) and in the interview with the founder of VivoKey (*Chapter 7.2.2*).

9.3 Phase 3: Design/Development - Microchip Web Solution

The first part of this subchapter will present two mockups of the microchip web app and describe its functionalities.

The second part of this subchapter is the Design and modeling of the functional requirements specified earlier in *Chapter 8.1*, The design/development in Phase 3 of the SDLC, is where the specified requirements and accepted components are designed and modeled, to develop the microchip web solution. The Design and development phase is more thoroughly described in *Chapter 9.3.2*.

Third and final part of this subchapter is the SBD security process in development phase 3, which is the critical security design review. The goal of the activities in this process is as mentioned in *Chapter 8.3*, to conduct a security review of the architecture as well as the security controls recommended in *Chapter 9.1.3*.

9.3.1 Microchip web service description and mockup

The employee preferences GUI is a web app, that the employees can use to monitor control and edit microchip related information and preferences for the installed IoT devices. This web app is used to provide personalization to the IoT devices in the company environments such as offices so that the IoT devices are set to the employee's preferred settings. When the system detects an employee with an implanted unique ID, this is applied to settings on everything from PC to IoT devices such as smart light.

Below are a mockup and description of the employee preferences GUI.

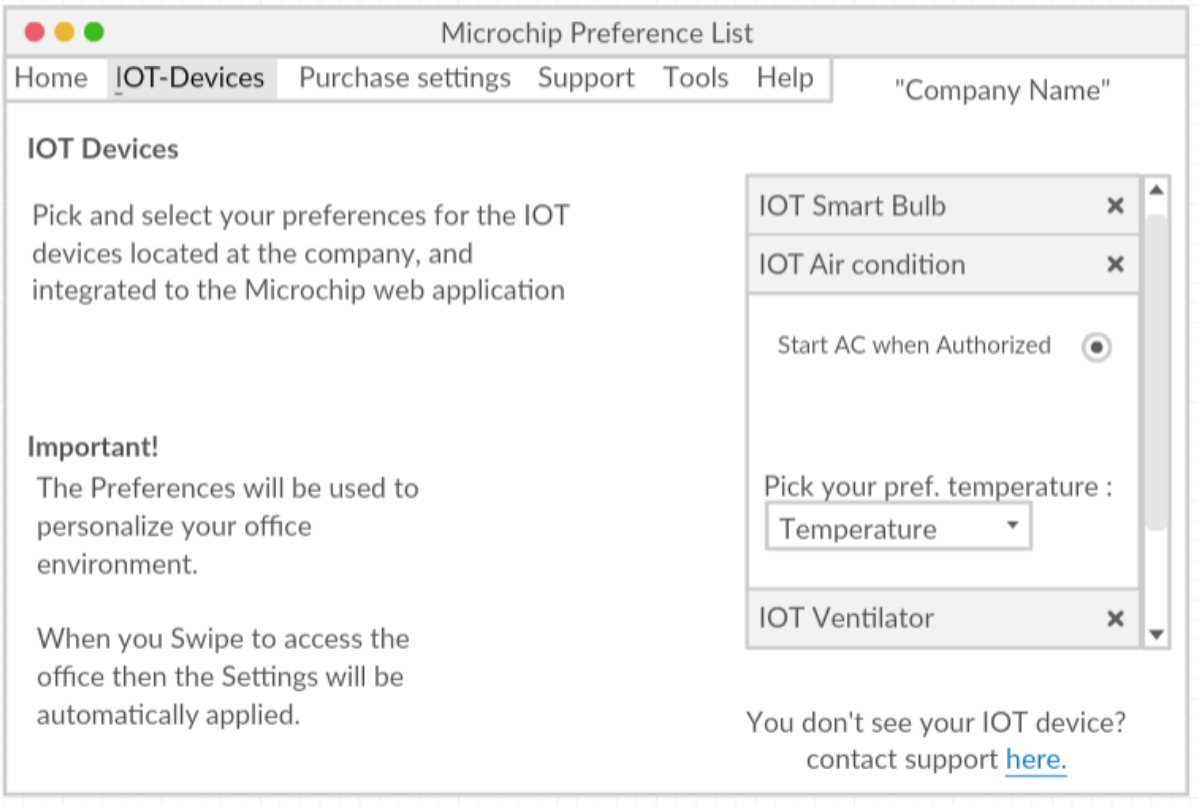

Figure 10.1: Mockup of employee preferences GUI (own figure).

As mentioned preference list is accessible from a web app where the employees can log in to set up and configure their preferences regarding the IoT devices that are integrated into the companies microchip system. The graphical user interface is designed to first and foremost to

be easy to interact with so that it is convenient and easy to navigate around while making it obvious what and where to configure the preferences.

The employee is able to navigate different pages through a menu located on the top of the page first page accessible from the menu is home.

The ‘home’ page is just for welcoming the employee with a presentation of the Microchip service.

The next page accessible from the menu is the “IoT devices” page, where the employee is able to set up and configure their preferences related to the IoT devices. The preferences will be used to personalize the employee's office environment as soon as they have been authorized to access an office or conference room through the microchip. The right side of the mockup presents a list of the IoT devices in the company that is integrated into the microchip web solution and made available to configure for the employee. On the table, one can see the IoT smart bulbs, IoT air conditioner/temperature, and IoT ventilator. These devices are as mentioned all integrated to this particular employee’s company. The employee can choose if these IoT devices should be activated and setup using the authorized employee's preferences. Authorization happens when the employee is granted access to the office via the RFID-enabled door lock, placed in front of the office door, each of these integrated IoT devices can be set to different kinds of values, i.e. IoT air condition have different temperature settings, which will be initiated if the checkbox of start AC with authentication is enabled. The same logic works for the other IoT devices, such as the IoT smart bulb, and IoT ventilator. If the employee cannot see their IoT device or if they want to add more IoT devices into the solution, then they can contact support.

This leaves to the next menu item namely, purchase settings. Here the employee is able to update and setup allergies and define foods to avoid, furthermore the employee is able to view a table with RFID devices that the employee is authorized to access with their implanted microchip.

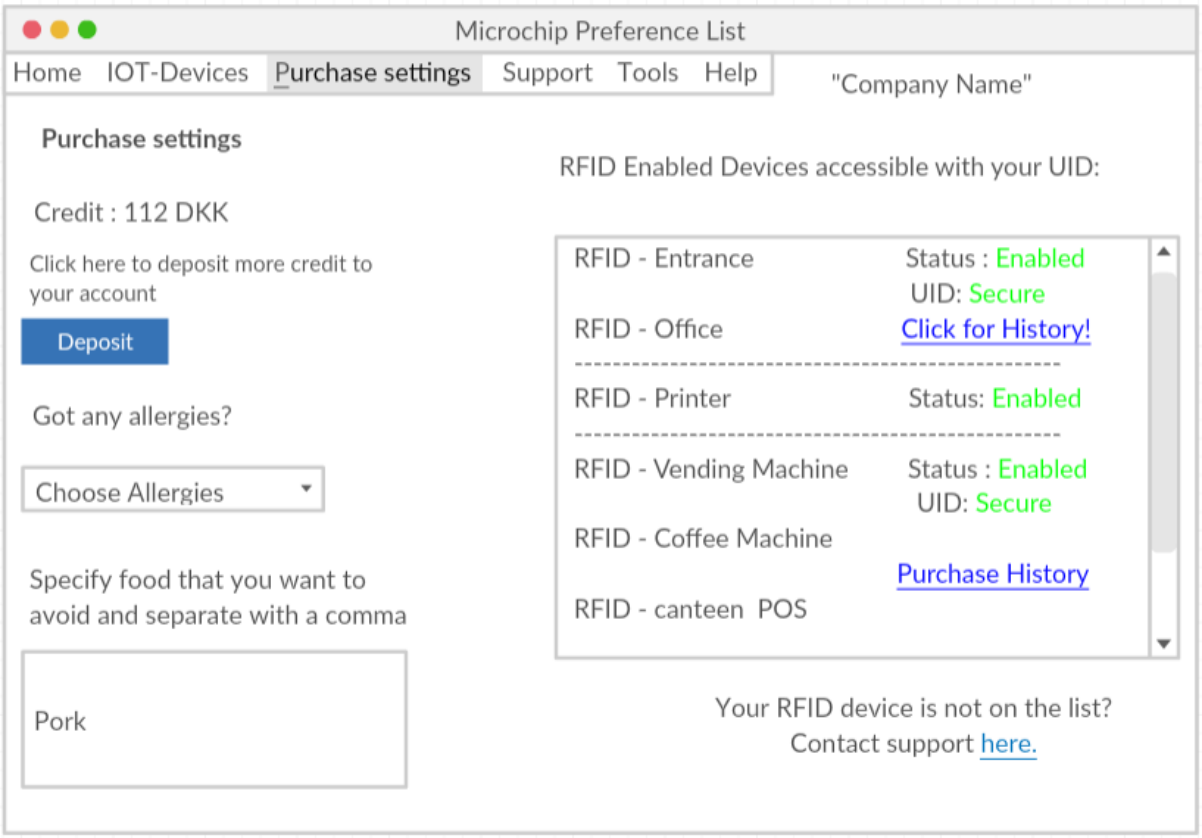

Figure 10.2: Purchase settings mockup (own figure).

The credit amount placed in the top left corner illustrates the employee's total funds. This particular employee has 112 DKK deposited to the microchip purchasing account which allows him/her to purchase goods in the canteen, buy coffee at a coffee machine and snacks and drinks in a vending machine, which can also be seen under our RFID enabled devices accessible from the employees microchip which will be explained in a bit. The next feature namely, choosing to notify the system if the employee has any allergies, so they can be notified whenever they are about to buy something with these allergens likewise if the employee chooses to avoid eating specific foods because of beliefs such as religious. This particular employee wishes to avoid pork. Consequently, the employee who is buying something in the cast canteen will be notified if there are any traces of allergies or any pork, for example.

The employee is able to view a table of the RFID enabled devices that are accessible through the employees microchip, or more precisely it shows the different RFID devices and identifiers, together with status and a function to check history, where the employee can view their history of interactions with different entrances and office/conference rooms. UID secure simply means that the employee microchip information is authorized and validated with encrypted data from the database. The employee is also able to look at their purchasing history.

The employee can always contact support If they encounter that an RFID enabled device is not on the list or for some reason the devices are disabled. This can be accessed from the next page, namely, the support page. The employee can find contact information if they need assistance in the GUI, help in maintaining and setup of devices, etc.

The final Page accessible from the menu is the ‘help’ page, where the employee can get documentation and information on how to to use and navigate in the microchip GUI.

9.3.2 UML diagrams

This subchapter will model, graphically visualize and document the specified requirements by conceptualizing the behavior and relationship of the artifacts that make up the microchipping system, which will be done using the standard UML (Unified Modeling Language).

The aim of using this standard is to identify and describe the different requirements enabling objects responsibilities in the system design (Ceta, 2018). When using UML one has to use a gradual process which means that the design is conceptualized in stages starting from context diagram and use cases, which is followed by sequence diagrams and activity/flowcharts (Ceta, 2018). In UML there are a number of different diagrams and structures and each specifies their own purposes. The one singled out for this conceptual design is not only adequate in terms of modeling the behavior of the system subparts but also great in terms of being extremely read friendly, easy to understand for developers and also other persons with interest, even if they are not IT or software system designers (Ceta, 2018).

9.3.2.1 Use case scenarios

The next section will provide three scenarios of use cases for the microchip system conceptual design. The scenarios take place in a company where the microchips IoT and RFID personalization solutions have been implemented. The Web app requires a login to the company subscription account and must have been invited by the company representative (admin) in order to receive access to the services.

Adding preferences in the microchip web app

The employee selects their preferences in employee preferences list presented as a GUI. The employees can access this by signing in via a web app accessible through the web browser as can be seen in mock-up of the GUI (*Chapter 9.3.1)*. It is also possible to pick and select preferences for IoT devices that are integrated into the company. The employee can choose the IoT device and select whether they wish to have this initiated when the microchip system has detected the employee when granted access to the office or conference room through the RFID reader. So let us assume that, one day, an employee wish to set up their preferences

for personalization. He accesses a PC with internet connection and logs into the microchip system home page. He updates different settings and preferences of the connected IT device and purchase settings. When pressed OK on satisfaction and closes the browser. The information is then updated in the Database for that employee. Next time when he swiped his hand outside the office door, the new settings for the IoT devices would be initiated to the preferred settings.

Purchase in the canteen and vending machine with microchip

This next scenario is about an employee who has put up funds to purchase via his implanted microchip. In addition, this employee is allergic to nuts. The deposit of funds and allergy notifications was applied and set up in the employee preference list as presented in the previous discussion. So, now the employee is at the company canteen to buy some food. He picks up a chocolate bar but can't really see if there are any nuts in it. He takes the chance and went to the cashier and swipe his hand at the RFID payment module, in order to pay. This prompts a notification dialog with ‘cancel’ or ‘continue’ options on the screen, warning that there are nuts in the chocolate bar. The employee then chooses to cancel the purchase. The same scenario could be applied to the vending machines.

Authorized access to a locked door in office or conference room that will initiate personalization

The next scenario which also encompasses the functions and applications of the microchip system solution is when an employee gets access to the office or conference room via implanted microchip. It will then automatically, without any other interaction from the employee, initiate the employee preferences regarding the devices integrated into the microchip solution. So, in this scenario, the employee has set up some preferences in the preference list graphical user interface and then stored at the database for later reference. Then one day, he is at the company premises and is about to access an office room. He swipes his hand at the reader which is placed next to the door. The reader identifies the employee and then sends a request for their preferences that is specific for that authorized employee. Employee barely opens the door before all the devices grouped to that office is starting up to exactly what the employee wants. So when the employee moved towards his desk, he can see that the PC is automatically logging in to his personal account. The air condition and light are set to his preferred temperature and dimness which consequently leads to the employee getting the sense of feeling enjoyment, comfort, and familiarity.

9.3.2.2 Context diagram

The different subparts of the system are modeled in a context diagram which is identified and introduced by different blocks. *Figure 10.3* below presents a diagram that predates UML but has been added to the UML standard, defined as a use case diagram type, which in UML is known as a top-level use case diagram (Ceta, 2018). The reason for beginning the modeling with a context diagram is that it helps summarise the interaction of actors within the system and displays the system of interest and all its factors. The context diagram hides the use cases themselves that provide an additional tool for better understanding and designing the use case diagram which will come after the context diagram. The microchip system can be seen in the middle square box of the diagram and surrounding them are all the external factors such as actors, external databases and so on. The arrows that connect them represents the relationship and the specific interaction is described in the text field above the arrows.

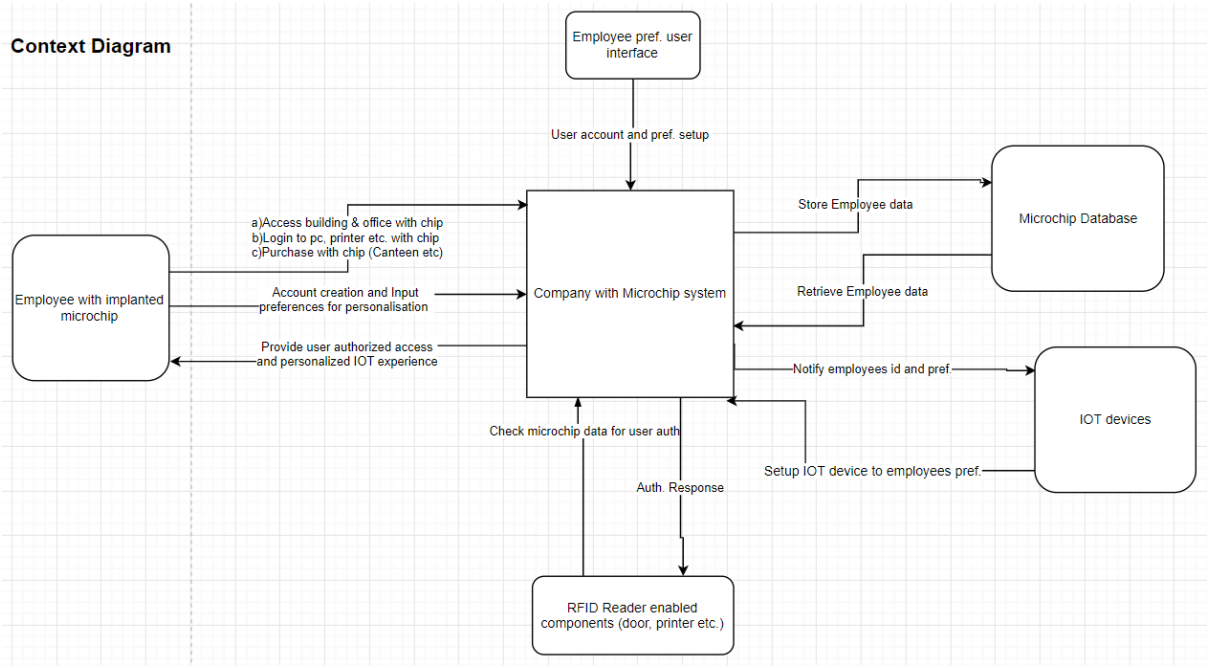

Figure 10.3: Context diagram for the system (own figure).

As mentioned, the middle square box on the diagram above represents the microchip system.

Microchip system consists of the employee preference web application which connects all the subparts of the system.

On the left from the center, namely, the employee with an implanted microchip is able to access building and offices with the chip. Furthermore, they can log in to PC, printer and other RFID-enabled devices with the implanted microchip. The chip also allows the employee to purchase at the canteen or vending machines etc. In addition, the employees can also create

an account and input preferences for personalization of the IoT devices that are attached to the office environment which in turn enables a personalized IoT experience.

On the rectangle on the bottom diagram, the RFID reader enabled component like a printer, etc which are a part of the company adopting this solution are shown. However, the microchip system basically functions as an interface between the employee and the RFID and IoT components. Through the communication between RFID reader enabled components and the implanted microchip, the reader can essentially check the microchip data it receives from the implanted microchip and checks for authorization. The system then provides an authorization response.

The next Square to the right from the center is the IoT devices which are attached to the office environment. Here, the microchip system can start and initiate the IoT devices to the preferred settings selected by the employee on the employee pref list in the web app.

And the final Square is the microchip database which is used to store all microchip related information such as i.e. the employee's user ID and their preferences etc.

This is an external DB that is set up to communicate with the microchip system web App. It is by design that most of the subsystems are external entities and the results in the proposed solution. It is considered as a loosely coupled solution that makes way and room for adding and upgrading pretty much all the subparts including the microchip, the DB, the IoT devices and so on which makes it a dynamic and flexible solution that has the architecture to withstand and adapt to changes in innovation, standard and technologies in the future.

9.3.2.3 Use case diagram

The next diagram is the use case diagram which is used to model the dynamic behavior of the system. Dynamic behavior refers to the behavior of the system when it is in operation (Ceta, 2018).

So far the requirements have been established identified and described.

The use case diagrams are used to gather the requirements of the system including its internal and external influencers (Ceta, 2018), this means that the functionalities of the system are gathered through use cases and the actors (which in this case is the employee who has an implanted microchip).

Additionally, the use case diagram explains the actor's different interactions with the system and its functionalities (Ceta, 2018), so the functional requirements are captured inside the use case diagram to provide an understanding of the microchip solution.

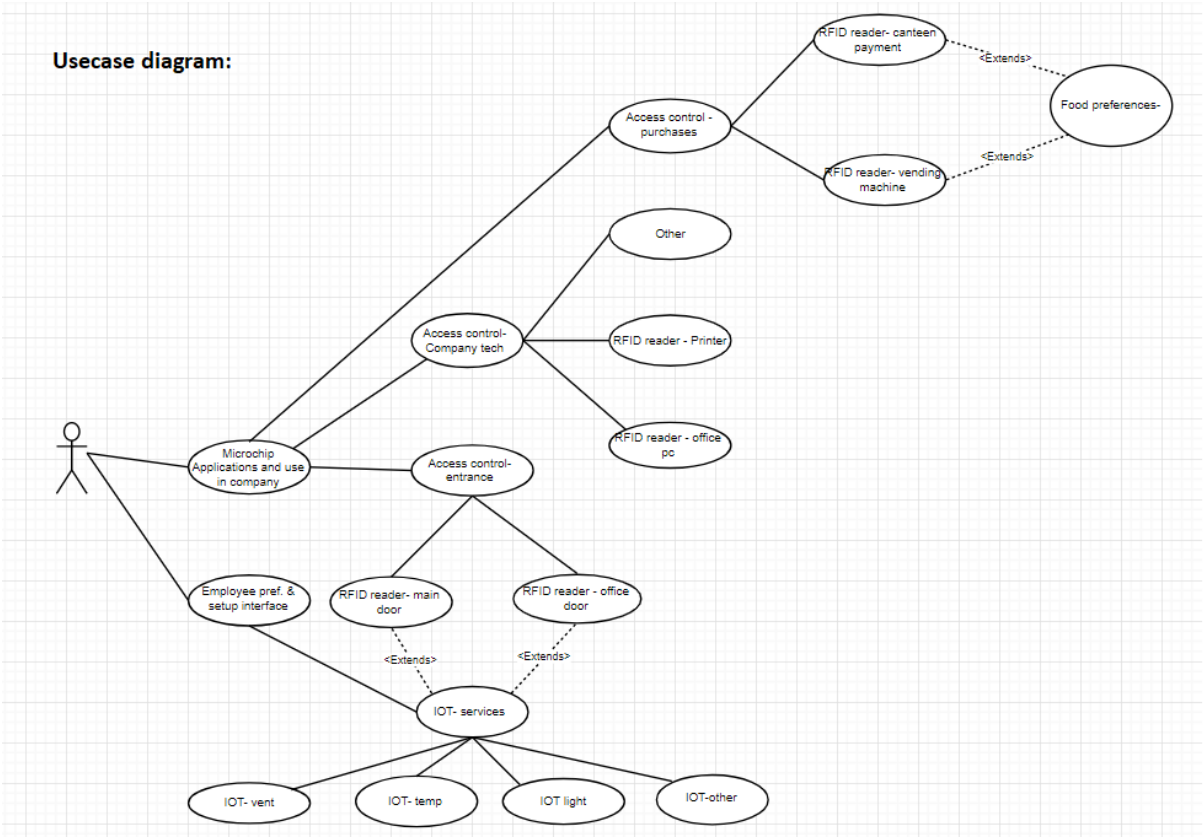

Figure 10.4: Use case diagram for the system (own figure).

The use case diagram shown above depicts the actor on the left which is the employee with the implanted microchip.

The actor is connected to two main types of interaction. The microchip application and uses in the company. The usage as shown in *Figure 10.14* may be purchases through the microchip which also extends its functionality to the food preferences notification that will appear if the employee is about to buy something that they are allergic to or something that they won't eat because of religious beliefs. These preferences are set up in the employee preference web app.

The next area is the accessing of RFID enabled tech devices in the company which means, it will be possible to access and interact with various RFID-enabled technology devices such as RFID readers printers, the PC in the office, etc. More RFID reader enabled devices can be added as long as they are compatible with NFC type 2 (*Chapter 4.1.6*) which are mentioned in *State of the Art*. The final entity is authorized access to entrances through the microchip which generally refers to accessing the main door as well as accessing the offices and conference rooms as mentioned before. Role-based authorized access permission can be applied in companies where there are restricted areas where only certain employees have

access. These two entities extend the IoT services to the next step on the use case diagram, which is employee preference extends and setup.

As mentioned before, the employee can define their preferences for the IoT devices attached to the office environment such as achieving personalized conditions through pre-selected setup of devices such as temperature, light, etc. This will be initiated when the system detects that an employee has accessed the office/conference room. IoT devices can vary and new ones can be added as long as they have access to the internet.

9.3.2.4 Sequence diagrams

It defines the sequence of action taking place when interacting with this solution.

Figure 10.5 below depicts a sequence diagram which shows the interactive behavior of the microchip system and its subparts in sequential order, meaning that, it describes how and in what order the objects in a system functions. Before that, an actor is required in the role of the employee with an implanted microchip followed by the actor's interaction with other parallel lifelines of the objects in the system.

The reason for applying sequence diagrams to capture the requirements is due to the fact that it is a popular dynamic diagram that specifically focuses on lifelines also known as the processes and objects that live simultaneously together with the messages exchanged between them to perform a function before the lifeline ends (Ceta, 2018). This can subsequently provide great insight into the microchip system and its functions. There are three sequence diagrams that are needed for fully understanding the interaction behavior of the use cases scenarios.

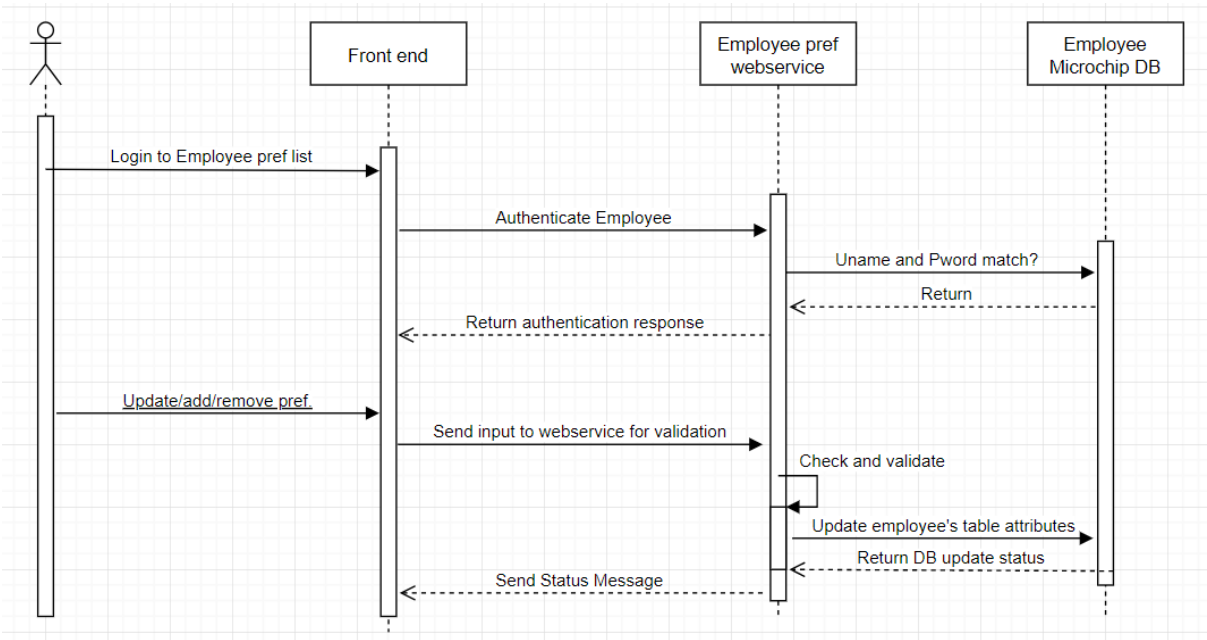

Figure 10.5: Sequence diagram for the first use case scenario (own figure).

The figure above (*Figure 10.5*) is a sequence diagram of the first use case scenario when the employee logs into the user preference web service and add personalization preferences. Looking at the diagram, one can see that there are four Lifelines running in parallel, the first one being the actor with the embedded microchip and the second one is the front end of the web service, the third one is the employee preference web service and the final one is the employee microchip DB. When the employee wishes to access the web app, then he or she needs to sign into the employee preferences list. The information will then be sent from the employee microchip web service to the database in order to see if the username and password exists and matches. So, the sequence above is the actor login to the preference list, then this information is transmitted to the web solution in order to be authenticated. The web service lookup the database in order to check the username and password. If it matches, it returns to response and if there is a match the user is logged in from where they can update it and remove preferences. The preferences when they do this input is sent to the web service validation. This means that it validated if it has been filled out correctly or if there are missing any important attributes and configurations. Development check is therefore useful in terms of making sure that the right information is stored in the database, which will hopefully prevent issues with the services later on. The database will return update status after the employee microchip database has updated the employees pref and setting. The web service then sends a message notification to the front end notifying that the information has been successfully updated or not.

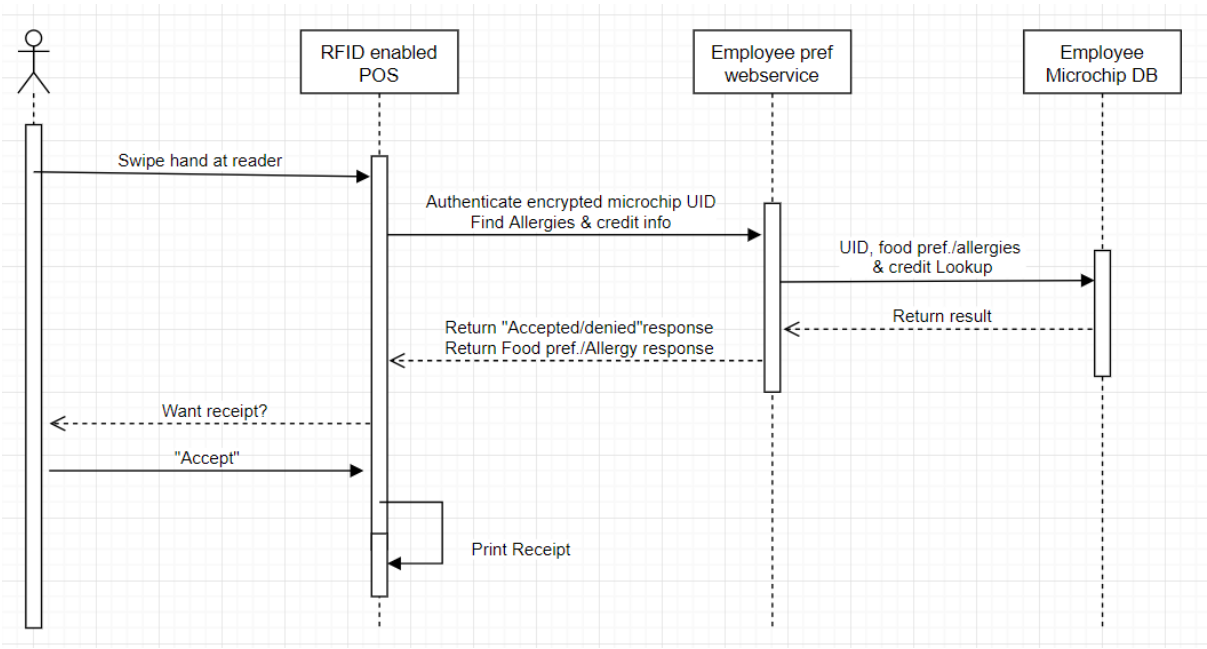

Figure 10.6: Sequence diagram for the second use case scenario (own figure).

This leads to the sequence diagram above, namely the use case scenario number 2 where the employee is able to purchase foods and snacks at the company's canteen or a vending machine located in the company through their implanted microchip. In *Figure 10.6*, one can see the lifeline of 4 entities, the first one being the actor, which in this case is the employee with the implanted microchip. The second one is there RFID-enabled point-of-sale (POS) device which is the device that receives payments, the third one is the employee microchip web service and the fourth one is the employee microchip database. So, here again, we have the employee who has bought something and now wishes to pay for it with his implanted microchip. So, he swipes his hand at the reader, the reader reads the user ID together with their credit info, as well as sales and item info from the purchased goods. This is then forwarded to the web service. The web server looks up the user ID in the Employee Database together with checking for sufficient funds in the credit status. The final request from the web service to the database is info regarding food pref. and allergies. The database then Returns the results to the web service which then process the information, meaning that it's checking the info retrieved from the database and compares it with the cost from the POS, to check if the employee can afford the food/snack. This response is then returned to the POS either accepted or denied. Similarly, the web service checks if the food is labeled with any particular allergens i.e. nuts and then compares it to the info received from the employee's Database. The web service will then return a notification if the employee has bought anything that they are allergic to or because of beliefs. Finally, the POS offers the employee a receipt, which the employee can choose to accept or deny. Consequently, the POS will print a Receipt if the employee accepts.

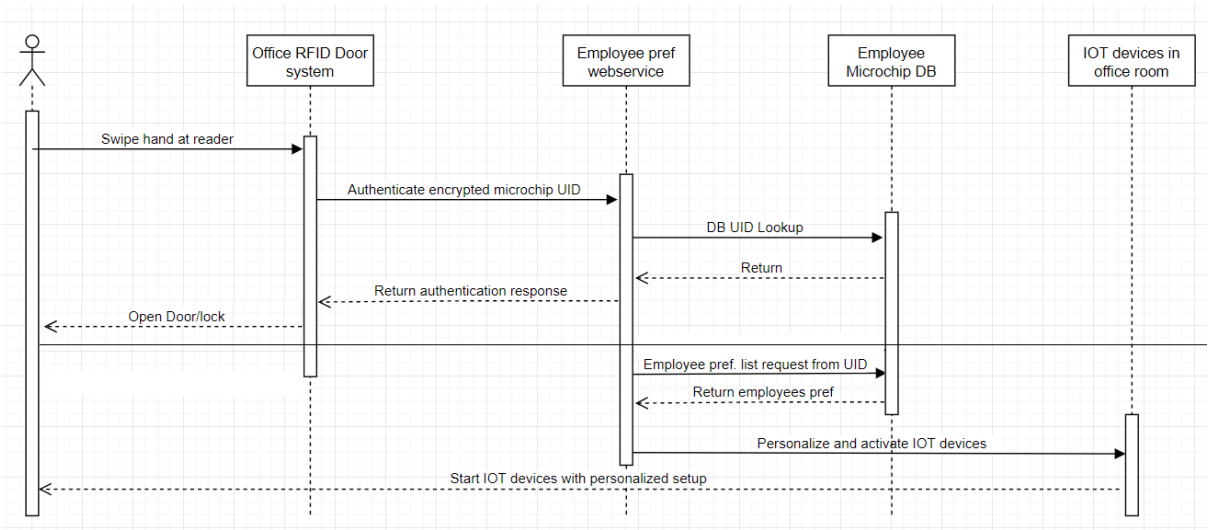

Figure 10.7: Sequence diagram for the third use case scenario (own figure).

Figure 10.7 describes the sequence of the use case number 3 which is when the employee implanted with a microchip, swipes his hand at the RFID enabled door lock in order to access

an office or conference room that is completely personalized in total accordance to the employees stated preferences (in terms of how they wish their IoT devices to be set up, etc).

This diagram has 5 entities each with their own Lifeline running parallel to each other. First, the employee swipes their hand at the reader on the office RFID door system which then reads the microchips unique identification tag, and forwards it to the web service. The web service then makes a database lookup and check whether the employee has authorization, the result is then returned. If the employee is authorized to access and enter the office room, the door will open.

Simultaneously, the web service receives the employee's preferences list from the employee microchip database. The web service then finally sends out calls to the IoT devices, which will set up the devices in accordance to the employee's wishes, meaning that the temperature, lights, PCs, etc. will be personalized to the employee.

9.3.2.5 Flowchart diagrams

The final UML diagram used for capturing the requirements and functionalities and their relations and interactions with the actors is the flowchart diagram more commonly referred to as an activity diagram, which describes what must happen in the system and provides clarity and brevity by demonstrating the logic in the system (Lucidchart, n.d.). This is done by identifying and describing the use case section and then describe the steps performed in order to illustrate the process of workflow between the actors and the system. The activity diagram is made up of actions which are presented as an activity in the microchip system. Each entity behind the actions performs a given task.

The next part of the activity diagram is the decision node that is represented by a diamond. It includes a single input and two or more outputs. This could for instance in the case of the microchip system while checking if a user is authorized. Here, the outputs are represented as yes or no, more of this is discussed under the figure below (*Figure 10.8*).

The next part of the activity diagram is the ‘control flows’. These are the connectors that show the flow between the steps in the diagram parts of an activity diagram (Lucidchart, n.d.).

Start node and end node represents where the activity starts and where the activity ends.

The figure below (*Figure 10.8)* depicts three activity/flow diagrams. One for each of the three use case scenarios mentioned in use cases, namely how to change, add, remove, etc in the employee web service, access office with the microchip which initiates setup and start of IoT devices in the office/conference room. The final diagram is where the employee can use their implanted chip to purchase food in the company canteen or vending machine, and then

receive a notification if the employee is about to buy something that they are allergic to or not eating due to religious beliefs. These Use cases are more thoroughly described in the use case scenario section (*Chapter 9.3.2.3*).

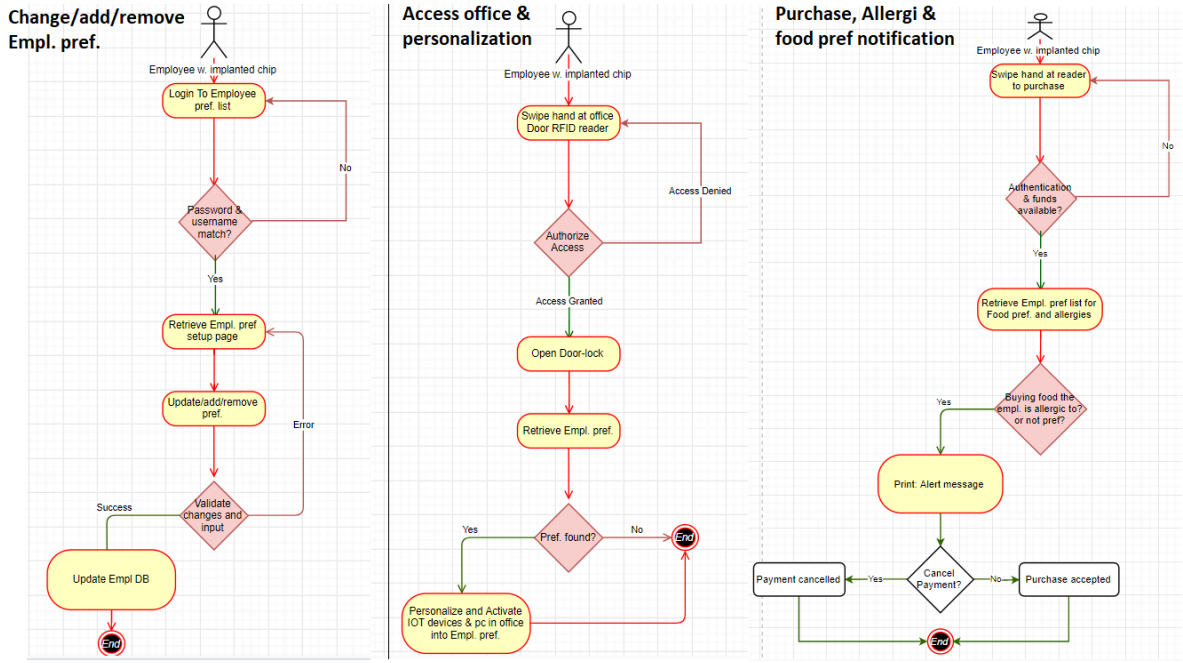

Figure 10.8: Flowchart diagrams for each of the three use case scenarios (own figure).

Farthest to the left of *Figure 10.8*, represents the flow of the first use case mentioned before. We have the employee with an implanted chip who sign in to the employee microchip web service and initiate a decision note (representing the decision made by the web service) to check if the password and username matches. If not, the employee will be returned back to the login and if yes, they will retrieve the employee preference setup page where they can update add and remove preferences. This is done and accepted by the employee.

Next is a decision note that validates and updates employee input. If it returns an error, then it will go back to the setup page with error description and input suggestions. If it is successfully validated with no errors, then the database will be updated and the activity ends.

In the flow diagram; access office and personalization (use case in the middle), the employee with an implanted chip at the start of the activity swipes his hand at the RFID reader enabled door lock in front of the office.

The information that the reader reads from the microchip is checked and validated for authorization. If access denied, then obviously the employee has to swipe again, if access is granted, the door will open and the web service will lookup the employee's preferences from the DB. If preferences are not found, then the lifeline ends. However, the web service will

personalize and activate the IoT devices and PC in the office if the employee has configured the preferences in the web service GUI and from here the activity ends.

The diagram located farthest to the right of the figure (*Figure 10.8)* depicts the flow; purchase allergy and food preference notification use case. Here, the employee with the implanted chip is again at the start of the activity.

The employee swipes their hand at the reader in order to purchase some food in the canteen or vending machine. The web service receives the information from the reader and compares it to the database to look for authentication and if there are funds available to make the purchase. If the answer to this is no, then the purchase will be declined and they can try again.

However, if the employee is authenticated and there are enough funds available, then the web service will retrieve the identified employees preference list for food preferences and allergies. This is to determine if the employee is buying food which the employee is allergic to or not eating because of religious beliefs.

If the employee is not allergic to the food purchased then the activity ends and the purchase is accepted. If the web service discovers that the food has an ingredient that the employee is allergic to or it contains foods that are against their religious beliefs, then the employee will be met with a dialog message on the POS alerting the employee of the purchase. This will be followed by a decision where the customer can accept or cancel the purchase. Either decision will end the activity.

9.3.3 Conceptual solution overview

This subchapter will introduce and present an overview of the microchip web solution. The solution overview is created on the basis of the functional and security requirements that are specified in *Chapter 9.2*. The solution overview is presented in a 3D floor design of a fictional company. The company used for illustration is inspired by work environments encountered by the team behind this project as well as Aalborg University campus in Copenhagen, Denmark. The architectural design has been developed with a license-free software called SketchUp.

It allows the designer to make scaled versions of buildings such as companies. Furthermore, it is possible to add multiple components such as tables, chairs, computers, plants and also possible to add own components, etc. All these made it possible to create a realistic 3D version of the inside view of a company that has adopted the Microchip web solution. This software has proven very valuable and crucial for visualizing the conceptual solution. The following sketches demonstrate and depict the solution in a simulated company environment.

9.3.3.1 Company overview

The first sketch depicts the top overview of the company premises. It consists of three main building departments. First one is the main hall followed by the left wing and the right wing as shown in the figure below (*Figure 10.9)*. These three buildings are connected via a ‘bridge’ (as can be seen in the middle of *the figure*).

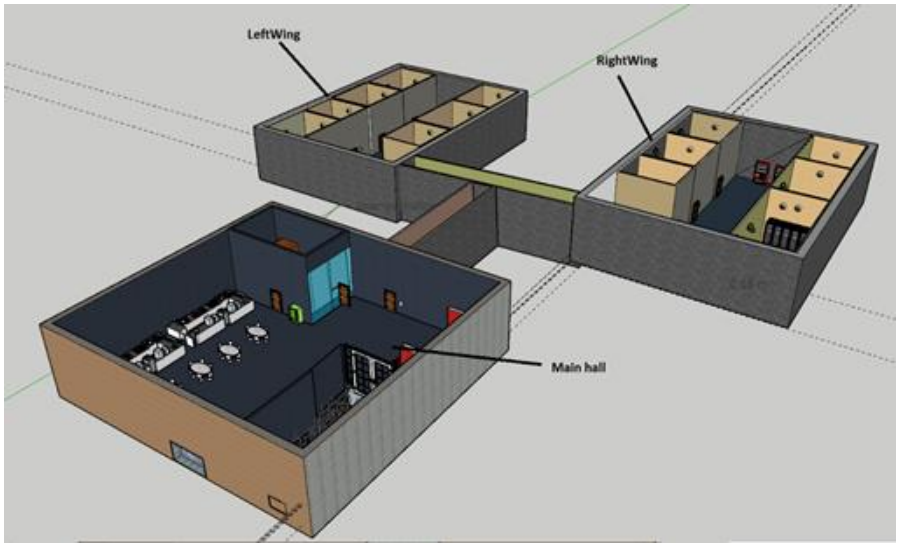

Figure 10.9: Overview of the company premises and departments (own figure).

The following images will look more into the inside contents of the company building that has adopted this solution.

9.3.3.2 Overview of the main hall

This screenshot (*Figure 10.10*) provides a closer view of the main hall. Here, there is an open room concept with a reception, canteen, and two open offices. Additionally, there are two rooms, one is the printing room and the other one is a conference room. To access the conference room and make a booking, the employee only needs to swipe his or her hand at the RFID reader which will set up the environment to the employee’s preferred settings as mentioned before. To configure the employee preferences, interfaces like the computer screen assist in login to the employee's account, while at the other desk it would be possible for another employee to login in a similar way. Similarly, the two hall office that is depicted on the screenshot as hall office 1 and hall office 2 has an RFID reader at the computer desk which employees can use for login.

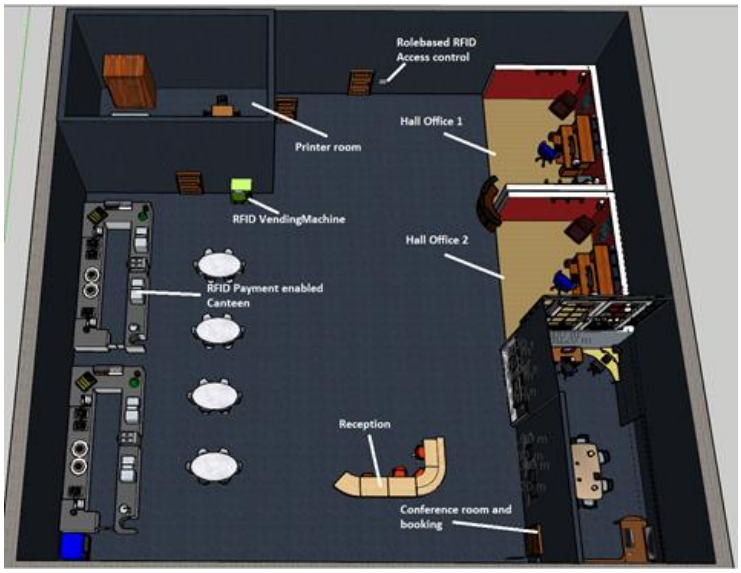

Figure 10.10: Overview of the main hall (own figure).

9.3.3.3 Printer room

The screenshot below (*Figure 10.11)* depicts the printer room seen from the top. Here, a printer is shown with an attached RFID reader. So, when the employee waves their hand at the RFID reader, then it will access the employee's account. This enables the employee the possibility to print followed printing jobs, log and prevent; if there are printing limitations, etc. This goes back to the previously mentioned feature where the employee now does not have to write in username and passwords on a small and not so user-friendly interface.

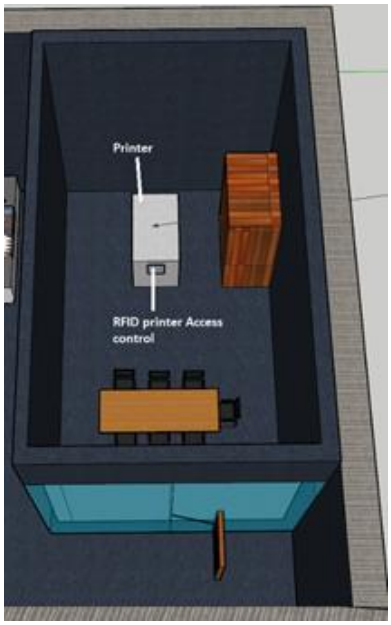

Figure 10.11: Printer room (own figure).

9.3.3.4 Canteen

Figure 10.12 depicts the overview of the canteen, where it is possible to purchase goods, drinks, and foods while being able to pay by swiping the hand implanted with a microchip at the RFID reader. An RFID-enabled vending machine can also be seen on screenshot where the employer is similarly able to pay with their microchip. The personalization aspect here is regarding the food and allergies notification which as mentioned is possible to specify in the employee preferences in form of notifications on a dialogue box in the POS screen, and/or on the receipt.

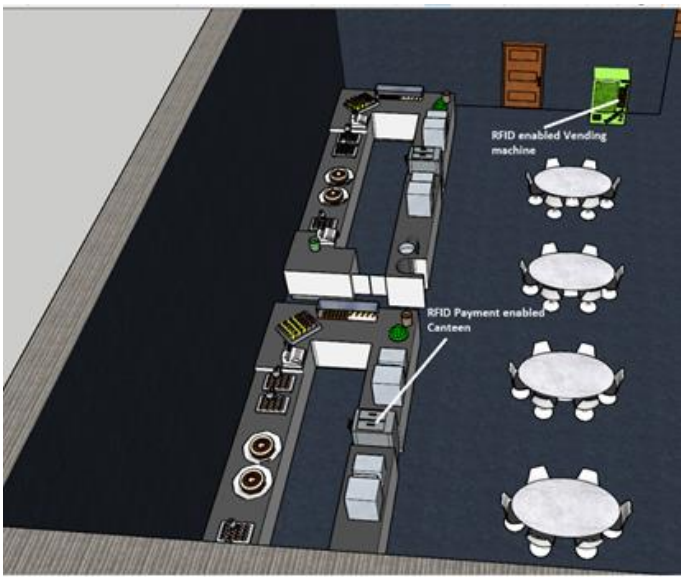

Figure 10.12: Company canteen (own figure).

9.3.3.5 Left and right wings

The next screenshot (*Figure 10.13)* shows the top view of the left and right wing. The employees can access different wings by having the right access/user-role.

When looking at the left and right wing from above, one can see that the buildings are divided into different rooms, which again consists of multiple offices, conference rooms, and maintenance room. The employee can also access the vending machine. In order for the employee to get access to their office, they have to swipe the hand with the chip at the reader. It triggers the setup and pre-configure the IoT device settings so that it matches the employee's preferences in the user preferences interface. This initialization can also be configured to be activated at different times, i.e. when the employee enters the company building, bridge or wing department.

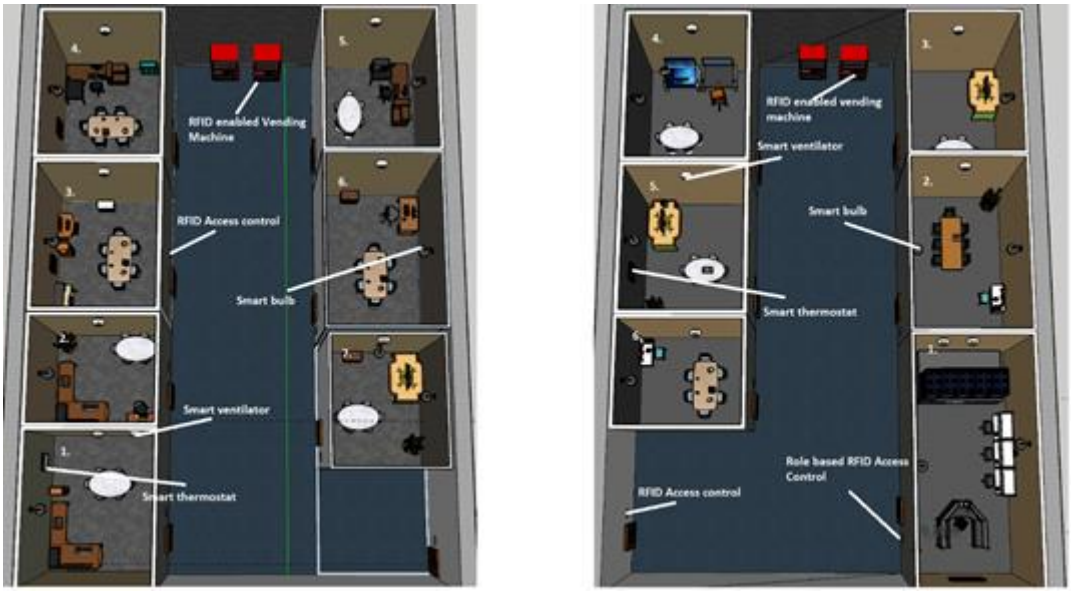

Figure 10.13: Left and right wings (own figure).

9.3.3.6 Office closeup

A closer look at one of the offices located at the left wing can be seen on the screenshot below (*Figure 10.14)*. This screenshot will give an overview of the functionality of the RFID solution together with the IoT devices inside one of these offices.

Figure 10.14 shows typical office appliances that one would expect in an office. When looking at the screenshot, one can see some white text on an outline. These are the components that are a part of this RFID solution which can be interacted through the microchip implanted in the employee's hand. The RFID access Authenticator is used to identify the employee and grant access to the office. If the employee is authorized to enter, then the door will unlock and the employee can enter the office. The smart ventilator, smart bulb, and smart thermostat will function as personalized to the employee's preferences. The employee can always change the settings according to their choice.

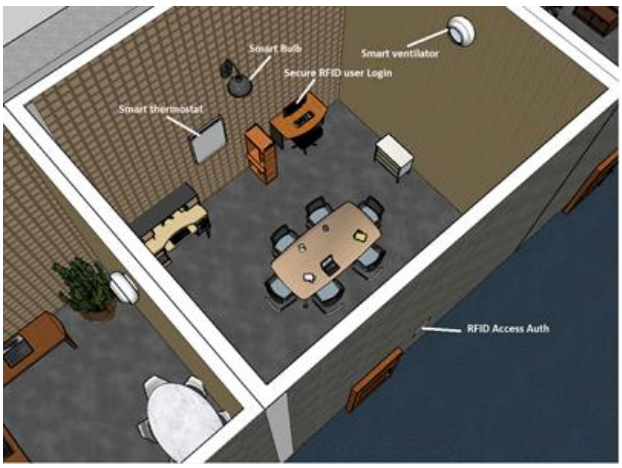

Figure 10.14: Office closeup (own figure).

9.3.3.7 Maintenance room

Below is a depiction of a maintenance room (*Figure 10.15)*. This is depicted to demonstrate the functional and security requirement regarding role-based access authorization (*Chapter 8.2*).

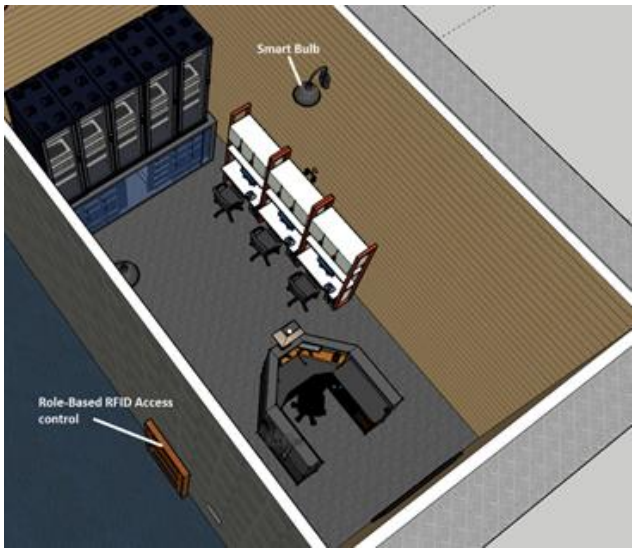

Figure 10.15: Maintenance room and role-based access (own figure).

The screenshot above depicts the maintenance room where only employees with clearance can enter. This is to specify that, each employee have the same fundamental access right to the main building but inside the main building, there exists different roles and permissions applied to different employees granting them different access. Since the solution in this thesis can differentiate access between employees and different user roles and thus it makes it a secure system.

9.3.4 Security-by-design process in phase 3: critical security design review

The SBD process of critical security design review is conducted in the SDLC phase 3 Design/implementation, which is conducted after the functional requirements have been approved and the tender has been awarded. As mentioned in *Chapter 8.1*, the critical security design review is applied in order to ensure that the system architecture is secured and that appropriate security controls are put in place in the design of the system. This result in that the security requirements are met throughout the system design (*Chapter 8.2*).

There are two activities in the critical security design review, namely review of the security architecture and the security control, that was specified in *Chapter 9.1*. The review of security architecture focuses on the security architecture of the system. Here, the system is decomposed into components and its inner workings in order to identify the data flow information entry and exit points (*Chapter 8.2*), this includes reviewing the system design proposed in *Chapter 9.2*. These reviews are conducted to make updated design vulnerability assessments and if needed provide extra security recommendations. The expected output is an approved security architecture, meaning that it is approved for the next implementation phase (*Chapter 8.2*).

The second activity in SBD process of phase 3: Review security controls, is concerned with reviewing the security controls that were put in place as part of the system design, this is done through a series of documentation, assessment of its effectiveness and its recommendations. This means that the proposed security controls must be justified and documented on the basis of the TRA and security requirements that were introduced in *Chapter 9.1.3*.

9.3.4.1 Review security architecture

The system design has been developed together with functionalities and a proposal for security requirements. The subparts of the system together with its inner working has been specified, modeled and designed. The task is now to determine and assess if the security requirements and controls are congruent with the overall functional requirements.

When reviewing the conceptual design of the Microchip web solution, it becomes apparent that, the usual risks and vulnerabilities that are associated with distributed systems in general. These are the risk that is related to vulnerabilities that exist in for e.g. the web app and its associated services. The architecture and dataflow of the solution are compatible with robust security measures such as cryptography and strict access control. The overall architecture is as mentioned in *Chapter 9.2*. distributed through a client-server system with the web app and its underlying services in the center. With this web app, people can log in and set up their account and preferences which is then transmitted and stored on a DB. Furthermore, the RFID enabled IoT devices are then integrated into the microchip web solution. The security controls were put in place in *Chapter 9.1.3* to mitigate the security risk and vulnerabilities that were identified in the system design.

9.3.4.2 Review security controls

The security controls that have been implemented into the system design, will be reviewed, by matching the security controls against the security requirements that were approved in

Chapter 9.1.3. These security controls are then checked for effectiveness in adequately mitigating the security risks.

Access control features

Authorized access to the facility, Role-based access within the facility, Authorized and personal access to IT equipment, seamless communication between integrated devices

Security controls and review: The Security control proposed here, was to only allow a 7 byte unique ID (UID), to be stored on the microchip. This is to prevent the private information that can be read from the chip by a malicious hacker. This control will protect the employees privacy, however, since the UID is stored in plain text means that this UID can be intercepted, spoofed and cloned.

This leads to the next Security control proposed for authorized access control, namely to, implement a process that requires a pin code for final authorization. So, access is not granted to a malicious hacker who succeeds in cloning the UID, he would need to know the 4 digit pin code. So, when the employee scans his/her chip at the reader, then the RFID reader device will prompt the user to insert a 4 digit pin. The RFID enabled access control device will then match the inserted pin against the pin stored in DB and linked to the UID. Here, it is necessary to encrypt the communication between the RFID device, web service, and DB. This is to be fully protected against malicious attacks such as man in the middle. The consequence of this control is that the RFID enabled devices provided in the system needs to have sufficient memory and processing power in order to conduct cryptographic computing.

Enable purchases using microchips

The feature of enabling purchases via microchip inherent different obvious issues such as the fact that, using the same UID for a payment service such as credit card, is difficult to implement since there will be a need for implementing specific software from the payment service providers into the system.

Security controls and review: The Security control for mitigating the above-mentioned issue, is to make an attribute in the employee table. This attribute consists of the value of deposited funds. This value is populated by making a payment to the microchip service, through e.g. wired transaction, credit card payment, mobile pay, etc. (*Chapter 9.1.3*)

The amount that is deposited to the account is registered and can be viewed in the microchip web app (*Chapter 9.3.1*). This security control prevents that employees can make purchases through their microchip, without direct influence from the employee's credit card. Here, it is necessary that the employee deposits are made in a secure outside channel. Furthermore,

the integrity and confidentiality of the stored employee information must have strict access control with only the administrator having access to the database. This is is in order to ensure that, e.g. the funds attribute in the employee table/database, is protected against modifications of data.

Microchip web app, Allergic and food preferences notification, Room temperature/ventilation/air-conditioner/lights settings

The functional and security requirements related to the web app and preferences are described in *Chapter 9.1.3*.

Security controls and review: The security controls that were proposed to meet the security requirements are as follows.

A. The employee has to login in order to be able to access their account.
B. The password of the account should be complex and changed regularly.
C. 2-factor authentication for every login to enhance account security.
D. Employee information e.g. allergies is to be secured from unauthorized access.

These proposed security controls ensure that unauthorized access to the employees are prevented by required sign in, complex password and two-factor authentication for login. This ensures that the web app is not an unprotected point of entry and that the settings and preferences will not be modified by a user with malicious intent. E.g. the allergies information has high health risk implications and therefore it should at least be encrypted. This is in order to prevent that the allergies information is accessible to a malicious hacker.

9.4 Subconclusion

This chapter proposed a microchip web solution for employees in a company. The development of the conceptual solution was documented and divided into 3 segments, namely Initiation, Acquisition and Design/development. The Initiation phase defined and specified the functional requirements of the solution. This was then followed by a presentation of subcomponents that needed to be acquired as a part of the system. This then consequently led to the Design/development phase of the chapter, where the functional requirements were modeled and designed using mock-ups and UML.

The proposed solution system was decomposed into finer components in order to understand the visualization and data flow of the system. The SBD framework, presented in *Chapter 8,* was applied to each of these development phases, in order to identify security risks and vulnerabilities at an early stage. The next chapter will provide a proof of concept, regarding

the development of an RFID enabled access control device. The microchip web solution will not be implemented in its entirety, meaning that the prototype is implemented for gaining knowledge, inspiration and for testing purposes.

10 Proof of Concept

The chapter will introduce and present a proof of concept of the microchip web solution. This Proof of concept consist of an RFID enabled access control device. This access device is programmed to authorize the microchip by reading the Unique ID (UID) of the microchip. The code, Microchip and the other components/modules used for the proof of concept will be thoroughly described in this chapter.

The RFID enabled access control device was developed with the purpose of research, testing and assessing the possibilities of microchip applications. The Development and testing phase began early on and in parallel with the development process. This was done to gain firsthand experience and understanding of the limitations and possibilities of the microchip and related technologies. The consequence of this was positive for the development of the microchip web solution and it helped coin and specify the solution's functional and security requirements. This results in the requirements defined for the microchip web solution are realistic, relatively cheap and highly probable, while still being unique and innovative.

It is important to understand that the Microchip web solution is conceptual and have not been fully developed. This means that it's only a small part of the solution that ideally can be presented in the implementation phase, namely the RFID enabled access control device.

The developed RFID reader component is used to demonstrate the RFID-reader aspect of the Microchip web solution. This RFID reader component is developed, installed and tested with a microchip. Since these components are integral parts of the proposed solution, and therefore testing of these components can provide a valuable proof of concept

10.1 The Microchip

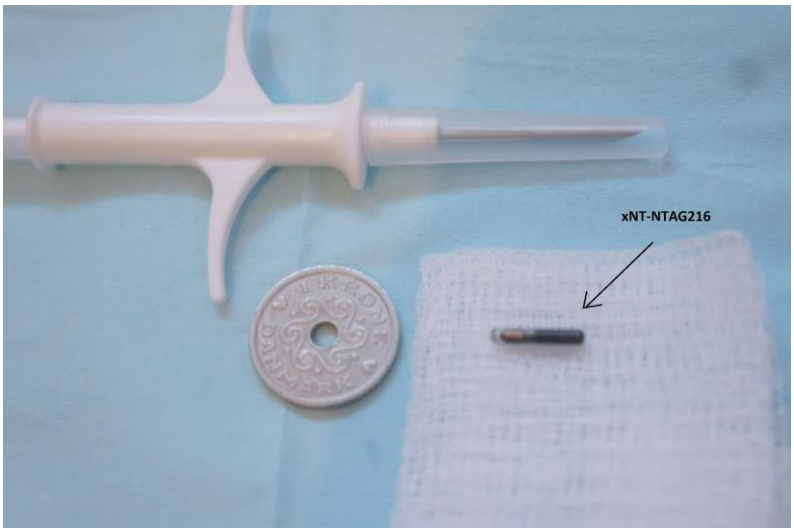

Figure 10.1: Photo of the xNT-NTAG216 chip (own figure).

The proof of concept consists of the microchip and the RFID enabled access control device. The Microchip used in the proof of concept is of model NTAG216 from xNT which as mentioned in *State of the Art* (*Chapter 4.3*) is a commonly used contactless transmission microchip which operates in 13.56 MHz frequency. The microchip has an operating distance of 100 mm, each device has a preprogrammed 7-byte UID and 888 bytes freely available for read/write data. This memory can be password protected with a 32-bit password, which prevents unauthorized memory operations. The NTAG216 (*Chapter 4.3*) used for the conceptual design was purchased from dangerousthings.com.

10.2 The RFID-enabled Access Control Device

The second part of the proof of concept is the RFID enabled access control device, which has the responsibility to read the microchip and if UID is correct then it should grant access. The development of the RFID enabled access control device together with its inner workings, is thoroughly described after the subparts of the device has been presented.

The subparts of the device are presented in the following sections.

10.2.1 Arduino UNO board and Integrated Development Environment

The Arduino Uno is a microcontroller board that is developed by Arduino.cc. The Uno is an open source electronic platform, which allows designers to control and sense the external electronic devices in the real world. The Arduino has different pins for power, analog, and digital I/O, and is powered by USB or battery (The Engineering Projects, n.d.).

The Arduino Uno can be programmed to do various of operations through the Arduino IDE, which is an open source coding development environment, which use C/C++ programming language to call a set of functions (Arduino, n.d.-a).

The Arduino is very flexible in the potential of functionalities that can be developed. Since that multiple modules can be integrated and connected to the Arduino. Some of these modules can include but are not limited to; RFID readers, lights, LCDs and even WIFI modules.

The modules that are connected to the Arduino board in order to make up the RFID enabled access control device, will be described next.

10.2.2 RFID reader module

The reader module RFID-RC522 (Last Minute Engineers, n.d.) can be used to read the UID from the Microchip. This reader is a low-cost unit commonly associated with the Arduino board and usually comes with the Arduino lifestyle package, this module operates in the 13.56MHz frequency (Last Minute Engineers, n.d.), which makes it compatible with the NTAG216 microchip (*Chapter 4.3*).

10.2.3 LCD module and servo/lock module

The LCD and servo/lock module is connected to the Arduino board. These two modules are both low-cost modules that are associated with Arduino boards and therefore also comes with the lifestyle package. The LCD module can be programmed to show text, notify and prompt the user, to take some kind of action e.g. write “Swipe hand at reader” (Kushagra, n.d.).

The servo/lock module is in reality just an extremely low-cost servo which can be programmed to rotate (Arduino, n.d.-b), the module is in the case of the proof of concept, used to simulate the opening of a lock when authorized.

The following chapter will describe the prototype of the RFID enabled access control device.

10.3 Prototype

The figure below (*Figure 10.2*), depicts the custom build RFID enabled access control device.

The device at the top left part of the picture is the Arduino Uno board. The Arduino board is wired and connected to a breadboard, allowing pins to be used for more than one module.

In the lower left corner is the RC522 RFID reader module, which is where the microchip is to be read.

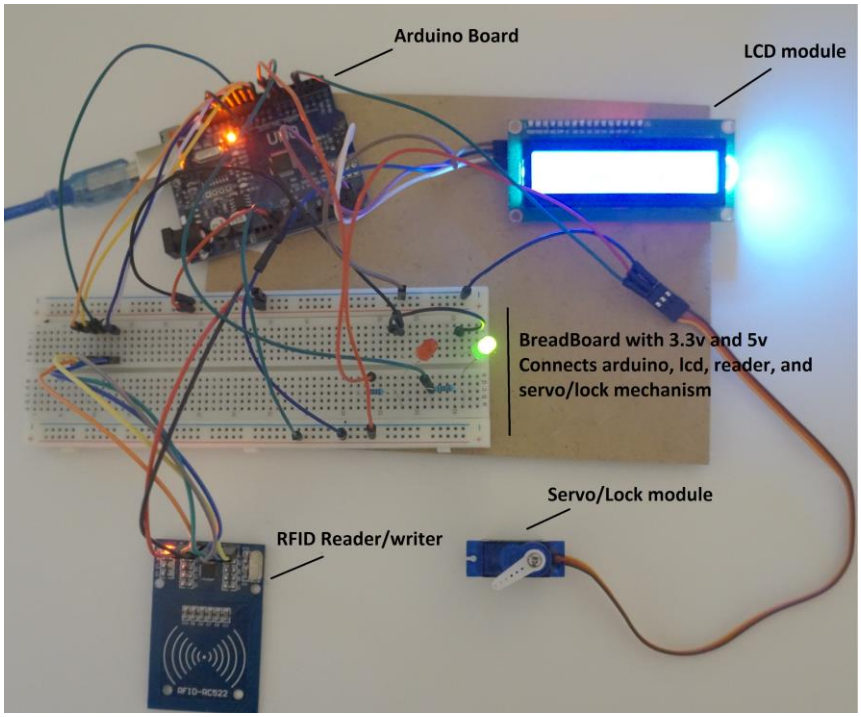

Figure 10.2: Photo of RFID-enabled access control device prototype (own figure).

The LCD and servo module can be seen at the top and lower right side of the figure. These two modules are also connected to the Arduino board and are programmed to do specific tasks, at given points or events.

In addition, there are two light LEDs one red and one green these are also integrated to the Arduino board.

The workings of the proof of concept device begin with the employee swiping their implanted hand in front of the reader.

The reader then provides the UID to the Arduino Uno IDE. The process that occurs from there is that the UID is checked for authorization.

If access is granted then the LED light turn green and the LCD, will show a text saying access granted.

This will initiate a 180° rotation which after a delay will turn back to the initial state which was 0°. This is applied in order to simulate an electronic door lock that turns when access is granted. The code behind the RFID-enabled access control device is presented and described in the following section.

10.4 Code

The Arduino IDE software can be installed from Arduino.cc. the Arduino has a huge community, where many of whom release libraries and code examples which can be used for inspiration to develop a multitude of Arduino related applications. These libraries that contain code examples, can be found in the Arduino IDE library manager. The library manager is depicted in the figure below:

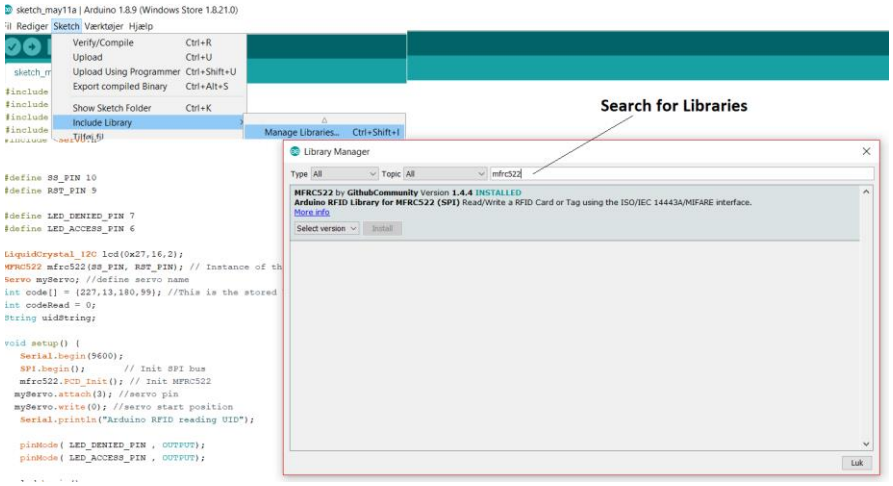

Figure 10.3: Arduino library manager (own figure).

When navigating to manage libraries one can search for specific module or functionality etc. and by that retrieve a list of libraries with readme descriptions and guidelines. These guidelines also contain information on how the module should be wired in order to perform a given task. The libraries can be added to the code project for use, Once the library has been selected and downloaded. Multiple libraries related to the modules in the proof of concepts were used to write the code behind the RFID enabled access control device. Below are a presentation and description of the code that is related to the defining and initial parts of the code.

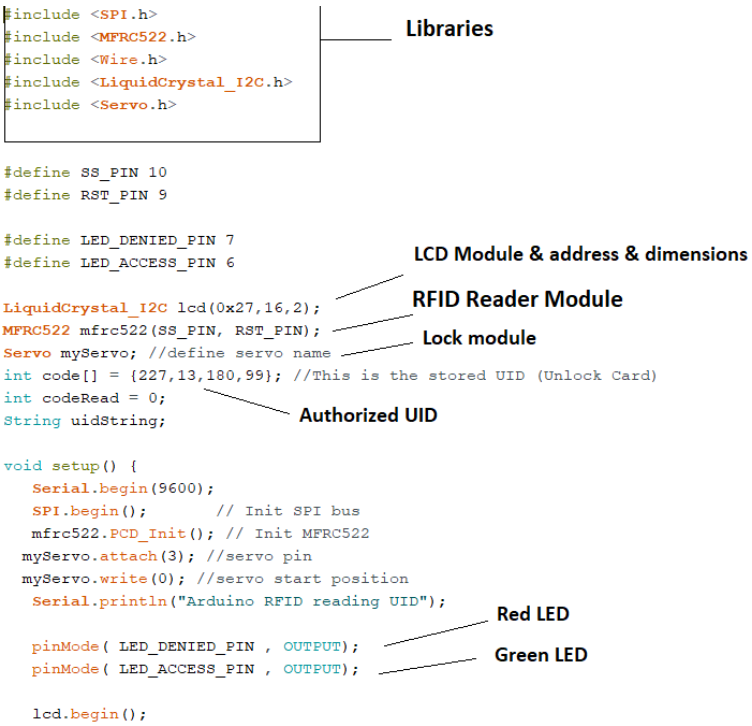

Figure 10.4: Initial parts of the code (own figure).

In the top of the code (*Figure 10.4)*, it can be seen that there are 5 different libraries included, these libraries are used for the different modules connected to the Arduino. Namely the reader, LCD and servo modules.

The first line of code is the function of the LCD module. The values that are assigned to this function is the LCD device address and the dimensions of the screen. The next line of code defines the value for the reader function, the values here are associated with the pins that it is connected to. The name is defined for the servo function on to the next line of code.

The authorized ID is the place where the UID that will be granted access is stored, this is understandably not an ideal solution, and is as mentioned only for proof of concept purposes. The ideal situation would be to match it against a database (DB) as mentioned in *Chapter 9.2*.

Finally, we see the implementation of the LED lights in the code. These lights were as mentioned used to indicate if access is granted or not (green LED for granted, red LED for denied).

The figure below (*Figure 10.5*) depicts the event handling that occurs when the UID value is read from the microchip.

```
if(match)                                   | If the Chips UID is succesfully authorized
{

   digitalWrite( LED_ACCESS_PIN , HIGH);    | Green Led blink
   delay(1000);                             |
   digitalWrite( LED_ACCESS_PIN , LOW);     |
   delay(1000);                             |
   digitalWrite( LED_ACCESS_PIN , HIGH);    |
   delay(1000);                             |
   lcd.print("Authorized access");          | Print success status on LCD
    myServo.write(180);                     | Lock Module turn 180*
     delay(5000);
     myServo.write(0);                      | Lock turns back to initial state
     digitalWrite( LED_ACCESS_PIN , LOW);   | LED turns off!

}else{                                      | when Access is denied
 digitalWrite( LED_DENIED_PIN , HIGH);      | Red LED blink
 delay(1000);                               |
 digitalWrite( LED_DENIED_PIN , LOW);       |
 delay(1000);                               |
   digitalWrite( LED_DENIED_PIN , HIGH);    |

   lcd.print(" Access denied  ");           | Print denied status on LCD
  Serial.println("\nUnknown Card");         |
  delay(2000);                              |
  digitalWrite( LED_DENIED_PIN , LOW);      | LED turns off!
}

  Serial.println("============================");

  mfrc522.PICC_HaltA();

  delay(3000);
  reset_state();                            | Reset state - "Show your card"
```

Figure 10.5: Event handling code (own figure)

The top of the code represents an if/else loop that checks if there is a match between the UID stored on the microchip and the UID that is applied in the code. If there is a match then the green LED will begin to turn on and off with a delay in between, which result in a blinking motion. “Authorized access” is then printed on the LCD screen, shortly after the servo will turn 180 degrees and stay there for a delayed time and then turn back to the initial state.

However, if access is denied, then the red LED light will start to blink, and “Access denied” will instead be printed on the LCD screen. The state will be reset after a short time, and the user can try again.

10.5 Subconclusion

This chapter presented and described a proof of concept, namely the development of an RFID-enabled access control device. This device was developed, assembled and coded in order to gain knowledge of the inner workings of a programmed RFID reader device and test it with a microchip. The device was built using an Arduino board together with different modules such as an RFID reader, LCD screen, LED lights, and a servo rotor. The result was successful in that the prototype is able to read the UID of the microchip and check for authorization. The LCD module functions and is capable of notifying on the screen while prompting the employe

to take action, e.g. “Swipe your hand”. If the chip UID is authorized, then the LED lights will turn on, LCD screen text will be “access granted” and then the servo module will rotate 180°. The rotation of the servo signifies that the door lock is opened.

The security-by-design framework was not applied to the proof of concept, however, many security considerations were kept in mind when developing the RFID enabled access control device. The implementation phase of the microchip web solution proposed in the *Conceptual Design* (*Chapter 10)* would be the next phase where the security-by-design framework should be applied. The implementation phase is not conducted in this thesis report. This is a result of the conceptual nature of the proposed solution, and that the solution consists of multiple parts and the RFID reader device is simply one part of it.

11 Discussion

In this chapter, a reflection of some of the choices and challenges presenting themselves throughout the project will be presented. This includes reflections on things such as the choice of the theoretical framework, the surveys, and the interviews.

First off, during the course of the project, it was quickly made evident that the technology has yet to take off on a global scale, especially for use in an enterprise setting. The market is still very niche and is arguably still early on in its diffusion process. It was for these reasons that the project explored the legal environment and rate of adoption to get insight into some of the potential barriers. However, based on qualitative data in the form of interviews, it also seems that the rate of adoption is finally seeing some acceleration.

In terms of the legal environment, it appears that there is a lack of a legal framework for data processing and legal rights of the workers in the context of human microchipping. As a result, enterprises adopting the technology and offering it to their employees have to rely on compliance with the GDPR and human rights legislation, which may act to impede the rate of adoption.

Having established that, let us consider the theoretical framework chosen for this project. Rogers' DOI theory provided a solid theory to help shed light on the rate of adoption of human microchip implant technology. By investigating the perceived attributes of the innovation as seen by potential adopters, it provided an overview of the aspects which could act as barriers and slow down the rate of adoption. Nevertheless, as mentioned in the Theory chapter, the theory uses the same set of attributes for all innovations, however different they may be. So, an argument can be made for modifying the attributes according to the innovation being investigated. As the attributes were not modified when investigating human microchip implants for this project, it may have affected or missed some of the inferences and conclusions which could be made.

For the survey on the perceived attributes of the innovation, the sample size was relatively small. However, since a big portion of the respondents were from the same organization, the data was arguably still useful for representing the attitude within an arbitrary IT and procurement organization.

Throughout the duration of the survey and based on feedback from participants and interviews conducted with early adopters, it was pointed out that there may be other barriers to adoption which were not considered in the survey. For example, concerns surrounding surveillance, privacy, security, and health were mentioned. For future research, it may be interesting to take

these aspects into consideration, also, when investigating the rate of adoption. Another point worth mentioning in regards to future research would be to investigate the opinions regarding perceived attributes at a point in time in the future, to see if things have changed.

From the interviews, it was pointed out that the adopters saw more potential for human microchipping in the realm beyond the workplace. Furthermore, it was also made clear that as of right now, there is no scenario where an employer would force an employee to get an implant. As such, it may be worth taking these points into consideration for future research.

During the course of the project, it was quite challenging to combine the knowledge acquired from the rate of adoption survey with the conceptual design of the proposed solution. As a result, a decision was made to divide the project into two main parts. One part with the objective of exploring the rate of adoption of human microchipping along with associated potential barriers impeding the rate of adoption. Moreover, the legal environment was considered. The other part was dedicated to the development and proposal of a conceptual solution, regarding a microchip web solution, together with the implementation of the proof of concept.

The conceptual solution was developed using a methodology with security-by-design principles applied to each of the development phases. The report provides documentation for the 3 initial phases of the SDLC. Namely, Initiation, Acquisition, and Design, whereas the 4th, 5th, and 6th phases are to be conducted after the solution is live, and are, therefore, not documented in this report.

The security framework integration is documented in this report after each corresponding phase. The activities of the SBD processes are applied to the best ability, however, these activities are conducted by the authors of this report. The most ideal is that the activities such as a risk assessment should be made by a third-party independent security officer/consultant (*Chapter 8.3*).

The security processes that are concerned with the implementation phase are not applied to the proof of concept nor the entire solution as a whole. This is because of the conceptual nature of the microchip web solution. This results in an inadequate implementation phase and, therefore, the SBD processes will not be fully appreciated.

12 Conclusion

The relevance of this project is quite compelling, as even though human microchipping is still in its early diffusion stages and appears to have a slow rate of adoption thus far, arguably due to many of the implications identified in this project, there seems to be an increased awareness and interest in the technology and its potential applications as of late. Furthermore, the amount of research exploring the rate of adoption of the technology is quite limited at the time of writing, which increases the novelty of the research conducted in this project. Finally, the technology has yet to see much use in an enterprise setting, which propelled the project into exploring how a secure human microchip implant solution could be developed.

To investigate the regulatory and legal aspects of human microchip technology adoptions in a business organization scenario, the project looked into current relevant regulation which was applicable to the field. This included relevant aspects of the GDPR as well as Human Rights regulation. Here, it was evident that there is a lack of a specific legal framework for directly protecting the rights of the employees of an organization in terms of data protection, for example, which could act as a barrier for the further adoption of the technology for use in businesses.

Moreover, to analyze the acceptance of the technology, Rogers' Diffusion of Innovations theory was applied. To shed light on the rate of adoption and identify factors facilitating and impeding the diffusion, the perceived relative advantage, compatibility, complexity, trialability and observability of human microchipping was surveyed among potential adopters. The data showed that the main barriers which may act to impede the rate of adoption were the compatibility with social norms and needs within the social system as well as the degree to which the technology could be tested on a limited basis prior to deciding to adopt or reject the technology. On the other hand, relative advantages of the technology appeared to be clear to the respondents as well as little perceived complexity.

Finally, it was significant to look into how a conceptual design would look like for enterprise adoption in order to increase convenience, allow for seamless authorization, and personalization of the employees, thus allowing them to get rid of the increasing management burden of having many different keys and cards, carrying the risk of being misplaced or stolen. To make the solution secure, a security-by-design framework was adopted for the development process. Specifically, a framework was introduced to be used together with the System Development Life Cycle (SDLC) development phases, namely the Security-by-Design (SBD). The purpose of implementing the framework was to provide a secure development framework for the development of the proposed solution and identify security risks and

vulnerabilities at an early stage. The development of the conceptual solution was documented and divided into three segments: initiation, acquisition, and design/development. The design was decomposed into finer components in order to understand the visualization and data flow of the system.

Finally, a proof of concept was created in the form of an RFID-enabled access control device, which has the functionality of reading a microchip and if authorized, grant access. This proof of concept proved to be successful in terms of the functionality of authorization and reading the microchip’s unique ID.

References

ABR. (n.d.). What is RFID and How Does RFID Work? Retrieved April 22, 2019, from https://www.abr.com/what-is-rfid-how-does-rfid-work/

Adrion, F. (2018). *Adaption and assessment of a UHF-RFID system for livestock management*. [American Society of Agricultural Engineers]. Retrieved from https://www.researchgate.net/publication/323471556_Adaption_and_assessment_of_a_UHF-RFID_system_for_livestock_management

Ahson, S., & Ilyas, M. (2008). *RFID HANDBOOK: Applications, Technology, Security, and Privacy*. CRC Press Web. Retrieved from http://ec-wu.at/spiekermann/publications/inbooks/ons security in rfid handbook.pdf

Ajibade, P. (2018). *Technology Acceptance Model Limitations and Criticisms: Exploring the Practical Applications and Use in Technology-related Studies, Mixed-method, and Qualitative Researches*. Retrieved from http://digitalcommons.unl.edu/libphilprac/1941

Ali, A. H. (2017). *The role of ICT in enhancing e-waste business opportunities in Members*. Retrieved from https://projekter.aau.dk/projekter/files/260345657/MasterThesis_34BD_L2.pdf

Arduino. (n.d.-a). Arduino FAQ. Retrieved May 5, 2019, from https://www.arduino.cc/en/Main/FAQ

Arduino. (n.d.-b). Arduino - Servo. Retrieved May 5, 2019, from https://www.arduino.cc/en/Reference/Servo

Atkinson, N. (2007). Developing a Questionnaire to Measure Perceived Attributes of eHealth Innovations.

Baghi, R. (2015). *Medical Treatment in the Digital Age - A Case Study of Mobile Healthcare Applications in Shanghai*. Retrieved from https://studenttheses.cbs.dk/xmlui/bitstream/handle/10417/5764/roxana_baghi.pdf?sequence=1

Bagozzi, R. P. (2007). *The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift.* (Vol. 8). Retrieved from http://www.sietmanagement.fr/wp-content/uploads/2016/04/2007-bagozzi-jinfosystems.pdf

Bayometric. (n.d.-b). Fingerprint SDK – Fingerprint Software for Identification. Retrieved April 4, 2019, from https://www.bayometric.com/

Bayometric. (n.d.-a). About Us. Retrieved April 3, 2019, from https://www.bayometric.com/about-us/

Bertram, D. (2007). Likert Scales, 10. https://doi.org/10.1002/9780470479216.corpsy0508

Best Quality Services Singapore. (2018). Pros and Cons of Biometric Access Systems. Retrieved April 3, 2019, from http://www.qualityservices.sg/pros-and-cons-of-biometric-access-systems/

Biohackinfo. (n.d.). RFID & NFC Implants. Retrieved April 24, 2019, from https://biohackinfo.com/rfid-nfc-implant/

Bright Alliance Technology. (n.d.). The Different Types of RFID Systems. Retrieved March 18, 2019, from http://www.batlgroup.net/the-different-types-of-rfid-systems/

Brown, A. (2016). Human Microchipping: An Unbiased Look at the Pros and Cons. Retrieved March 13, 2019, from https://www.freecodecamp.org/news/human-microchipping-an-unbiased-look-at-the-pros-and-cons-ba8f979ebd96/

Business Wire. (2003). VeriChip Corporation Receives First Orders for VeriGuard Secure Access Control Scanning Devices - 2,100 Additional VeriChips and 130 Handheld Scanners Also Ordered. Retrieved April 5, 2019, from https://www.businesswire.com/news/home/20031021005517/en/VeriChip-Corporation-Receives-Orders-VeriGuard-Secure-Access

Ceta, N. (2018). All You Need to Know About UML Diagrams: Types and 5+ Examples. Retrieved April 6, 2019, from https://tallyfy.com/uml-diagram/

Chen, E. T. (2015). RFID Technology and Privacy (pp. 140–155). https://doi.org/10.4018/978-1-4666-6308-4.ch007

Chuttur, M. (2009). Working Papers on Information Systems Overview of the Technology Acceptance Model: Origins, Developments and Future Directions. Retrieved from https://expertiseweek3.files.wordpress.com/2014/04/chuttur-2009-tamreview3.pdf

CLODOC. (2017). Pros and Cons of Wearable Technologies. Retrieved April 1, 2019, from https://www.clodoc.com/blog/pros-and-cons-of-wearable-technologies/

Cmiljanic, N., Landaluce, H., & Perallos, A. (2018). A Comparison of RFID Anti-Collision Protocols for Tag Identification. *Applied Sciences*, *8*(8), 1282. https://doi.org/10.3390/app8081282

CNBC. (2017). Start-up Epicenter implants employees with microchips. Retrieved April 7, 2019, from https://www.cnbc.com/2017/04/03/start-up-epicenter-implants-employees-with-microchips.html

Council of Europe. (2019). *Guide on Article 8 of the European Convention on Human Rights - Right to respect for private and family life, home and correspondence*. Retrieved from www.echr.coe.int

CSA Singapore. (n.d.). *Security-by-Design Framework.* Retrieved from https://www.csa.gov.sg/~/media/csa/documents/legislation_supplementary_references/security_by_design_framework.pdf

Czaja, S. J., Charness, N., Fisk, A. D., Hertzog, C., Nair, S. N., Rogers, W. A., & Sharit, J. (2006). Factors predicting the use of technology: Findings from the center for research and education on aging and technology enhancement (create). *Psychology and Aging*, *21*(2), 333–352. https://doi.org/10.1037/0882-7974.21.2.333

Dimov, D. (2014). Human-implanted RFID chips. Retrieved April 1, 2019, from https://resources.infosecinstitute.com/human-implanted-rfid-chips/

DoITPoMS. (n.d.). Loss in dielectrics. Retrieved May 1, 2019, from https://www.doitpoms.ac.uk/tlplib/dielectrics/loss.php

EdgeConnector. (n.d.). RFID cards & tags in access control. Retrieved March 22, 2019, from https://www.edgeconnector.com/rfid-cards-tags-access-control/

Electronics Notes. (n.d.-a). RFID Standards. Retrieved April 21, 2019, from https://www.electronics-notes.com/articles/connectivity/rfid-radio-frequency-identification/standards-iec-iso-epcglobal.php

Electronics Notes. (n.d.-b). RFID Coupling Techniques: Backscatter Capacitive Inductive. Retrieved May 1, 2019, from https://www.electronics-notes.com/articles/connectivity/rfid-radio-frequency-identification/coupling-techniques-capacitive-inductive-backscatter.php

Equal Employment Opportunity Commission. (n.d.). Religious Discrimination. Retrieved May 5, 2019, from https://www.eeoc.gov/laws/types/religion.cfm

European Union. (2016). Consolidated Version of the Treaty on the Functioning of the European Union. *Official Journal of the European Union*. Retrieved from https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0006.01/DOC_3&format=PDF

European Union. (2008). EUR-Lex - 12008E019 - EN. *Official Journal 115 , 09/05/2008 P. 0056 - 0056;* Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12008E019:EN:HTML

FERMAX. (2017). Biometric Access Control Pros and Cons. Retrieved April 2, 2019, from https://blog.fermax.com/eng/biometric-access-control-pros-and-cons

Fidesmo. (n.d.). Home. Retrieved May 12, 2019, from https://fidesmo.com/home/

Firfiray, S. (2018). Microchip implants are threatening workers' rights. Retrieved April 22, 2019, from http://theconversation.com/microchip-implants-are-threatening-workers-rights-107221

Foster, K. R., & Jaeger, J. (2008). Ethical Implications of Implantable Radiofrequency Identification (RFID) Tags in Humans. *The American Journal of Bioethics*, *8*(8), 44–48. https://doi.org/10.1080/15265160802317966

Furnham, A. (1986). Response bias, social desirability and dissimulation. *Personality and Individual Differences*, *7*(3), 385–400. https://doi.org/10.1016/0191-8869(86)90014-0

Gaille, B. (2015). 14 RFID Pros and Cons. Retrieved March 27, 2019, from https://brandongaille.com/14-rfid-pros-and-cons/

GAO RFID. (n.d.). What is RFID tag collision? Retrieved April 17, 2019, from https://gaorfid.com/faqwd/what-is-rfid-tag-collision/

Gasson, M., Kosta, E., & Bowman, D. (2012). *Information Technology and Law Series Volume 23*. https://doi.org/10.1007/978-90-6704-870-5

GDPR. (2018). General Data Protection Regulation – GDPR. Retrieved April 26, 2019, from https://gdpr-info.eu/

Global Venture. (n.d.). History of RFID. Retrieved April 29, 2019, from https://www.globalventurelabels.com/history-of-rfid/

Grauer, Y. (2018). A practical guide to microchip implants. Retrieved April 15, 2019, from https://arstechnica.com/features/2018/01/a-practical-guide-to-microchip-implants/

Graveling, R., Winski, T., & Dixon, K. (2018). *The Use of Chip Implants for Workers*. Retrieved from http://www.europarl.europa.eu/RegData/etudes/STUD/2018/614209/IPOL_STU(2018)614209_EN.pdf

Greenhalgh, P. Robert, G. MacFarlane, F. Bate, P. Kyriakidou, O. (2004). *Diffusion of Innovations*. *Milbank Quaterley* (5th editio, Vol. 82). Free Press.

Heiberger, R. M., & Robbins, N. B. (2014). Design of Diverging Stacked Bar Charts for Likert Scales and Other Applications. *Journal of Statistical Software*, *57*(5), 1–32. https://doi.org/10.18637/jss.v057.i05

Humavox. (2016). Wearable Tech Advantages & Disadvantages. Retrieved March 30, 2019, from http://www.humavox.com/blog/exploring-advantages-disadvantages-wearable-tech/

Impinj. (n.d.). RFID Standards. Retrieved April 20, 2019, from https://www.impinj.com/about-rfid/rfid-standards/

Inner Range. (2017). 8 benefits of smart cards - for door access control and much more. Retrieved March 23, 2019, from http://www.innerrange.co.uk/8-benefits-of-smart-cards-for-door-access-control-and-much-more/

in-Pharma. (2017). FDA clears RFID chip for humans. Retrieved March 21, 2019, from https://www.in-pharmatechnologist.com/Article/2004/10/18/FDA-clears-RFID-chip-for-humans

Ismail, S. (2006). Detailed review of Rogers' diffusion of innovations theory and educational technology-related studies based on Rogers' theory. *The Turkish Online Journal of Educational Technology*. Retrieved from https://www.researchgate.net/publication/284675572_Detailed_review_of_Rogers'_diffusion_of_innovations_theory_and_educational_technology-related_studies_based_on_Rogers'_theory

Jamieson, S. (2004). Likert scales: how to (ab)use them. *Medical Education*, *38*(12), 1217–1218. https://doi.org/10.1111/j.1365-2929.2004.02012.x

Jefferson, G. (2017). Are embedded microchips dangerous? Ask the Swedes — and pets. Retrieved April 7, 2019, from https://eu.usatoday.com/story/tech/talkingtech/2017/07/25/do-microchip-implants-pose-health-risks-ask-swedes-and-pets/507408001/

Kapoor, K. K., Dwivedi, Y. K., & Williams, M. D. (2014). Rogers' Innovation Adoption Attributes: A Systematic Review and Synthesis of Existing Research. *Information Systems Management*, *31*(1), 74–91. https://doi.org/10.1080/10580530.2014.854103

Kaur, M., Sandhu, M., Mohan, N., & Sandhu, P. (2011). RFID Technology Principles, Advantages, Limitations & Its Applications. *International Journal of Computer and Electrical Engineering*, *3*(1). Retrieved from http://www.ijcee.org/papers/306-E794.pdf

Khan, N. A. (2015). *RFIDs Chip Implants and their related Ethical Issues*. https://doi.org/10.13140/RG.2.1.3717.6166

Kiourti, A. (2018). RFID Antennas for Body-Area Applications: From Wearables to Implants. *IEEE Antennas and Propagation Magazine*, *60*(5), 14–25. https://doi.org/10.1109/MAP.2018.2859167

Kotzé, T. G., Anderson, O., & Summerfield, K. (2016). *Technophobia: Gender differences in the adoption of high-technology consumer products*. *J.Bus.Manage*. Retrieved from https://pdfs.semanticscholar.org/bf5f/a8ac1c0304acd7cdf8460276f1eb23c9c615.pdf

KSEC Solutions. (n.d.-a). Vivokey. Retrieved May 12, 2019, from https://cyborg.ksecsolutions.com/service/vivokey/

KSEC Solutions. (n.d.-b). Abouts. Retrieved May 12, 2019, from https://cyborg.ksecsolutions.com/about/

Kushagra. (n.d.). 16 x 2 LCD Datasheet | 16x2 Character LCD Module PINOUT. Retrieved May 5, 2019, from https://www.engineersgarage.com/electronic-components/16x2-lcd-module-datasheet

Lai, P. C. (2017). The literature review of technology adoption models and theories for the novelty technology. *Journal of Information Systems and Technology Management*, *14*(1), 21–38. https://doi.org/10.4301/S1807-17752017000100002

Last Minute Engineers. (n.d.). In-Depth: What is RFID? How It Works? Interface RC522 with Arduino. Retrieved May 8, 2019, from https://lastminuteengineers.com/how-rfid-works-rc522-arduino-tutorial/

Lucidchart. (n.d.). What is a Flowchart. Retrieved April 9, 2019, from https://www.lucidchart.com/pages/what-is-a-flowchart-tutorial

Lyytinen, K., & Damsgaard, J. (2001). What's Wrong with the Diffusion of Innovation Theory? The case of a complex and networked technology. https://doi.org/10.1007/978-0-387-35404-0_19

Marie-Sainte, S., Alrazgan, M. S., Bousbahi, F., Ghouzali, S., & Abdul, W. (2016). From Mobile to Wearable System: A Wearable RFID System to Enhance Teaching and Learning Conditions. *Mobile Information Systems*, *2016*, 1–10. https://doi.org/10.1155/2016/8364909

MD Magazine. (2007). The VeriChip Implantable Microchip: The Future of Patient Identification. Retrieved April 5, 2019, from https://www.mdmag.com/medical-news/verichip

Medynskiy, Y., Gov, S., Mazalek, A., & Minnen, D. (n.d.). *Wearable RFID for Play*. Retrieved from https://www.researchgate.net/publication/253814046_Wearable_RFID_for_Play

Meyer, G. (2004). Diffusion Methodology: Time to Innovate? *Journal of Health Communication*, *9*(sup1), 59–69. https://doi.org/10.1080/10810730490271539

Michael, K., Michael, M. G., & Ip, R. (2008). *Microchip implants for humans as unique identifiers: a case study on VeriChip*. Retrieved from http://ro.uow.edu.au/infopapers/586

Michael, K., & Michael, M. G. (2010). The diffusion of RFID implants for access control and epayments: A case study on Baja Beach Club in Barcelona. In *2010 IEEE International Symposium on Technology and Society* (pp. 242–252). IEEE. https://doi.org/10.1109/ISTAS.2010.5514631

Mitrokotsa, A., Rieback, M. R., & Tanenbaum, A. S. (2010). Classifying RFID attacks and defenses. *Information Systems Frontiers*, *12*(5), 491–505. https://doi.org/10.1007/s10796-009-9210-z

Nanalyze. (2017). Who Makes the RFID Chip Implants for Humans? Retrieved April 6, 2019, from https://www.nanalyze.com/2017/08/who-makes-rfid-chip-implants-humans/

NPR. (2018). Thousands Of Swedes Are Inserting Microchips Under Their Skin. Retrieved April 6, 2019, from https://www.npr.org/2018/10/22/658808705/thousands-of-swedes-are-inserting-microchips-under-their-skin?t=1552594604697

NXP. (n.d.). NTAG213/215/216. Retrieved April 15, 2019, from https://www.nxp.com/products/identification-security/rfid/nfc-hf/ntag/ntag-for-tags-labels/ntag-213-215-216-nfc-forum-type-2-tag-compliant-ic-with-144-504-888-bytes-user-memory:NTAG213_215_216

Ocampo, S., & Ambrose, J. (2015). Wearables in access control. Retrieved March 29, 2019, from https://futurelab.assaabloy.com/en/wearables-in-access-control/

OWASP. (2016). Security by Design Principles. Retrieved May 6, 2019, from https://www.owasp.org/index.php/Security_by_Design_Principles

Papiewski, J. (n.d.). The Advantages of Smart Cards With RFID. Retrieved March 21, 2019, from https://itstillworks.com/advantages-smart-cards-rfid-18520.html

PC Dreams. (2016). Pros and Cons of a Biometric Attendance and Access Control System. Retrieved April 2, 2019, from https://pcdreams.com.sg/pros-and-cons-of-a-biometric-attendance-and-access-control-system/

Perakslis, C., & Wolk, R. (2006). Social acceptance of RFID as a biometric security method. *IEEE Technology and Society Magazine*, *25*(3), 34–42. https://doi.org/10.1109/MTAS.2006.1700020

Prutchi, D. (2011). VeriMed's Human-Implantable VeriChip Patient RFID. Retrieved April 5, 2019, from http://www.implantable-device.com/2011/12/30/verimeds-human-implantable-verichip-patient-rfid/

Rackspace Support. (2018). Manage Backups for Cloud Databases. Retrieved May 6, 2019, from https://support.rackspace.com/how-to/managing-backups-for-cloud-databases/

RFID Journal. (2011). What Is a Semi-passive RFID Tag? Retrieved May 1, 2019, from https://www.rfidjournal.com/blogs/experts/entry?8117

Roberti, M. (2005). The History of RFID Technology. Retrieved May 31, 2019, from https://www.rfidjournal.com/articles/view?1338

Rogers, E. (2003). *Diffusion of Innovations* (5th Ed). Free Press.

Roosendaal, A. (2012). Information Technology and Law Series Volume 23. https://doi.org/10.1007/978-90-6704-870-5

Rotter, P. (2008). A Framework for Assessing RFID System Security and Privacy Risks. *IEEE Pervasive Computing*, *7*(2), 70–77. https://doi.org/10.1109/MPRV.2008.22

Rouse, M. (2018). What is RFID tagging? Retrieved May 2, 2019, from https://internetofthingsagenda.techtarget.com/definition/RFID-tagging

Roy, S., & Boyer, C. (2014). Backscatter Communication and RFID: Coding, Energy, and MIMO Analysis. https://doi.org/10.1109/TCOMM.2013.120713.130417

Sani, A., Rajab, M., Foster, R., & Hao, Y. (2010). Antennas and Propagation of Implanted RFIDs for Pervasive Healthcare Applications. *Proceedings of the IEEE*, *98*(9), 1648–1655. https://doi.org/10.1109/JPROC.2010.2051010

Sathya, K. (n.d.). *Size Reduction of Low Frequency Micro Strip Patch Antennas with Koch Fractal Slots*. Retrieved from http://www.ece.iisc.ernet.in/~kjvinoy/adspdf/Sathya.pdf

Sisodiya, S. (n.d.). What are the Passive RFID Tags? Retrieved April 25, 2019, from https://www.engineersgarage.com/articles/passive-rfid-tags

Smiley, S. (2016-b). Active RFID vs. Passive RFID: What's the Difference? Retrieved May 3, 2019, from https://blog.atlasrfidstore.com/active-rfid-vs-passive-rfid

Smiley, S. (2016-a). 7 Types of Security Attacks on RFID Systems. Retrieved May 2, 2019, from https://blog.atlasrfidstore.com/7-types-security-attacks-rfid-systems

Smith, D. (2017). Advantages and Disadvantages of Smart Card Technology. Retrieved March 29, 2019, from https://www.esoftload.info/advantages-disadvantages-smart-card-technology

Soper, T. (2013). Crowdfunding campaign will embed an NFC chip in your hand for $99. Retrieved April 13, 2019, from https://www.geekwire.com/2013/xnt-implantable-nfc-chip/

Stark RFID. (n.d.-a). About Stark RFID. Retrieved April 2, 2019, from http://www.starkrfid.com/about/

Stark RFID. (n.d.-b). RFID Tags, Bracelets and Credentials. Retrieved April 2, 2019, from http://www.starkrfid.com/rfid-products/rfid-tags-bracelets/

Taherdoost, H. (2018). A review of technology acceptance and adoption models and theories. *Procedia Manufacturing*, *22*, 960–967. https://doi.org/10.1016/J.PROMFG.2018.03.137

Technovelgy. (n.d.-a). RFID Reader Collision. Retrieved April 19, 2019, from http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=58

Techopedia. (n.d.-b). What is a Microchip Implant? Retrieved March 10, 2019, from https://www.techopedia.com/definition/15184/microchip-implant

Techopedia. (n.d.-c). What is a Radio Frequency Identification Reader (RFID Reader)? Retrieved March 13, 2019, from https://www.techopedia.com/definition/26992/radio-frequency-identification-reader-rfid-reader

Techopedia. (n.d.). What is a Radio Frequency Identification Tag (RFID Tag)? Retrieved April 22, 2019, from https://www.techopedia.com/definition/24273/radio-frequency-identification-tag-rfid-tag

Thakkar, D. (n.d.). Synopsis of a Biometric Access Control System. Retrieved April 2, 2019, from https://www.bayometric.com/synopsis-of-a-biometric-access-control-system/

The Engineering Projects. (n.d.). Introduction to Arduino Uno. Retrieved May 6, 2019, from https://www.theengineeringprojects.com/2018/06/introduction-to-arduino-uno.html

ThomasNet. (n.d.). Biometric Access Control Principles. Retrieved April 2, 2019, from https://www.thomasnet.com/articles/automation-electronics/principles-biometric-access

Thompson, C. (2015). What's inside a Dangerous Things body hacking kit. Retrieved April 12, 2019, from https://www.businessinsider.com/whats-inside-a-dangerous-things-body-hacking-kit-2015-7?r=US&IR=T

Thrasher, J. (2013). What is RFID Used for in the Real World? Retrieved April 20, 2019, from https://blog.atlasrfidstore.com/what-is-rfid-used-for-in-applications

Tigrisnet. (n.d.-a). About Us. Retrieved March 29, 2019, from https://www.tigrisnet.com/about/

Tigrisnet. (n.d.-b). Card solutions. Retrieved March 29, 2019, from https://www.tigrisnet.com/card-solutions/

Tigrisnet. (n.d.-c). Payment card solutions. Retrieved March 28, 2019, from https://www.tigrisnet.com/payment-card-solutions/

Tornatzky, L. G., & Klein, K. J. (1982). Innovation characteristics and innovation adoption-implementation: A meta-analysis of findings. *IEEE Transactions on Engineering Management*, *EM-29*(1), 28–45. https://doi.org/10.1109/TEM.1982.6447463

Wahlquist, C. (2017). Under the skin: how insertable microchips could unlock the future. Retrieved March 11, 2019, from https://www.theguardian.com/technology/2017/nov/01/under-the-skin-how-insertable-microchips-could-unlock-the-future

Watson, D. (1992). Correcting for Acquiescent Response Bias in the Absence of a Balanced Scale. *Sociological Methods & Research*, *21*(1), 52–88. https://doi.org/10.1177/0049124192021001003

Wolfe, S. (2018). Biohax says UK businesses planning microchip implants for employees. Retrieved April 8, 2019, from https://www.businessinsider.com/biohax-uk-businesses-microchip-implants-employees-2018-11?r=US&IR=T

Wright, K. B. (2006). Researching Internet-Based Populations: Advantages and Disadvantages of Online Survey Research, Online Questionnaire Authoring Software Packages, and Web Survey Services. *Journal of Computer-Mediated Communication*, *10*(3), 00–00. https://doi.org/10.1111/j.1083-6101.2005.tb00259.x

Zhang, Q. (n.d.). *Backscatter Communication*. Retrieved from https://www.cse.ust.hk/~qianzh/MSBD6000F/notes/7-backscatter-2.pdf

Appendices

APPENDIX A. Diverging Stacked Bar Charts

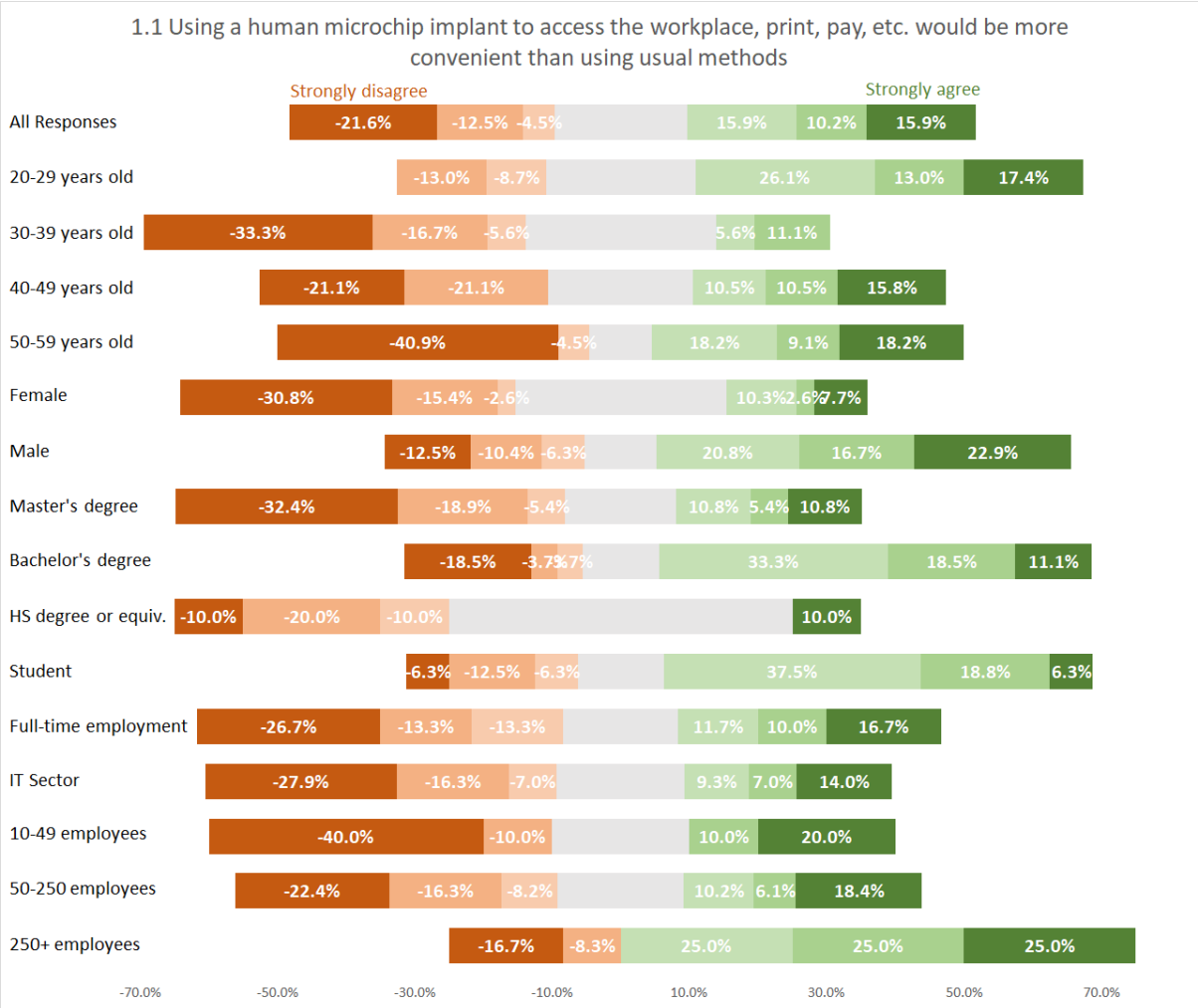

Figure A1: Diverging stacked bar chart showing all responses and demographic groups for statement 1.1 (own figure).

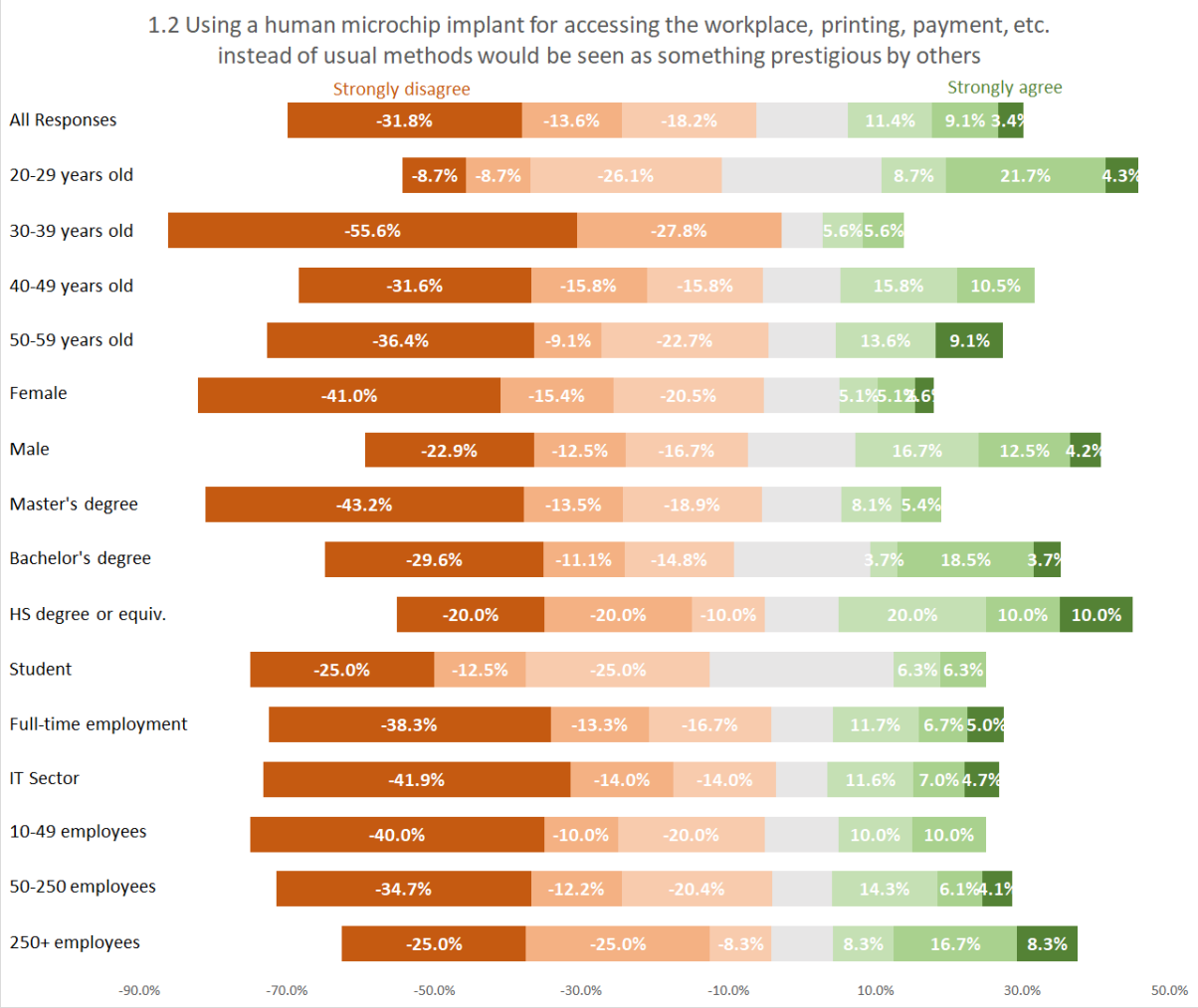

Figure A2: Diverging stacked bar chart showing all responses and demographic groups for statement 1.2 (own figure).

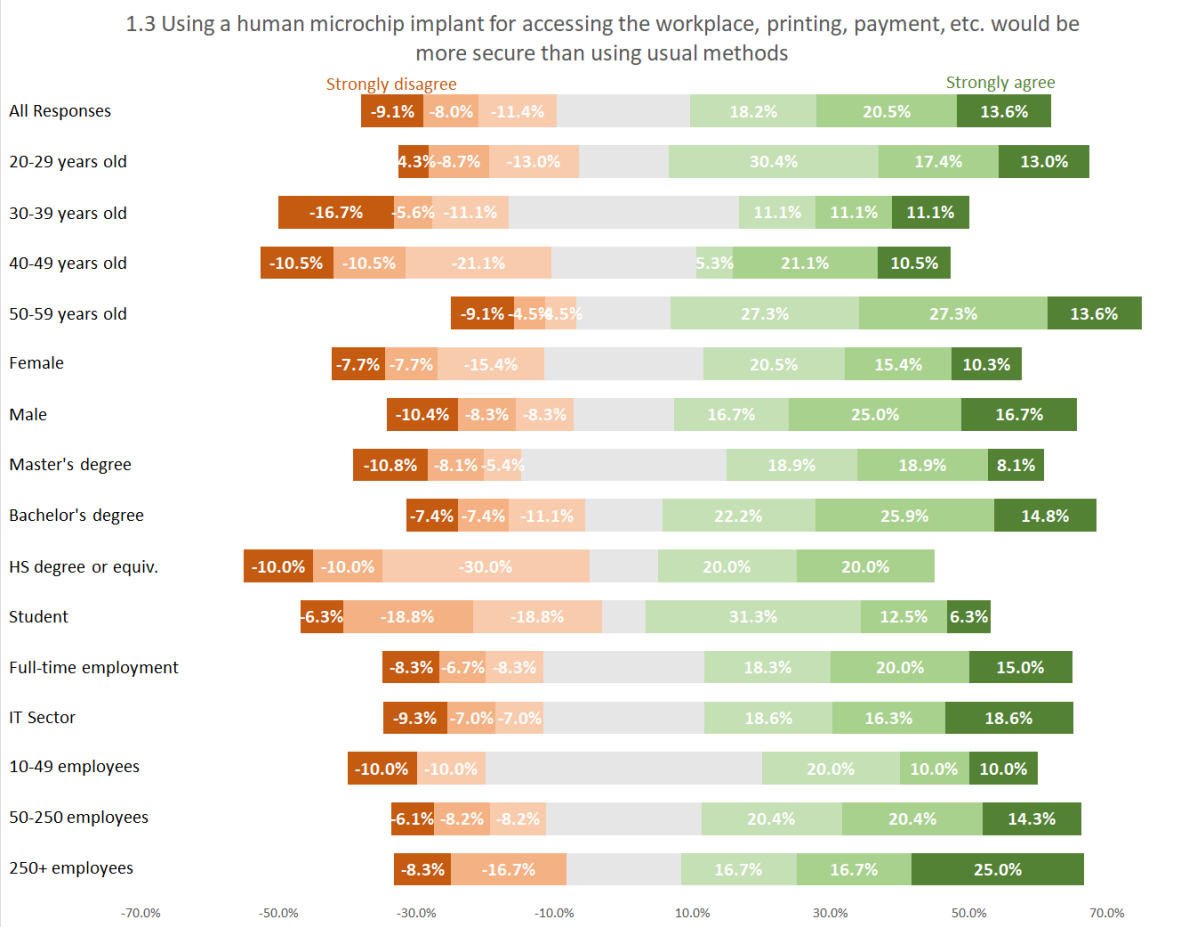

Figure A3: Diverging stacked bar chart showing all responses and demographic groups for statement 1.3 (own figure).

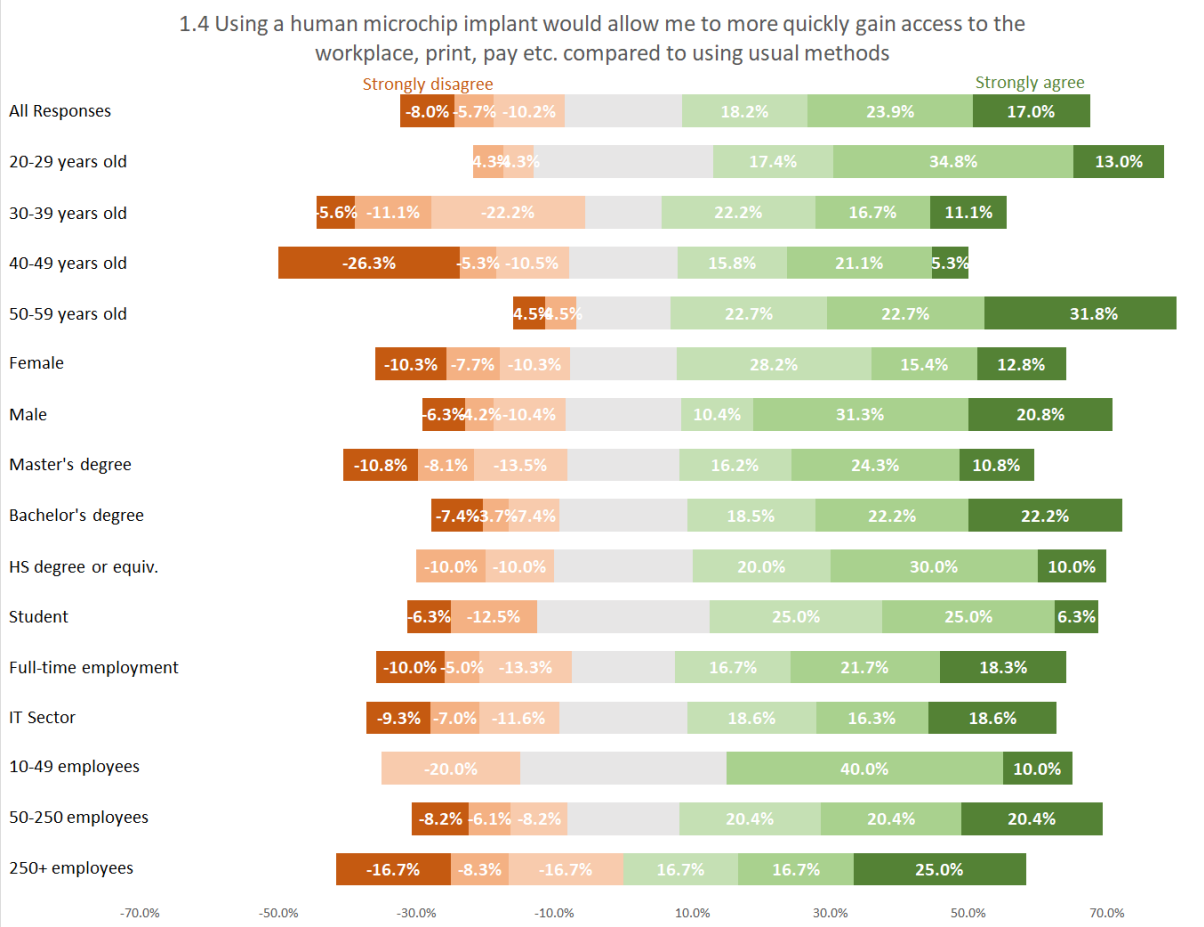

Figure A4: Diverging stacked bar chart showing all responses and demographic groups for statement 1.4 (own figure).

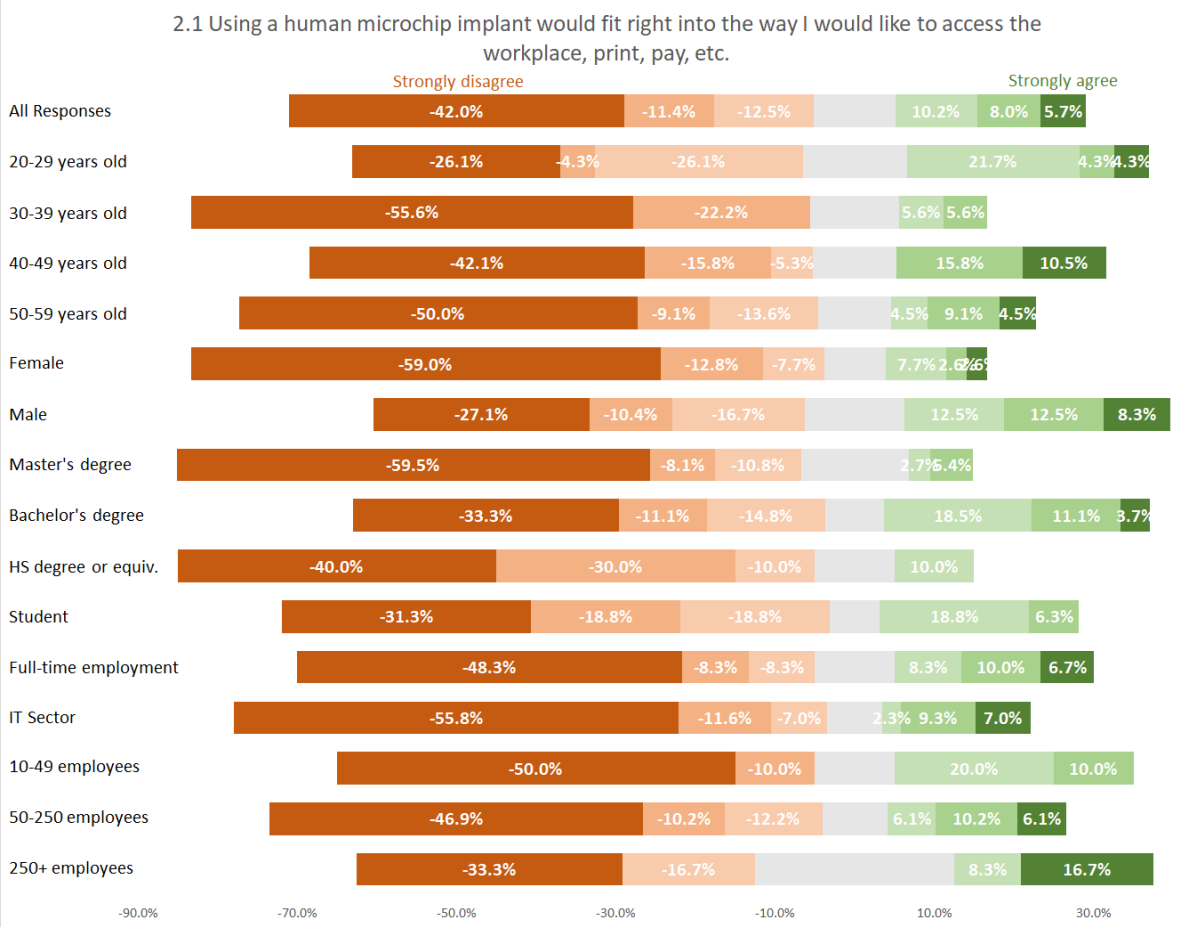

Figure A5: Diverging stacked bar chart showing all responses and demographic groups for statement 2.1 (own figure).

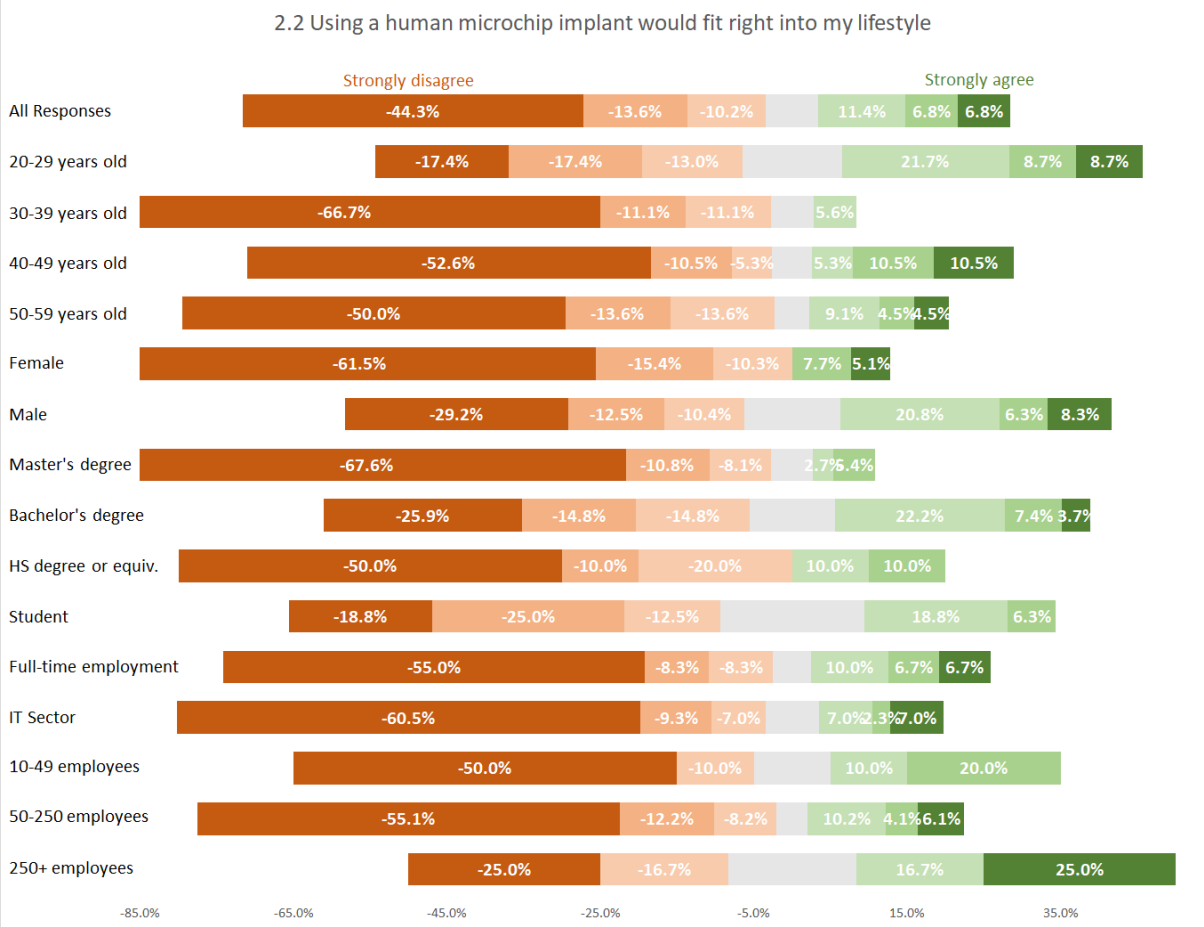

Figure A6: Diverging stacked bar chart showing all responses and demographic groups for statement 2.2 (own figure).

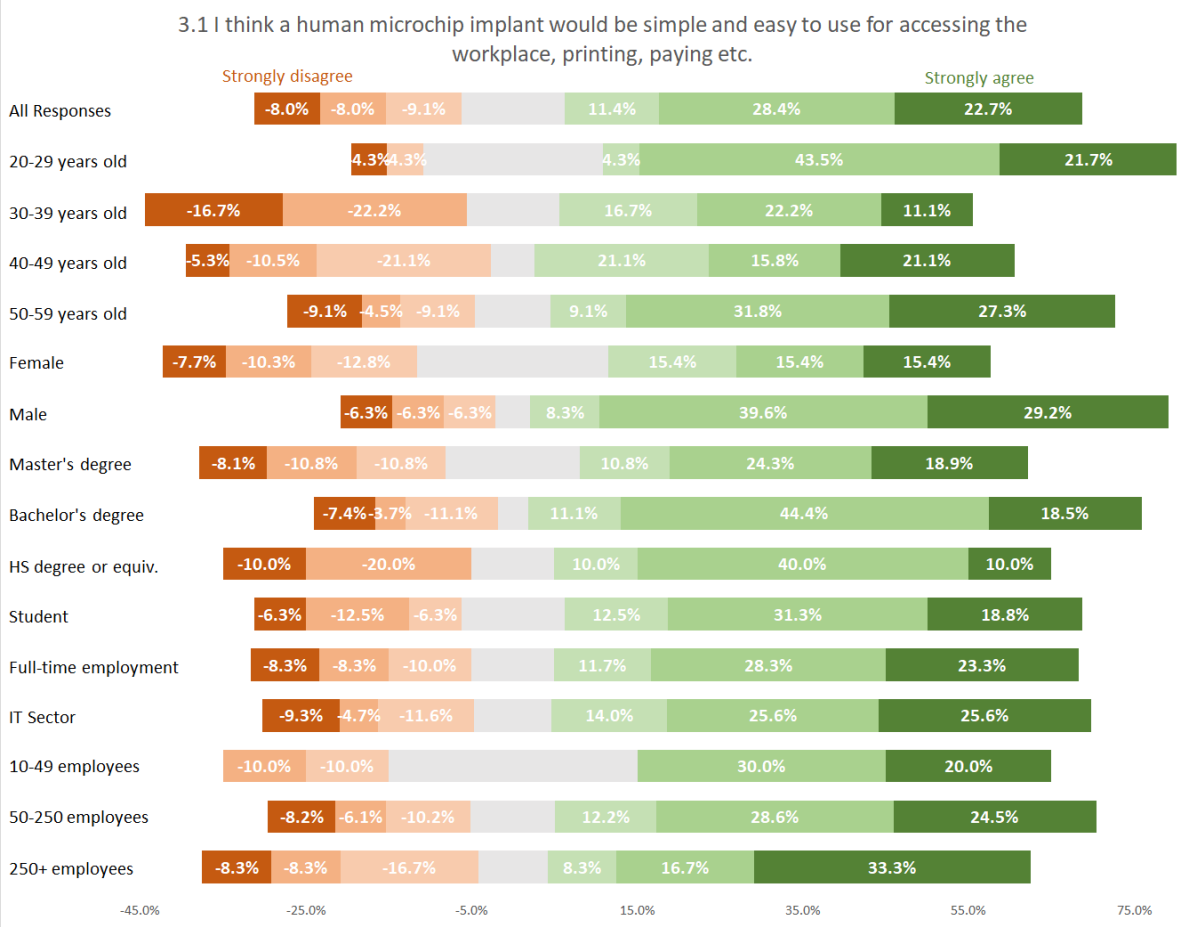

Figure A7: Diverging stacked bar chart showing all responses and demographic groups for statement 3.1 (own figure).

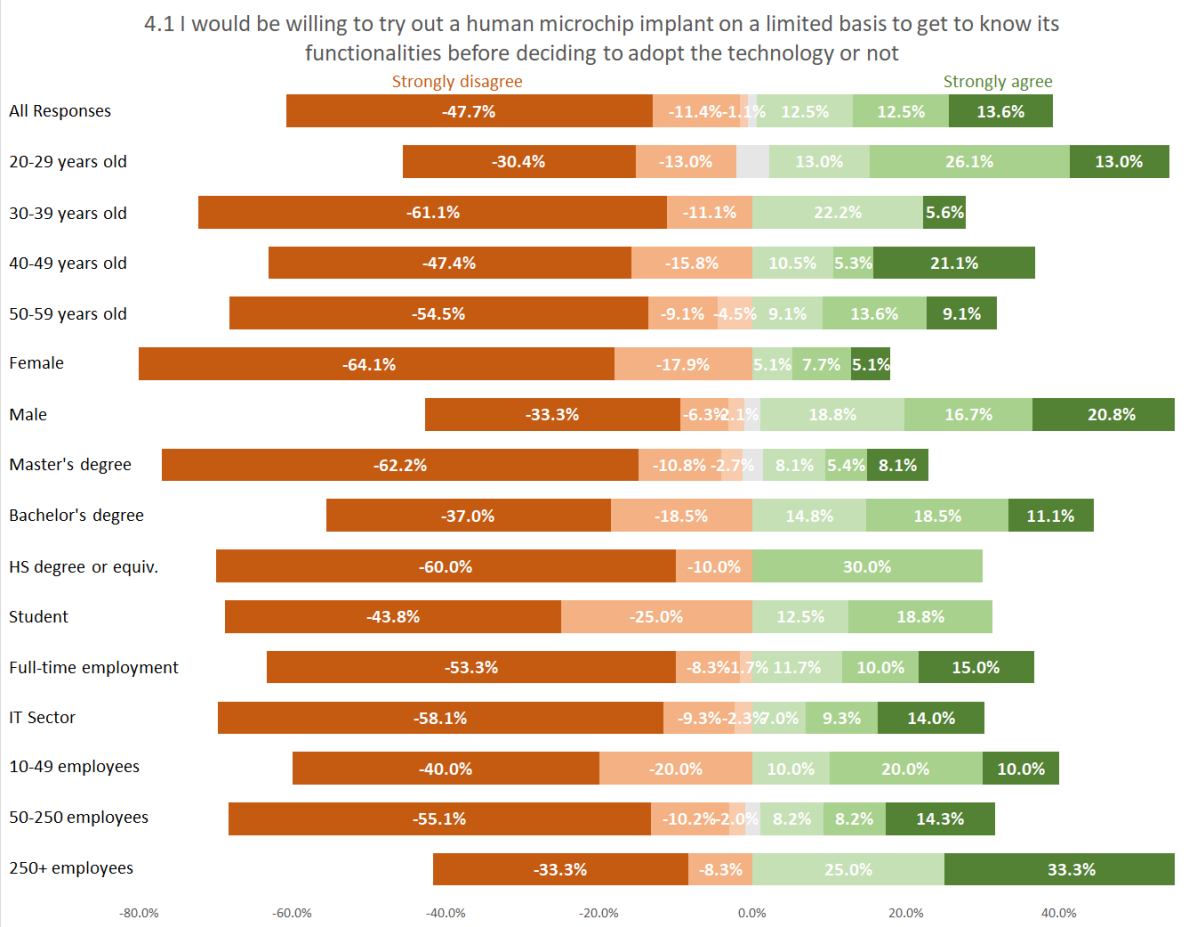

Figure A8: Diverging stacked bar chart showing all responses and demographic groups for statement 4.1 (own figure).

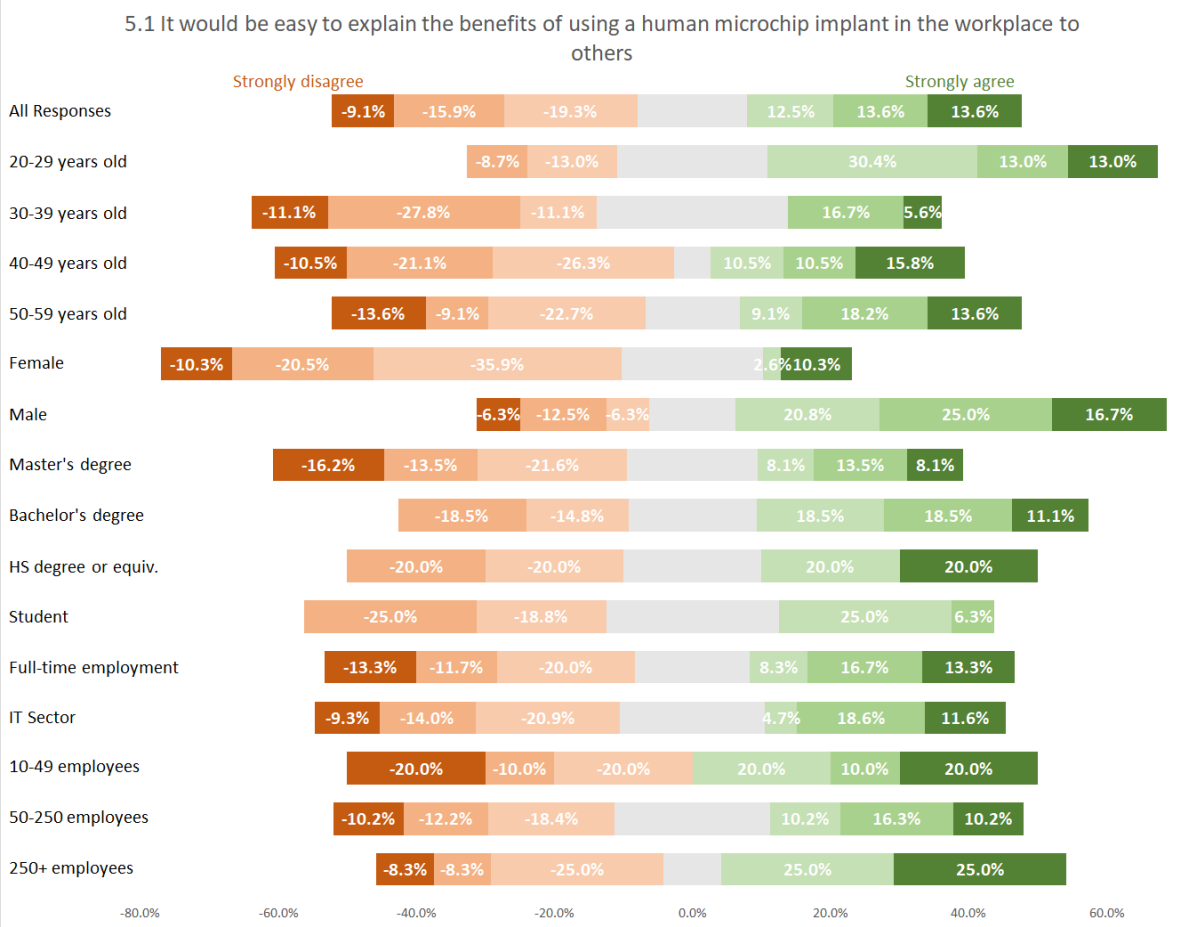

Figure A9: Diverging stacked bar chart showing all responses and demographic groups for statement 5.1 (own figure).

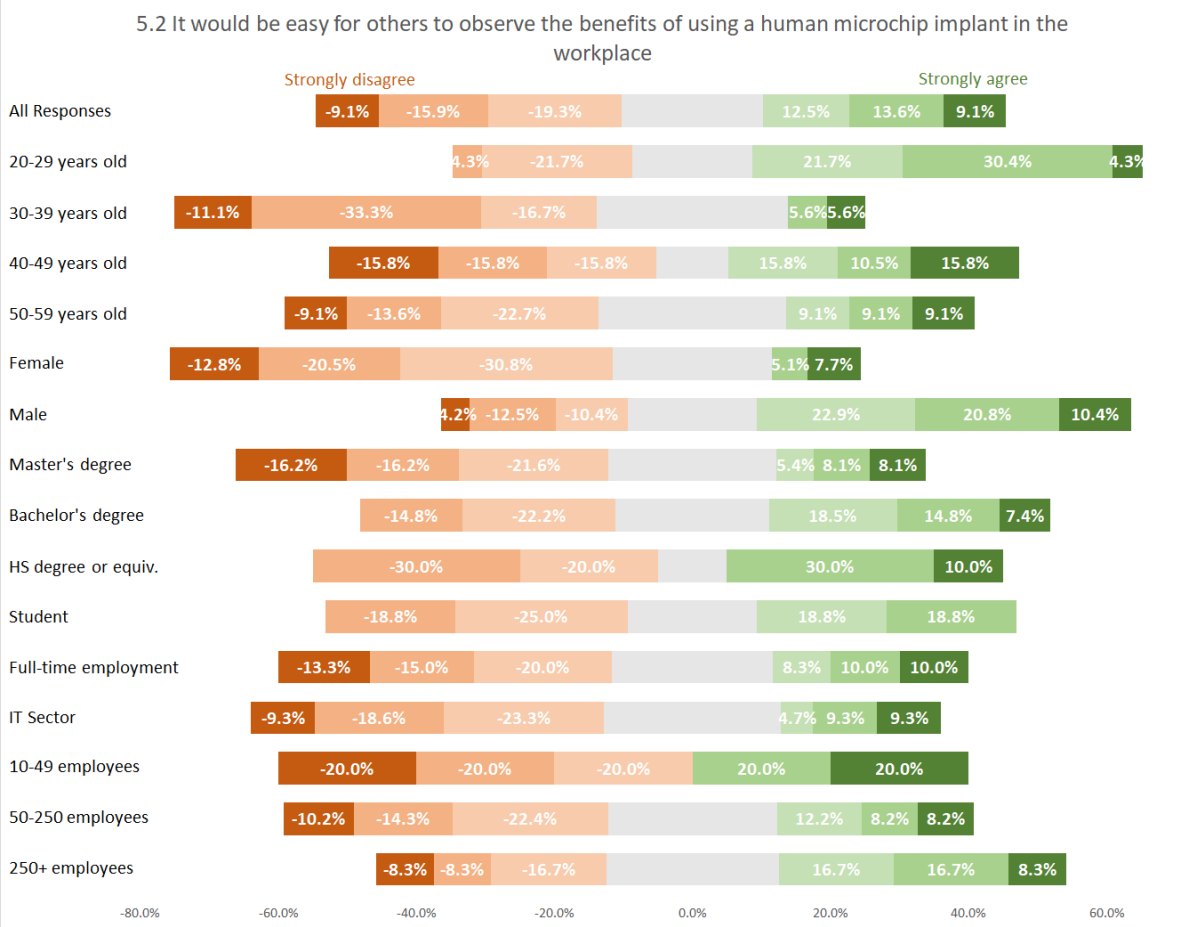

Figure A10: Diverging stacked bar chart showing all responses and demographic groups for statement 5.2 (own figure).

APPENDIX B. Transcript of Interview with TUI

Interviewees: Marc, Nikoline, and Alexander from TUI, who all have microchip implants
Date of interview: 06.05.19
Location of interview: TUI Office in Copenhagen

Interviewers: When and how did you adopt microchip implant technology? What is the background story?

Marc: From a TUI perspective, we adopted it about a year ago through a contact with Biohax who we have partnered up with. We have around 110 employees chipped, more or less. Around 100 of them in Sweden, 1 in Norway and we are 7 in the Copenhagen office. So we have played with the technology for more than a year, mainly in our Stockholm office, where they can use it for printers, entrance to the door, they can use it at the vending machines. I think it is quite different how much people are using it. And then, of course, we have a lot of colleagues using the train.

Interviewers: So it was in the office in Sweden who first set this in motion?

Marc: Yes, there was a contact in the company Biohax in Sweden known by our CEO, and it happened from there.

Interviewers: What did you guys think about microchips when you heard about it initially with Sweden?

Alexander: My first thought was why should I carry a chip in my hand when I have a chip in my phone, watch and everywhere else. And I still have that question, but I want to be a part of this technology because I think it is exciting that I no longer can forget my key. I always have it with me. I can lose my normal key card, but the chip I can always carry with me. So I can always get access to my personal belongings in the office and stuff. And I think it is just really exciting where it is going. What I can use it for in one year or two years or further on. So, there were some doubts, but there was also big excitement about what the future will bring.

Interviewers: Was it ethical doubts that you had?

Alexander: Not at all. I just did not want to have something inside me that I don't have a use for or doesn't add anything else. But I hope and think that the future will bring more possibilities.

Nikoline: I think it was the same for me. First, it sounded a little bit crazy.

Interviewers: Were you concerned about the chip being able to track you?

Nikoline: No, not really.

Alexander: No, because it was quite clear what the chip could and couldn't do. There was a lot of comments from friends and family about how they now can track everywhere I go. But it is not a GPS, that would take a much bigger chip. Explaining that, they understand a little bit better. But of course, you think this is the case in the beginning but once you get the information it is not so scary anymore.

Interviewers: Yes, that is a common misconception that we have heard as well. People think that the chip just radiates information to everybody. They are unaware that you have to be really close to the chip.

Marc: That is what we have experienced as well with the use of the chip. We have our lockers as well and the key card is much quicker because you really need to be close with the implanted chip, so it feels quite safe. But I think that our 110 colleagues are all informed and aware that the chip doesn't have much of a use today. But it may be more the view that if we don't drive the chance of getting a chip today then how can we influence the future. Now we have talked to guys like you today which is fantastic and we have had much more media coverage than we thought we would have, but that's the part of driving it further. Of course, it doesn't change anything for the three of us. Mainly it is seconds saved during the day, but it is more for the future. So if we don't try it out, then perhaps nothing will happen here in Denmark.

Interviewers: So you want to be the frontrunners regarding microchipping in Denmark?

Marc: Yes, I think we are called frontrunners or first movers by the media as well, and we are, but of course we are not the people coding and everything behind the scenes. We just have the chip in our hands using it for the stuff we can at TUI today, and maybe then whatever people bring up, then hopefully there will be some guys looking at the media or guys at university and think maybe we can use us for some apps or whatever it could be, and I think that would be the way forward maybe. We would have to test it but nothing more. Hopefully, more will get on.

Interviewers: Maybe we already covered this a little bit. But, what was the reason behind getting the implant?

Marc: For me, it is definitely fun. But also this aspect of looking forward. If we don't drive it, I mean today I don't have a big use, but if I can use it for something during the day then that is fun. Information technology is interesting to me. But it is more about the future, what comes and who can develop something that can make my day easier. I have a big wish that maybe someday we can pay with the chip and that could ease a lot of my day.

Nikoline: Yes, I think it was quite the same for all of us.

Alexander: I think also the possibilities that are there because we talked about in the beginning, I want to have it as something that can make my day easier and more convenient. It is the same question as to why do you buy the new iPhone when it can basically do the same thing. But you want to have the new thing and the new technology, you want to try it and learn more and I think it is the same thought behinds the chip.

I was at home, I come from Northern Jutland, close to Aalborg, this weekend, and went to a party and the rooms they hired were also opened by the small chip they have in the key, and for the fun of it, I tried to put my chip in front of the reader and that reader is already adapted to this same coding that I have in my hand, so we could technically code my chip to open the door, so that would be really fun and a big opportunity in the future. If I can install a lock, and I already could if I wanted to pay for it, but in my own home which would be much better than bringing around a key which I could lose.

Interviewers: The technology is out there, as it is similar to the RFID chips used in ordinary key cards.

Marc: Yes, so there is a lot of talk about safety, and of course it feels safer to have the key inside of your hand. Of course, they would have to take your hand, and that would be very sad if they should steal it but we are just ordinary people.

Alexander: I got a question on TV about what is the big dream I have about this, and big dream really is, and I carry around a cardholder and that just gets thicker and thicker, day by day because you get cards for so many things. If I could store all of that in my hand, and not have to bring around any card; credit card, member cards, access cards - then it would really fulfill a purpose to me. And that is my big hope about this, that I can include all of those.

Interviewers: Have you encountered any issues using the chips so far?

Alexander: I think it is the signal strength of it. Because, you know, when you swipe a card near the reader it registers immediately but with this chip, it takes longer because you have to find the right spot. It depends, some readers read it straight away. But, for example, for our lockers, it takes time to find the right spot.

Marc: And you feel it on mobile phones, too, when using the lockers. One colleague has a Google phone, which is really quick. The iPhone is okay, but it might also be the different technologies in devices, and so on. We don’t really know how great the signal is from our lockers. So if you know exactly where the reader is, then it might not be an issue. Some days

you hit the right spot and it opens straight away. Then on other days, you stand there for half an hour and cannot go home.

Interviewers: But that is something you think will become better in the future with better reader technology and whatnot?

Marc: Hopefully, yes. Our lockers were created with implanted microchips in mind. It is made for access cards. Hopefully, for the next iteration they will have thought about it.

Interviewers: Yes, perhaps the readers will become different taking microchips into consideration.

Marc: Right now, it is about learning where the sensors are and where your own chip is. I think all of our microchips are placed a little bit differently. I am learning the position of my chip and the direction to put it.

Interviewers: But aside from that, have you experienced any other issues, i.e. medically, annoying in the hand, do you feel it?

Nikoline: Well, you can see it and feel it all the time.

Interviewers: Can I see your microchip?

Alexander: Yes, I can press mine really much upwards.

Interviewers: It feels weird, haha.

Nikoline: Mine is a bit deeper down.

Interviewers: It is something you have to get used to, right?

Alexander: Yes, it is a little bit strange that you can feel it but there is no pain or anything. it is just like when you press your bones.

Marc: I was a little sore for a week, but that is it.

Interviewers: I must say you are brave.

Alexander: I compare it to getting a blood test in the hospital. When you come out, you can also feel it if you press where the needle was injected and it will be sore. It was the same kind of feeling with the microchip implant. Today it is gone.

Interviewers: What about overall reactions from media, friends, and family? How has that been?

Alexander: Huge. I think it has a big wow factor. Because there are so many questions and reactions. Some people are just like “what, how could you do that?”, others are like “I am glad that some people are trying it but I wouldn’t do it”, so yes it is different but you get a reaction from basically anyone. And, of course, it is a different reaction when I speak to my grandmother or young friends. But there is a reaction.

Nikoline: I think there were like 800 angry comments on our news coverage article from DR.

Marc: Negative, not angry. They were not angry with the chip but they were more afraid. Especially with the tracking aspect. Nikoline was on the radio where there was one from the union saying that TUI is giving the chip, but it is actually our own chip. We can code whatever we want and we can remove whatever we want, so it is not TUI who owns the content of the chip. Today, I don’t have anything coded from TUI. I don’t think any of us have. Because it is just our locker. So right now it is just personal. A lot of coverage has been about the future is coming. And mostly that is because, as we also read from comments on the news article, they don’t know what the chip can do and cannot do. They just hear something and then they think it can read anything and follow you around, and the bank can check if you are using too much money. They just don’t know what it can’t and can do. They don’t know how much an iPhone can and still they think the chip can do a lot more.

Interviewers: The chip can listen in on you, haha.

Marc: Yes, they should read about the iPhone instead. And all of those people who have commented on the news article have given their identity to Facebook.

Alexander: Yes, there is a lot of misconceptions out. I have been on TV a lot the last week and a lot of people I don’t know have written to me personally. There was one acupuncture who told me that it is dangerous for me since the chip sits on a spot that controls the digestive system. So people have been really worried. Some people said that it would leak liquid into my body, but there is no liquid in the chip. And the most common one was Christians.

Nikoline: Mark of the beast.

Alexander: Yes. There is this part in Revelation 13, which I started to read because of this. Yes, there is a lot of Christians, actually, that’s the most common one. They have written to me that now I am wearing the sign of the Antichrist.

Interviewers: I read a funny response to that. Since Revelation 13 says it is a mark on your forehead or right hand, so I can just put it on my left hand, haha.

Alexander: We all have the chip in our left hand. I usually don't comment on a lot of posts, but I commented on a post that said you cannot be sold or bought without this mark. I replied, I cannot be sold our bought and it is on my left hand.

Marc: But I always think that the positive side of all of the coverage we have in the media and so on, and you again being here, is about us just talking about new technology. Of course, it is one thing what TUI wants as a company and what we strive to do. Trying to new technology and being as digital as possible, but also just creating conversation. This is a fun thing to talk about. Either, people hate it or they love it, it is interesting in both ways, but it just creates conversation and that's really fun. And hopefully, looking at the company side, TUI also does it for the sake of the customers. We are a travel and service business, so if this could help us being in front in 15 years because we have some information. Then that could be fun.

Interviewers: So, for instance, they could check in or something?

Marc: Yes, of course, we are traveling a lot ourselves. Having that on my chip would be a lot of fun in the airport, and it would start conversations as people observed me using my hand. So that hopefully can help us. But, of course, that would need all of our customers to have a chip in the hand. But just having something made for the mobile, whatever it could be, there are many directions we can go with this.

Alexander: I talked to a reception manager from a hotel this weekend and he said that I could basically put the room key in my hand if I wanted to. And I mean, we sell holidays and hotels, so I mean, maybe not tomorrow but in the future it could be something that we could offer may be, to set us apart from other companies. I think it is interesting.

Marc: And if it doesn't become a widespread thing, then I won't feel like it is been a big loss. I mean, it did hurt a little bit and I do have a chip in my hand but, of course, it can be removed quite easily, as we have been informed. I feel anything odd, then I will just remove it. If it doesn't help me in 10 years and we hear the technology is out of service, then let's remove it and hopefully something else will replace it. I don't feel any consequences today.

Interviewers: What are the specific uses of the chip in the organization right now? Is it only the locker?

Marc: Let's find the full list, haha. We have lockers at our office, and we have printers. We don't print that much, but it is possible to access your account instead of logging in. We have entrance through doors in our Stockholm office. There are also vending machines which can be used with the chips. Basically, the first step is to remove the physical access cards. We don't have that many options here in Denmark yet. Alexander lives in Sweden, allowing him to use the railway also.

Alexander: Yes, so in Denmark, we have a smart travel card which can be used all over the country. But in Sweden, it is divided into regions, and you need a different travel card for each region. And I think it is two or three regions now which have adopted chips, which will allow you to load your travelcard onto the chip. Unfortunately, it is not in Malmö right now, where I live. But they are talking about it as well, so that would be quite fun to have that because then other people could see me using it in public as mentioned before.

Interviewers: So basically a tool with some fundamental functionality which you can use at the office, as you just mentioned, and somehow you can take it home and apply to some of your own private stuff. If you were limited to only using it at the office, then perhaps it wouldn't be as interesting for you to adopt?

Marc: Yes, so the first thing we got onto our chips were our LinkedIn profiles. I have LinkedIn and Instagram on my chip. That has nothing to do with TUI. We haven't signed anything stating that it needs to be used at TUI. If I choose to not use it at TUI at all then that's fine. TUI just invested in the technology. We have our CEO as well. He has a reader for his passwords now, so he doesn't have to remember all of his passwords. It is just connected to his chip. That was quite amazing, especially with then number of passwords we have today. I don't know how that technology is working, but that is lovely.

Alexander: But I think the most important and interesting thing about this chip is not happening in the office. I think the fun stuff is what I can do with it outside. And that is also why I said yes to getting it. It is not a TUI chip. It is not a TUI thing. It is a personal thing. And it is a personal development that I can then come back and share with my workplace, and maybe we can develop something together. There are so many possibilities outside and inside the office. I want to see progress outside the office because that's where it really gets useful.

Marc: And also if you look at what you can use it for. We don't use so much in our office. We sit with our laptops and that's more or less it. We are not going around opening stuff and buying stuff. We do that in our free time. I don't think it is created as a work tool.

Interviewers: The reason we are asking is that we are developing a solution ourselves with microchips and Internet of Things in companies. We are mostly concerned with what you can get out of it from a company perspective. For example, using Internet of Things and microchips for preferences within the office, such as air conditioning, temperature. Also just getting devices ready for you.

Alexander: So kind of like a car key that puts the seat the way you wanted.

Interviewers: Yes, so you will have a profile and an interface with some settings you can choose between.

Marc: Yes, then it becomes a work tool. That would be fun to see. Then I could have a cup of coffee being prepared as I move to the machine.

Interviewers: Yes, and also if you are in the canteen buying things, it could inform you about allergies if you are about to buy something containing these and these ingredients. So instead of being just a tool like a key card, it is more like an assistant.

Marc: I also think that is where it can create differences.

Interviewers: Yes, that is also how we can differentiate ourselves from other solutions.

Marc: Yes, that is also great. We don't know what the chip can do. We don't work with IT in our jobs today. So, on a big scale, what can we end up with? We just hope that one day it can be my VISA card or maybe it can be much better.

Interviewers: Yes, so if it can identify it is you, then you can set some preferences on how you would like it. So that is how we are moving into the future by combining Internet of Things with microchips.

Interviewers: So you don't have any concerns about privacy?

Alexander: I had one. And that is because I use Apple Pay a lot on my watch and phone. And when I want to buy something on my phone, I authenticate with my fingerprint or face ID. With this chip, I have no way to lock it so it cannot be read as I have on my VISA card or my phone. And that was one thing. Because I can dream about many things, but this is really hard for me to imagine how could I turn it off and turn it on. So that's a concern when thinking about paying with the chip. I wouldn't feel comfortable. Waiting in a queue for the train, a bystander could just put a reader on my hand.

Interviewers: You could actually put a password on there. You can encrypt the information and then you have a code. So before you can read my information, you have to insert this code. That is something we have in mind for our solution to ensure privacy.

Alexander: There is this app. Unfortunately, it can only write stuff to the chip on Android. There are basically lines where we can put different things on our chip, links, and stuff, mostly gimmicks. There was also this opportunity to do this with a line if you wanted to do that. But thinking about putting my VISA card into then I get more concerned. I mean, my LinkedIn profile or locker key is not the most important thing.

Interviewers: Can you explain the thing with the LinkedIn profile? How do you use that?

Nikoline: You can see it here.

Marc: On Android phones, it has a native reader already installed. But for iOS, you need an NFC reader app. Android devices just read the first thing you put on. I've put LinkedIn in first, so this is what will pop up when read. If you have the app, you can just read the whole thing and see what is coded onto the chip.

Alexander: There was also one function where you could put your health details in. And then you could basically scan it. Of course, if you put this in they can see your blood type, allergies and such. But at least what I heard, most hospitals will not start scanning you for a chip. They will be looking for something else. But in the future, I think it could be interesting as well to have that.

Interviewers: So if you want something on your chip, you use an app. Is that correct?

Marc: Yes. An Android app. But that is mostly to write in gimmicks and links and stuff. If you want to code it to become a key, you need this writer. For example, like the ones they have in hotels used for the access cards there.

Interviewers: If you have some issues with our chips. Or perhaps you want to apply some more solutions to it. Do you have a partnership with Biohax and do they act as customer support for you?

Marc: No, we don't. They just implanted it. If we would have that as a wish, I think many companies are trying to create apps to ease the use of the chip and so on. Then we would have to order something and then it would be just a separate case for that. But we don't have service or wishes like this, then we would need to buy equipment. The easy thing would be to buy an NFC reader connected to the laptop and we could do some coding or add something.

Interviewers: So you buy the components from Biohax? Or do you buy them from elsewhere?

Marc: They sell it, yes, for example. We have one in our Stockholm office since we have the majority of people there. But yea, it could be any NFC reader. We don't have any agreements, so we should fix it ourselves.

Interviewers: We are asking because we were also trying to get an interview with Biohax since their name keeps popping up.

Alexander: I asked the CEO of Biohax when he was here to chip us how many people he injected. He said he didn't have the exact number, but at least 5,000 people. So it is quite a lot of people, that he personally chipped. Mostly in Sweden.

Interviewers: So, Alexander, now that you live in Sweden, why do you think Sweden are frontrunners?

Alexander: It is a question for me as well, and I don't have the answer to it. When I first moved to Sweden, I thought Denmark was all about not using cash anymore. But once I came to Sweden I realized it is, even more, a case there. They are a lot more adapted to the future with no cash and access cards. In Sweden, you see all offices using access cards, but in Denmark, many offices are more open. I don't know. But I see it all around. They are really adapted.

Marc: I think they talk more about digital innovation in Sweden, be it companies or politicians.

Interviewers: So they are not so conservative about new technology?

Alexander: Yes.

Marc: Yes, and I guess if Biohax were a Danish company then maybe the technology would have developed more in Denmark. It is also about finding 5,000 people who want an implant.

Alexander: I think they are also great at explaining technology in Sweden. For example, my grandparents here in Denmark still have problems with figuring out NemID. Then they cannot authenticate on their phones etc. Whereas in Sweden, when I am with my girlfriend's grandparents, they have something called BankID, and it doesn't feel like they have the same concerns. They just use it with ease, because it is really simple. They explain it very simply how to use it. I don't think the older generation in Sweden has the same concerns as the one in Denmark. And that seems like the big blocker for us in Denmark. We can change, but we still have a generation which won't adapt. Whereas in Sweden, they adapt a little bit faster, but also because they are better to inform about the technology. In Sweden, they have this Swedish way that you cannot say something if everybody doesn't understand it. So instructions in Sweden can sometimes be too much and seem unnecessary, but it is not unnecessary. There will always be people that don't learn so fast. That's one reason I think it is going faster in Sweden.

Interviewers: It is also a pretty early stage for this technology, so it is also pretty interesting to have this discussion right now. And we also think it is pretty interesting and cool that you are sort of pioneering this technology. You almost make me want to get a chip as well. We have actually bought our own chips also, but that is only for testing purposes. We won't inject anything.

Alexander: Yes, so when the CEO of Biohax was here we asked him if a private person approached him for a microchip. And the first time you see it, you are thinking that it must be really expensive, but it is actually not. He said he doesn't really have a price for private people since that is not his target group, but that it would cost around 2,000 SEK. So it is not super expensive.

Interviewers: Do you have any data about what kind of chip you have implanted into you? Such as the model number and manufacturer?

Marc: I don't know if it says when you read it.

Interviewers: Anything about the standard they are running?

Alexander: There was one guy who wrote to me, some tech guy. Let's see.

Nikoline: I have no idea.

Alexander: No, I'm not sure.

Interviewers: But the phone is pretty good at reading the chip, right?

Alexander: Yes, it is.

Marc: The locker is worse, haha.

Interviewer: Do you see this technology as something that is accessible to all kinds of people? Do you need any technical know-how?

Marc: Today, yes.

Interviewers: Or is it only a matter of finding the right people to put the data into the chip for you?

Marc: I think, as it is today, if a person doesn't have any interest in IT or technology, I think they would just get it and never get something on it. Because today there are no services. Yea, just download this and you can get all of those things. You can just code it with those readers as we are doing. And that would require you to do it yourself. But hopefully, that's something people will pick up. The companies should be able to do this much easier. But yes, maybe if it should be for everybody, I think some public services would need to adopt the technology so we can have some healthcare or something. I don't think it will be a requirement for everyone in Denmark to have an implant. I think that is asking for too much. And I don't think it will be a requirement at any company, either. If you work at our place, we can provide you with a chip.

Nikoline: But I don't think you need a lot of IT knowledge. If you can just get someone to help you put something into it. I don't know how to code. I just got help to do it. So I don't think you need to know much about it. You just need help to put it on there.

Alexander: It took a few seconds, and I have this video from this weekend showing how you can unlock a door using your chip. So if you have this function, my grandmother could use it as a key to her door. When you spend the 10 seconds to program it to do that, you don't need

to know anything. You just need to know how to put your hand onto the reader. And, I mean, if it gets that easy, then I think it will be for everyone.

Nikoline: It is exactly as if you get a key card in your hand. The user will know how to use the key card.

Marc: Yes, you just need something to put the stuff onto the chip for you, and then you are fine.

Interviewers: Do you believe, in the future, all of TUI's employees will have embraced this technology?

Alexander: I don't think so.

Nikoline: Yes, there will likely always be someone who doesn't want it, of course. I think if it gets more functions, a lot more people will get an implant.

Alexander: When, for example, e-Boks came to Denmark, a lot of people had to receive their post digitally. There were a lot of people who said they would never want to do that. And then the government kind of tried to enforce it, unless people were at a certain age. So unless people are forced, I don't think you will ever have a technology which everybody wants to accept. I think today e-Boks is accepted and people like it now. But in the beginning, there is of course, always some people that are reluctant.

Interviewers: Is it everyone who is offered to have this chip injected within TUI?

Alexander: Yes. And also part-time employees, I think. People working here for 5-10 hours a week could also say yes.

Interviewers: Cool. Well, that's it. Thank you.

APPENDIX C. Transcript of Interview with Dangerous Things & VivoKey Technologies

Interviewee: Amal Graafstra (CEO) of Dangerous Things and Vivokey Technologies
Date of interview: 10.05.19
Location of interview: Online

Interviewers: First of all, I want to hear something about Dangerous Things. What is the story behind it and why did you embark on this endeavor?

Amal: Sure, so essentially, in 2005, I got an implant in my left hand and started using it for my own uses: getting into my office, eventually starting my car, unlocking the computer, that kind of thing. So, that was all well and good but some people found out and then some blog posts about it and then a lot of interest came. But most of it was interest in terms of wanting to know why and not really interested in wanting to follow suit. So that was fine and then around 2009-2010, somewhere in there, the maker ethic and market really started to pick up. People starting making their own things again and getting into electronics. By 2013 there was a lot of interest in RFID in the hobby market and, of course, then people were like “oh this guy put a chip in, that seems kind of interesting”. So a lot of interest started coming in, and I had to decide if I was going to just ignore it so I could do other jobs or if I was going to try to, you know, do something with it. So I decided to start a store, and it was just a store based on my personal website, and then I quickly realized that this wasn’t going to work so I then I ended up saying well what would be a funny name for kind of a biohacker, bleeding edge technology, so I thought well Dangerous Things is kind of fun. So I bought the domain from somebody who had already registered it and then set up a store and that was it.

Interviewers: What is the current and future role of Dangerous Things in terms of biohacking, as you mentioned?

Amal: Dangerous Things will never be more than a retail channel for specific types of products. In 2018, I started a company called Vivokey technologies and that company is really about bringing implants beyond the simple NFC transponder or RFID transponder that you would use in a personal scope. I call these products that Dangerous Things provide personal scope products. They are not really secure enough to use for a global application or a business use case or something like that. They are personal scope device, so it doesn’t really matter that the xNT chip isn’t secure if you’re using it on your front door only. And there is no in between, right.

Interviewers: Can you elaborate on this? When you say personal scope, do you mean that it's combined with IoT to provide personalization and to recognize that it is you, for example, entering the door?

Amal: No, not really. I mean, personal scope could be that. Present your tag to the home automation system and you know and everything gets customized to you. There is no real danger if someone pretends to be you in that scenario. What I mean is like authenticating to websites, proving your identity, cryptographically, you know, those kinds of applications. So in VivoKey, we have two products, one is called VivoKey Spark and one is called Flex One. The Spark is already available.

Interviewers: Is that the beta version one you have on your homepage?

Amal: No, it is not the beta version. That is probably the Flex. The Flex is in private beta right now.

Interviewers: But those chips have like a different form factor to it right?

Amal: The Flex has a different form factor. The Spark is a standard 2mm injectable. The difference is that the Spark has AES encryption built in. And we have pre-personalized them with user keys and other settings that will work with our web-based platform. So one of the differences is that Vivokey products are meant to interact with our platform and other services online, they are web-connection devices. Much more similar to IoT devices.

Interviewers: Do you see an increased interest in this kind of technology globally and domestically?

Amal: I think so. I mean, at least I can see that our types of customers are changing. Early customers for Dangerous Things were very technical. They just wanted to buy the widget, right, the thing, and then do their own with it. The kind of customer that is coming to us now is more is what I would call the Apple type customer. They just want to buy a few things and make it work.

Interviewers: So sort of the early adopters?

Amal: They are kind of early adopters, yes. Were they programmers and developers, no. You know, they want to be able to say what three things do I need to buy to lock away my stuff and get into my house. They don't want to have to build their own thing. And I don't blame them, right.

Interviewers: So that's where you provide the access control unit and so on?

Amal: We do, but again, even on Dangerous Things, it is just the controller. You still have to wire things up. It is sort of a component you can use to further your project. That is not really what we want for Vivokey. SO we are not only working on the platform and the web, API and cloud integration, but we are also working on a line of hardware that we will be able to just plug and play.

Interviewers: So Vivokey is up and running?

Amal: Yes, so we have Vivokey.com, and our API is going to be published probably next week and a new APK pushed.

Interviewers: Cool. So, specifically for Dangerous Things. What are you providing your customers?

Amal: Yes, so we have RFID technology, and it is up to the customer to figure out which chip they need, buy it, and figure out what they are going to do with it. There is no real plug and play solutions that Dangerous Things sell. We sell components that you can kind of put together to make your own thing. But if you are not able to do that or don't want to huddle together your own stuff, you just kind of have to wait for Vivokey to come out with our full line of hardware and different solutions. So you know if you want to buy, for example, some people want to clone their work badge to an implant. Well, the question is then is that even possible, what technology does your badge have, what implants do we have that might be able to do that. There are so many questions to lead to an answer, so there is a lot of overhead in customer support and trying to figure out all of the stuff for them and then the actual action of cloning the card to the implant. Everything is a big technical support nightmare.

Interviewers: Is it mostly private customers or also businesses?

Amal: Yes, we have seen that. Some companies take in the initiative to do that, and they have already figured out how to apply it to their solution. We have seen bulk buys from companies, you know, 10-20 chips. But it is not a phenomenon because there is a high technical bar and there is a lot to figure out. So it really all comes down to if we want to start supporting enterprise, then the best channel for that is Vivokey.

Interviewers: Do you send people out to enterprises to install things?

Amal: No, so that is not really a thing. We have had chipping parties and stuff, but it is not a regular occurrence by any means.

Interviewers: Can you describe the sentiment Dangerous Things has received in the past and up until now?

Amal: Yes, so it kind of mirrors my own experience. In the early days, the reactions were very negative and not a lot of curiosity by the public. But then it changes, like the mere-exposure effect. The more people hear about things, the more people start to develop a preference for it. Over time it changes and reactions are less visceral and more accepting. Even though they don't want to do it, they are not opposed to it.

Interviewers: Why do you think people were opposed to it?

Amal: Same reasons as people are opposed to other new things. They don't know anything about it, so all you can do is make assumptions at that point, and all the assumptions are bad. That is just how human beings work. The concerns are all based on assumptions which are wrong. You know, "I don't want the government tracking me with a GPS chip". None of those things are accurate. GPS tracking, no. Government involvement, no. There are just so many wrong assumptions. Mind control chips, I have heard it all. And these are legitimate concerns, not by crazy people. "What about when they turn the chip off?", well, the same thing is true when you freeze your bank account. The risks to you are the same, there is no difference in the threat models. The only difference is you are just logically moving something from your pants pocket to a skin pocket, that's it. It doesn't matter if you throw your bank card away. If you throw the bank card away, you are still not using it. That is the point. And when you use your bank card, you give up all of your information about where you were, what you spend, what store you were at, time of day, all of that stuff goes to a ton of companies and you don't bat an eye.

Interviewers: Yes, so it is the same with the iPhone, right, with sharing GPS location and what not.

Amal: Yes, absolutely.

Interviewers: What about Christians, they also seem to be opposed to this idea?

Amal: Yes, so Christians are concerned about the so-called mark of the beast. I used to get into these philosophical debates about it but it is really irrelevant so I the only thing I say now is for them to read the passage extremely literal with your interpretation, so let us take it to the fully literal conclusion. If you put our devil microchip in your left hand, you will be fine because it very clearly states right hand or forehead, so you can take all of it or none of it, right. You cannot split up the bible and say that it is any chip anywhere in the body. It is just fire with fire with these people, and a lot of time they just disappear.

Interviewers: Is that why you carry your chip in your left hand because somewhere you don't want to start a debate?

Amal: I have six. They are everywhere. The first one went to the left hand because I wasn't sure how long the healing process would take and I was right-handed, so I just didn't want to mess with it. The healing process is nothing, so I was using my hand immediately. A month later in 2005, I put another chip in my right hand.

Interviewers: I will likely get an implant one day, but only when it gets more commercialized and more services are available, I think.

Amal: Well, the Vivokey Spark is available now, and that's the point. This is the beginning of service integration. If you get any other chip, the utility of it is going to plateau at some point. Maybe you will be able to change the lock on your door. Maybe you will be able to hack something together for your computer. There are a lot of maybes there. But Vivokey, if you get the Spark, we are going to come out with more services, we are going to come out with hardware that works with it. So it is really not just buying a thing and then trying to make it work with others. When you buy a Vivokey Spark, you are kind of joining the Vivokey community. Immediately, you are going to get some benefits, and then as we develop different services as a community, you will get those benefits as well. Right now, we have a Vivokey forum that is closed to just the private beta customers working with the Flex. We are considering to open this for Vivokey Spark users. So, unless you have a Spark you are not going to be able to get into that community, and that is just one element.

Interviewers: What kind of functionalities and services are the most appealing to your customers?

Amal: I think it just getting rid of your management burden. Your daily management burden is phone, wallet, and keys. That is the three main burdens you have to deal with. And if you think of everything from patient compliance for medical devices to people buying Fitbits. If you add to that burden another element: also my watch, my Fitbit every day, make sure it is charged, make sure I get all of the data off it. It is a management burden that doesn't always result in 100% compliance. Something you forget your wallet, sometimes you forget your Fitbit. So when you keep adding all of these elements, you will start to see a drop-off and this is why when people buy Fitbits, around 50% of them end up in the drawer after a few weeks and is never used again. And the reason for that is the management burden. So that is what the chip can help with. And eventually, we will want to replace the wallet also. If a chip can do that, then you have just reduced your management burden by at least one-third if not two-thirds. So the idea is really about convenience, but in a way that always you to move through digital and physical environments with the same ease of just walking around right. You don't have to manage all of these things. You can just to websites securely. Prove your identity securely. Hopefully one day you will be able to travel and pay securely.

Interviewer: Yes, it would be cool to have your passport, driver's license and so on a chip in the future.

Amal: Yes, so the idea behind this is basically right now if you think about all of those things you mentioned, and every key on your keychain, and every card in your wallet, they are all identity tokens. They represent you to some system. But it is up to you to manage all of these tokens. So you get a driver's license, that is issues to you as a token, that represents you to the police when you are driving and maybe in some identity situations. But all of these things require you to be the manager, so what we want to explore with the Vivokey is the idea of bringing your own identity. So if a person shows up with a Vivokey identity, that is secured, you can either issue an app to the Vivokey system to be able to interact with whatever it is you are doing, so building access and employment cards. Or we can actually enable our platform to integrate with yours so that the identity is transferable. So basically, I show up, I can prove my identity, I can get access, I can do these things, and then when you no longer need me in those systems, you can just remove my privilege. But you are not managing an identity a token and neither am I. It is all tied to the same identity for me.

Interviewers: Do you have anything to consider or comply with in terms of data protection such as the GDPR with these?

Amal: No, not really, but this is the responsibility of the concerning party. Meaning it is not a problem for the Vivokey member with the chip to do that. If I bring my identity to your service, your website, your building, your company, and then I want to be removed from that. Then that is the responsibility of the other party. Not the person with the Vivokey. So really, those laws are good, but they don't affect us. They affect the people you interact with.

Interviewers: But you wouldn't need to have some information stored about your customers somewhere?

Amal: Yes, so basically we have government-proved identities as a verified or validated identity. So in say a bank scenario you have money laundering laws and know your customer laws. So we would the same and then we would vouch for the authenticity of the identity when you bring it to our service, web service for example. So how would GDPR affect us, it would be if a customer said to us that he is removing the Vivokey and that he wants out of the whole thing. That is fine. You can do that. And that is going to be a no-brainer, but we don't keep a collection of, for example, we wouldn't keep a collection of places that you have brought your identity to. So we wouldn't know if you went to work for whatever. We only say this chip is this person, and we are validating that identity for whatever service they bring it to. So really the amount of data we have per user is extremely slim, and that is by design. All we care about is

validating the authenticity, cryptographically, with your identity with whatever service you want to bring it to.

Interviewers: Are there any limitations on the chips in terms of bit size and so on?

Amal: Yes, so that is a different idea of. That is a very kind of archaic way of approaching it. Essentially what you are proposing is that it is a keychain and I keep adding keys. But that is actually a very inefficient way to deal with it. It is still not bring your own identity. It is bring your own keychain. We don't want that. We want you to bring your own identity. So the idea being, I can prove my identity, cryptographically, using different protocols or whatever. But it is still my identity. You as a service accept that identity. Not issue me a new one. It is going to start somewhere. So the idea with the Flex exactly is that it will function with our platform but you can also add applets, so companies that aren't ready or services aren't ready to integrate properly, they can issue an applet and you just carry around the issued token with you. But it is not the same as bringing your own identity. And the benefits won't be the same either. There is still a requirement for those services to do their own verification on your identity, your own money laundering law verifications. It doesn't benefit them to do a halfway implementation. They could do that, but it is not what we are shooting for.

Interviewers: So what you are shooting for is basically that it works as a passport almost?

Amal: Yes, sort of. It is like a cryptographically provable public key. Instead of saying I am going to copy your name and passport number and birthday, and then you need to present your unencrypted static data to then verify it is you, that doesn't work. But what does work is saying here is my public key that I retain the private key for, and I can sign any request that comes to it. So when you present your Vivokey identity to a door or an employer, you say hey, I want to apply for this job, here is me, public key. And the employer says great, I want to get your identity information from Vivokey, they will submit that public key, we will then contact you through our app, push notifications, person XYZ wants to get verification of your identity: scan to verify. So when they scan the chip, we say here is the identity information but we sign it with their private key for that public key upon which it was requested. So now they know, okay here is the static data that they have required and we are vouching for it. And all of that is signed by you, the person bringing your identity to that organization.

Interviewers: What kind people expect from human microchip implant technology in the future?

Amal: I would hope that there is a future where we want our Vivokey members to be kind of considered to be trusted. So if you are a business and you're dealing with a Vivokey person, who can sign their purchases. Yes, this is me. I am authorizing the purchase. I have signed it

with my Vivokey. These are important things. So right now you have these things like DocuSign, where you have a contract, and I am going to sign that electronically. How do you sign it? Well, you type your name out. Anybody can do that. It is really ridiculous. So, you know, just the simple idea of contract authorization, even if it is a printed contract. But if you get into something like Blockchain, where you are saying now I want to interact with a Blockchain contract.

Interviewers: Is Blockchain a part of your solutions now?

Amal: This is not something we are doing yet, but we will do. The blockchain aspect is right now is simply that you can deploy a Blockchain wallet to the Flex. So that is it. It doesn't interact with our platform.

Interviewers: Can you talk about the flow information and architecture of your current solution?

Amal: Basically, the flow on the Vivokey side is all patented and everything. But when you are talking about the Dangerous Things products, the xNTs and so on, there is no flow. And that is part of the problem. There is no encryption. There is no nothing. And if you try to use one of those types of chips for those applications then it would be a massive security hole. You have the most amazing encryption-based vault in the world, but if the key that opens it, you know, you poke a button, really, cause that is the level of difficulty we are talking to emulate and xNT or something then it doesn't matter. So that is the issue. There wouldn't be any real utility.

Interviewers: What about the incorporation of personalization?

Amal: That is all dependent on the other things and not the chip. I don't know if that is something we will ever really offer. And the reason for that is that idea, well there is going to be some logic that we will apply to open the door, unlock the computer, all that stuff. It is like the idea of saying I want to create an access control system. The amount of detail and specific application developments for that, yea, anybody can make a door lock. But when you talk about integrative services, the complexity of that door lock grows exponentially so it needs to be a door lock that now also has a safety egress. So if you are inside the door you can still get out of the door. There needs to be power backup and data service backup in event of a power or network outage. There are so many details to consider for something that just seems simple. So the idea of integrating lights, computer login, get the coffee pot brewing, the amount of detail in a giant cloud of services is exponential. So it is outside of our scope for now and it probably always will be. But what we want to do is say hey if these companies want to integrate with our identity platform to do that is great. We could trigger events, we could do these kinds of things, but we wouldn't want to be the ones providing the light and so on.

Interviewers: So, for example, some integration with a web-based solution combined with IoT?

Amal: We could integrate potentially this and that. Finding ways to be able to link these things together. Even in IoT, no one tries to do it all. It is just too complex and crazy to also include this for us. Too big a chunk to undertake. We just want to be able to say without a doubt unequivocally this person is the person they say claim to be. And who they are talking to might a door, a web service, a bank. That doesn't matter. We just want to say we know this person.

Interviewers: Are there any reasons why you are specifically using the xNT chips etc. And for the Vivokey side of things, are you manufacturing the chips yourself or?

Amal: Yes, so we develop everything ourselves, design, and then we have an assembly factory to put together our stuff. We don't own the factory, but we definitely don't do Turn Key production. I have tested Turn Key productions from all over the world, and most of them in China of course. You have these material issues, half of the batch will be okay, the other one not. Oh, it didn't work. These are human safety issues. There is just not any quality assurance when you are buying from these vendors. So we have always done our own manufacturing, and that is a little more expensive.

Interviewers: Also with Dangerous Things?

Amal: Yes, so for the xNT chip, I don't know if you have seen it on Indiegogo, but we crowdfunded manufacturing of that. So, the actual silicon chip is from a company called NXP, and they are probably the number one silicone chip manufacturer, but that is where everything ends. So we buy the wafers of those silicon diode chips from NXP, then we buy the glass, we buy the epoxy resins, we have that all assembled together by a factory Whereas some of these other suppliers in Europe just buy it off of Alibaba. So, you know, the human body is very resilient, it can put up with a lot of stuff. But you might put in some glass that is, you know, has led or aluminum contaminants, and it is not going to irritate your body to the point where you go "wow, my implant is very pissed off, I should take it out" but it will leech those materials into your body. The effects of which are subtle. Or the glass could be fine, but the epoxy resin inside is highly toxic. So if you did break it, then you would be in real trouble. So there are all these elements that all matter. Even in terms of the internal components, we ensure that the stuff we put together is run through sterilization internally before we do the external sterilization. So if you break it open, one of our implants, and test it for pathogens, it will be negative. Because it is sterile inside and out. But some of these other ones might not be. So not only could you have maybe toxic epoxy resin leaching into you, but you could also have actual infectious agents in there. These are big questions.

Interviewers: So that might also affect your business, right, if something bad happens with the bad chipsets?

Amal: Yes, so most of those things that could happen, typically are not noticeable. Some people get infections, I have seen that before with some of the competitors' chips. We have seen them break as well. There is different robustness of glass integrity wise. So if you get cheap glass it will break. We have seen competitors chips break. None of ours have. So it is irritating, but all we can do about it is to make better technology Vivokey stuff. Platform integration. Things that aren't just buy something off Alibaba and compete with me.

Interviewers: Yes, so people may start injecting themselves with these chips, which sounds dangerous?

Amal: Yes, and that does happen. We tried to build a partner network of professional piercers to do these installations, and actually the two companies in Denmark and Sweden, that are competing with us, with this Alibaba stuff, they were our partners originally. We worked with them. Several of the body modifiers that we worked with started their own business selling and injecting these chips, becoming my competitors, buying cheap knockoffs from China. Even using my actual medical data, an x-ray, as marketing material. Very irritating.

Interviewers: Do you see the biggest potential of microchips in the workplace or for the individual people?

Amal: It is always going to be private and the reason for that is even if it is through enterprise, it will always be private. There is no scenario in which I think it is prudent for a company to deploy microchips to its employees wherein the company retains some sort of ownership over it. Even if the companies purchasing the chips, deploying them and using them in their environment, in their enterprise, it is always still going to be the user, the person who is chipped, their property. So it is critical that these enterprise deployments consider it an employee benefit, just like giving an employee a bonus. A benefit like a phone, it is still an employee phone. You have given it to an employee. And that is the important aspect here. So, in that respect, you might find utility in the enterprise for chip implants that the company paid for, but the real benefit is for the individual.

Interviewers: There will never be a scenario where a company offers you a chip which you cannot use privately, right?

Amal: Right. That is a terrible idea.

Interviewers: Have you been assured of medical safety of the chips? Are there any concerns we haven't talked about?

Amal: Well, so what I can say is this. The medical safety of the chip has been proven to me by not only the tests we have done but also by the billions and billions of test animals that have had these chips put in them for decades. The materials used in those chips are the same. The glass that we buy for our implants is the same glass that is used for pet implants. The epoxy resins we use are medical grade USP class 6 approved resin for permanent implantation. We know the materials that we put into devices and we know the history of the materials. We have performed tests on those finished products. So in no way am I concerned about the safety issues surrounding these products. Where that changes is when you something completely safe, but have it installed or implanted incorrectly, leading to other issues, right. So if somebody justs stab it directly into their body. They put it in the deep muscle tissue or something, that could be bad, right. Those situations would create an issue. And that is always the case. So one half is the device itself, and the other one is the installation. So there are two things. That is why I started Dangerous Things in the first place; to deal with those two issues. One was making sure the stuff we sold was safe. And two was to create a procedure guide and partner network so that these people could get them installed safely.

Interviewers: So the reason I am also asking is that we stumbled upon some articles talking about different issues.

Amal: I am assuming you are talking about the cancer research related to these. Yes, so, that all tracks back to one person. Katherine Albrecht, who wrote the book Spychip. She has a financial interest in raising concerns about chip implants. The three medical papers that she references are not available anywhere since they have never been published. They reference tumorous growths around implants, but the primary thing about those studies, is that they were studies not about chip implants, they were cancer studies. So one set of animals were pre-determined genetically to get tumors. Another set of animals were given tumor-inducing drugs. So those animals were always going to get cancer. The finding that was worthy of a small footnote, was that there were tumors surrounding the chip implant. But if you know anything about cancer, and how the chip implants work particularly in lab animals and pets. Animals have very loose fascia tissue. So you need something around the chip to allow the tissue to grow into and hold it in place so it doesn't move around. That is called an anti-migration coating. That coating is very porous. Your tissue grows into it. And then it sits there and produces inflammation throughout its lifetime due to the coating. Our chips don't have that coating. Because we don't have that coating. It is just smooth glass. Our human fascia tissue is very dense, so we don't need it. So inflammatory response is always going to elicit tumor growth if you are prone to cancer. Cancer is essentially started around areas of inflammation. So if you have an animal that is implanted, and you give it drugs to give it tumors, then one of

those animals will have tumors around the chip implant since it is a major source of inflammation.

So there are two factors. One, the animals were forced to get cancer either genetically or through drugs. Or two, the inflammatory response. So the fact that we are human beings that are not given drugs to grow cancer and the fact that the chips that we have don't use that coating, greatly reduces the inflammatory response. So it is really not an issue.

Another thing that was also a telling thing. Katherine Albrecht pulls a quote out from one of the scientists who worked on one of the papers, and she quotes him "it was clear that the implants were the cause of the cancer" and I said that is a load of bullcrap. No scientist would ever say that is the cause. They would not establish a causal relationship in that way, that must be a made-up quote.

Interviewers: Let's talk security of the chip. Are there issues? Can you copy it in one's sleep etcetera?

Amal: Here is how it works. All the chips have a serial number, called a unique ID or UID. They will report those serial numbers based on ISO protocols they are compliant to, so they all have to report serial numbers, that is how they are selected in the field. So if you have ten chips in the field, the reader can say I want to talk to chip five. It does that with the ID. There really is no way around it. However, one of our chips does allow you to set up a privacy mode where you have a random UID every time the chip enters a field. But that is really not relevant. Every application you run into, the coffee makers in Sweden or Denmark, the doors, every one of those applications, they just read the serial number. There is no security. So it just says what is your serial number, and the chip says here it is, and the door opens. It is ridiculously insecure. Every door lock you buy for your home, the same thing, It doesn't care about any of the security functions. It is not a secure system.

But the interaction of proving the identity. In that capacity, yes, anybody that can get that serial number from you can then emulate it. They can pretend to be that chip. And pretty much do whatever they want. This is why those chips are not used for bank cards. Payment. And really secure systems, they don't use this. They might use the serial numbers to initiate communication. But they don't use the serial number alone to allow access right. So Vivokey chips are the same. Vivokey chips have a serial number. They report it. But, the secure aspects, the aspects that we actually use to identify you, have nothing to do with the serial number. It has to do with a cryptographic proof. That requires once you have a chip in the field, you get the serial number, we say great, we want to talk to you. At that point, what we do is we send special commands to the chip, with a cryptogram, and the chip accepts that

cryptogram, runs it through a cryptoprocessor and produces a result. So you can imagine the first part as a challenge, the chip does the calculation and sends back a response. We get that response back through the phone. We get it back and say okay, is it going to match the key that we programmed into the chip at the factory. Yes, it does match, so you can't send anything to the chip as an attacker, that is going to reveal that key. The chip says I am this guy, and then we go okay prove it. So there is no way to get involved in that process or modify it. Or anything. So for things like doors and so on, that is also what we are exploring with our hardware. It goes beyond just the serial number. So that way you wouldn't be able to do an attack. So if you snuck up on me or the door, you are thwarted by the cryptographic features. In a bank card, bank cards work similarly, they are smart cards and run an applet. The card itself, when you put it up to the reader, it does the same thing. It says my serial number is X, it accepts the serial number, then it enters into selecting the application, the bank card application on the card. The card says I want to pay for stuff. Then there is a whole secure interaction using encryption to say basically prove it. Prove that you are the account holder. And then, when you send your pin, the proof from card and pin go online to a processor, and the processor says it is correct. The card has to cryptographically prove itself to the reader.

Interviewers: Some of the implanted people we have been talking to think that the chips are secure since the reader has to be really close to the chip to read it.

Amal: That is not security. But the reality is. If you could trick the person to put their hand up to a reader that wasn't the real reader, it was an attack reader. Or putting a sniffing device near the real reader. These are not difficult problems. The proximity is very small. You have to get really close.

Consider this. This again why personal scope versus business matters. If your personal scope, chip, that is fine if you use it at home. Because who is going to want to break into your home. They are probably going to be random, they are probably going to be hitting a window. They probably won't care. But that is not true when you are talking about businesses. If somebody wants to get into a business, they don't care who you are, as long as you have a chip that lets them in. So how are they going to attack that? In a personal scope, again they are going to set up somewhere near your house. They are not going to bother, they will just break a window or whatever. But if they want to get into a business, that is a different risk-reward scenario for the person. They are just going to walk up to the businesses' readers and put a little thing next to it and it is going to sit there and sniff identities.

Yes, similar to skimmers with ATMs. It is a similar problem. You just put a little thing over the top, and it just listens to all of the interactions. It collects serial numbers. It is very simple to do. And you don't have to target a specific individual. Any serial number will let you in. So, now you are not targeting the person, the target is now the reader. And that is a very easy-to-attack device. So if your chip doesn't support encryption and the reader does not support encryption, then you are really in trouble. Because attacking those key points is very easy. Once I get into the building, then I am like okay, now I just put a skimmer on the next reader to sniff the serial numbers.

So that is the thing. People don't realize, that in an enterprise environment, or in any other environment aside from your personal scope utility, these chips are terrible. The systems are terrible. So this is why not only are these chip implants not great for enterprise, they are really not good for anything that is going to require any amount of security that is beyond the personal scope.

For personal use, you want to put it on your computer at home, great. That will work fine. But if you want to put one of those readers at work, terrible idea. Being able to use these secure functionalities of these devices is really critical. That is why we are starting though with the personal level. Because coming into a company saying, well I know you already have this access control stuff and that is managed by this company over here, that also manages your security alarms. But then you have also got your network security stuff and that is managed by another company. And we are saying we want to replace all of it. That is not going to work. But, we see people with Vivokeys to start to enter society and use their keys in different ways. And providing individual-level solutions, they then bring into the company, then there is a possibility that the company might say hey, we want to explore this. And then we say great, let us talk.

Interviewers: You have been in the microchip business for some time now. Is this aspect of encryption a recent thing?

Amal: It is only recently possible. When you are dealing with physics, you are dealing with the magnetic field strengths and coupling of these cylindrical shapes and these antenna readers, also used in phones. So when doing encryption, that is a lot of processing power. For this, you need a lot of energy or current, and that is not what is happening in this small tag. So you are getting very low efficiency when it comes to coupling an implant with a reader. It wasn't really until recently that the chips were small enough to be implantable and low power enough to make it viable. So really those two issues pushed out the requirements, that is really what it comes down to.

Interviewers: And don't you find it cool that you are the pioneers in this aspect?

Amal: It is only cool if you can eat. Right not, it is still challenged. Not to mention, it is such a niche market. It is very very niche. And to have four other competitors come in and sell knockoffs of your flagship product. It has really forced things in Vivokey to move much more slowly. Because we are self-funding. We are funding with revenue. So it's tough. But we are approaching the idea of actually going for funding.

Interviewers: What about crowdfunding or business angels etc?

Amal: Crowdfunding is possible, but the problem is the idea of what are the benefits. When I crowdfunded the xNT initially, the idea was very new. Now, you can buy the cheap knock-offs off Alibaba where the Vivokey only has a few other features. So it is a hard sell.

Let me put to you this way. Security will not sell a single chip. ANd here is why. Security is always an afterthought for people. And it is prevalent in the idea of what we just talked about. Look at any enterprise. Until they have a breach that financially impacts them, they don't care. So security is not what we are selling with Vivokey, haha. It is secure. It must be secure. But we cannot sell it based on that. Right now it feels like there are no applications compelling enough to drive a crowdfund. I have run probably five crowdfunding campaigns, all of which have succeeded, but only because the application was suitable enough to get to that target goal. And right now, VIvokey is not suitable for that goal. For people who get it, and understand the importance, yes it is. They will just buy it. There will not be enough people wanting to buy it during a crowdfunding campaign to make it work. But it is something we are looking at. We explored equity crowdfunding to actually make money.

There are hype cycles for sure. And I think we are probably approaching the peak for chip implants. Right now it is a lot of hype, "oh I can use it to pay for things" but none of that is true. And that is the problem. A lot of hype. And not a lot of real utility. And we are trying to change that, but there is going to be a tough time coming. There are quite a few articles out there talking about how they got an implant, and now they aren't using it for anything. And that is the reality for general purpose users. That is the problem.

A lot of people have the chip, but don't use it for anything. Zero. ANd that is the problem. They got it on the hype. Promises were floating around. Made them excited. They bought it. And now none of those promises came into fruition. And that is why the hype-cycle is a true reality of most technologies. A lot of hype in the beginning, and then it falls off. So hopefully we can make that trough of the hype-cycle very limited and actually build utility.

Interviewers: But you don't really have any competitors right?

Amal: Not really for the Vivokey. Biohax is making knockoffs of the xNT so, Vivokey is in a class of it own right now. But surely, that is not going to last. We try to build the community now.

Interviewers: Thank you very much for the interview and your time. It was very valuable.

APPENDIX D. Questionnaire Introductory Text

The purpose of this 5 minute questionnaire is to find out what potential users think about human microchip implants for use in a workplace setting. In brief, a human microchip implant can be seen as a tiny identification card which is implanted underneath the skin (in the hand, usually) which can be used for accessing the workplace, printing, payment etc.

Please answer the questions to the best of your ability. The data will be used in a way that will make it impossible to determine the identity of the individual responses. If you are interested in the results of this research, send an email to nolse14@student.aau.dk and we will send the report once it is finished.

Thanks,
Podder, A., Ismail, K., & Olsen, N. (Aalborg University Copenhagen, Denmark)