# Aalborg University Copenhagen

**Semester:** 10th semester

**Title:**
Development of a Mobile EEG-Based Feature Extraction and Classification System for Biometric Authentication

**Project Period:** February 1st 2012 to June 8th 2012

**Project type:** Master thesis


Aalborg University Copenhagen
Lautrupvang 4B,
2720 Ballerup

Semester Coordinator: Henning Olesen

Secretary: Judi Stærk Poulsen


**Supervisors:**

Associate Professor Henning Olesen
Research Assistant Allan Hammershøj

**Members:**


Juris Kļonovs
(20112204)

Christoffer Kjeldgaard Petersen
(20100997)


**Copies:** 4
**Pages:** 86
**Finished:** June 8th 2012


**Abstract:**

The aim of this work is to investigate the possibilities to build a mobile biometric authentication system based on electroencephalogram (EEG). The objectives of this work include the investigation and identification of the most feasible feature extraction techniques and how these features can be used for authentication purposes. Therefore, we review the relevant literature, conduct several EEG measurement experiments and discuss their procedure and results with experts in the EEG and digital signal processing (DSP) fields. After gaining enough knowledge on the feature extraction and classification techniques and proposing the most applicable ones for our problem, we build and present a mobile prototype system capable of authenticating users based on the uniqueness of their brain-waves. Furthermore, we implement a novel authentication process, which leads the authentication system to be more secure. We also assess the usability of the system and define possible usage scenarios and propose a number of practical suggestions for future improvements of the system.

# Table of Contents

# Acknowledgements

We would like to express our deepest gratitude to Dr. Jesper Rønager, an expert in the EEG field and neurologist, who agreed to invest his time for sharing his expertise and gave us a major contribution for clarifying open issues regarding our project. A very special thanks goes out to Dr. Henrik Bohr, who gave us a lot of valuable information. We are grateful to Bent Raymond Jørgensen for being a facilitator in arranging meetings with top Danish researchers and by this making it possible to raise the quality of this project. We want to thank Nina Nielsen for investing her time in reading our report and giving valuable comments.

We are also very grateful to our supervisors, prof. Henning Olesen and Allan Hammershøj, who were abundantly helpful and offered invaluable assistance, support and guidance. We appreciate their vast knowledge and skills in many areas and their assistance in writing the project report. Finally, we would like to thank PhD student Per Lynggaard from Aalborg University Copenhagen for assistance and advices in digital signal processing.

# Preface

This report is written as a master thesis for the Innovative Communication Technologies and Entrepreneurship program at Aalborg University Copenhagen in the spring 2012 on the sub-specialization track Service development.

This report includes a product in form of a prototype system demonstrating the objectives of the project. The source code for this prototype system and this master thesis report in PDF format is enclosed on a DVD disk.

# 1 Introduction

Electroencephalogram (EEG) systems capable of measuring brain-waves of an individual have received a lot of attention in recent years. These brain-waves measured as electric activity on the scalp can reveal various information about a person. Traditionally EEG has been used in clinical contexts to diagnose a patient in different areas; including testing for brain death [1] or coma, distinguishing between epileptic seizures, movement disorders, or migraine variants [2] or testing for the depth of anesthesia [3]. Furthermore it is possible to see changes in EEG signals when the eyes of a person are either opened or closed, or the state of drowsiness changes.

EEG signals of an individual are just as unique as fingerprints [4]. The uniqueness of EEG signals are particularly strong when a person is exposed to visual stimuli, and the visual cortex area of the brain on the backside of the head is the best place to measure brain-waves, related to the visual sense [5]. Therefore we will investigate if EEG can be used for identification of a person, and if it is possible to create a reliable authentication system using EEG. The idea of such a system is that instead of using e.g. normal textual passwords, the system stores a user's personal recording of brain-waves when exposed to an image, and compares this recording to new brain-wave recordings using an image when the user authenticates prospectively. In this way the system acts as an involuntary challenge-response system.

Using brain-waves to authenticate users has some advantages compared to other biometric authentication systems based on fingerprints or iris scans, since brain-waves and thoughts cannot be read by others.

Nowadays it is possible to purchase relatively cheap wireless EEG headsets capable of detecting and reading the brain-waves of a person. In this project a 14-sensor EPOC headset from Emotiv Systems will be used to present a prototype authentication system based on EEG. One of the new approaches in this project is that we will combine EEG with mobile phones. We believe that if EEG is considered as an extra context trigger in addition to the ones that currently exist on many smartphones (like camera, accelerometer, web or GPS) it reveals several potential usage scenarios.

Besides describing technically how a mobile EEG system for authentication can be built, a part of this project will also focus on the usefulness of such a system. We will examine whether such a system adds more value than already existing authentication systems, if it is better, and investigate the possible areas where it could be put to use. If our brain-waves are changing throughout life like many other parts in the body, it is appropriate to investigate if an EEG authentication system working as expected today would still be reliable in just a few years.

Also it is worth to consider how secure such a system is, and to take various challenges related to this topic into consideration.

## 1.1 Motivation

The project group previously did a semester project together at the Innovative Communication Technologies and Entrepreneurship program at Aalborg University Copenhagen in the fall semester of 2011 (this project can be found on the attached DVD in PDF format) [6]. The main objective of that project was to combine EEG headsets with mobile phones and to identify different usage scenarios where this combination could be put to use. We also demonstrated the capabilities of current EEG technologies and developed a prototype system capable of recommending a music playlist based on the user's current emotional state. Furthermore, various EEG headsets available on the market today were analyzed and assessed in that project.

In that project, we learned that an individual's brain-waves are unique. This formed the idea to investigate how EEG can be used as a basis in an authentication system.

The following reasoning motivated us to work specifically on this topic:

1) Feasibility of using EEG for biometric authentication;
2) There is a growing need for mobile authentication [7];
3) Combining EEG and smartphones can reveal several potential innovative services;
4) EEG hardware is getting cheaper, smaller and wireless;
5) Biometrics is an emerging area and it can improve the existing authentication mechanisms.

## 1.2 Problem Formulation

The project group will try to answer the following questions in the project:

- Can EEG be used as a mechanism for authentication, and if it is possible, in which contexts would it be useful from a user perspective?
- How can the feasibility of using EEG for authentication be proved by implementing a mobile prototype system? What mobile context triggers can possibly benefit the authentication procedure?
- What features can be extracted from the raw EEG measurements and which are

the most informative in terms of biometric authentication? How can EEG-based feature extraction be technically realized and what features should be selected for biometric authentication?

- What level of security can be reached with a mobile EEG-based authentication system?

## 1.3 Methodology

To outline the problems stated in the problem formulation, the overall aim of this project is to demonstrate the hypothesis that it is possible to use EEG for authentication purposes and furthermore assess the usefulness of such a new procedure. Here we describe the method we use to attempt answering the stated problems.

Methodically, we start by carrying out a literature study in order to obtain information about the current state of EEG systems and authentication systems in general and investigate similar works. Next, we perform a number of experiments, where we gather EEG data by recording brain-wave signals from subject persons in order to have a data collection that can be analyzed with the intent to find unique features, which can be used for authentication purposes. We use these data for the purpose of defining an initial approach on how an EEG based authentication system can technically be developed. In order to interpret the obtained data material, we carry out a qualitative interview session with an expert in digital signal processing.

As this project is an extension of a previous project about EEG in general, we will subsequently carry out another qualitative interview session with an expert within the EEG area, which we also did in the previous project. This interview will serve as the primary source in this project when it comes to EEG and its possibilities and limitations. We use the outcome of this interview to validate whether our initial approach is plausible, and define a requirement specification for an EEG based authentication system.

On the basis of these requirements, we develop an EEG based authentication prototype system tailored for mobile use. When implementing this prototype, we analyze and assess different available hardware and software technologies, and construct the prototype system with the chosen technologies.

Finally, we assess the different possible usage scenarios where EEG based authentication systems could be put to use, and analyze the security aspects related to such systems in order to evaluate whether using EEG in authentication systems gives better security than in current systems.

An illustration showing visually how the method is carried out and the order of the various steps has been created and can be found in the appendices on page 81.

Speaking of the way the project work is organized, the project group consists of two persons, and therefore the distribution of tasks is manageable compared to large projects involving many persons. For developing the prototype and organizing the work, the project group has decided to use best practices and characteristics from some of the known software development methods; especially the development method Unified Process [8], that is followed loosely. In this particular case, we decided to split the project period in phases and had regular meetings to keep on track and work in the same direction. As the project is obviously not just a development project, the method used covers all aspects of the project, including development of the prototype and report writing.

The project group has created a risk analysis at the beginning of the project period in order to meet potential risks. An evaluation of the risk analysis will be presented later in this report. Furthermore, a time plan containing working tasks is used to set up project milestones and track when to work on different tasks throughout the project period. Both the risk analysis and time plan can be found in the appendices on page 84 and 85.

## 1.4 Related Work

In this section we briefly present works that are similar to the scope of this project. The various similarities and differences between other projects will be covered in depth throughout the rest of the report. As the attention on biometric person authentication nowadays increases rapidly, we can find a growing number of publications covering several innovative authentication approaches, and some of them present the perspectives of the EEG-based approaches. This serves to give a quick overview of what has been done in the field so far.

One of the early ideas about combining EEG with authentication systems was presented by Thorpe et al. [9]. In 2005, they presented their novel idea for an authentication system using thoughts (calling them *pass-thoughts*) and describe the design for such system. This paper argues that such a system is feasible and could work since brain signals from an individual might be unique even when thinking about the same thought as others. This paper also briefly mentions the need for an open debate about the ethical considerations for such systems.

Processing brain-waves evoked from visual stimuli for the purpose of authentication has been described by Zúquete et al. [10]. This paper argues that visual stimulations

lead to very focused brain activities known as Visual Evoked Potentials (VEP), and presents an EEG authentication system using a picture set of black-and-white line drawings made by Snodgrass and Vanderwart [11] - the latter originally conceived to investigate the differences and similarities in the processing of pictures. This is similar to this project, since we are also using visual stimuli to build an authentication system. However, we are aiming for a more simplified image processing approach.

Ashby et al. proposed an EEG based authentication system based on a low cost EEG headset [12]; specifically a 14-sensor Emotiv Epoc EEG headset, which is also used in this project. In this paper it is argued, that a low-cost EEG headset might pave the way for mass adoption in consumer applications.

## 1.5 Scope and Delimitations

The project group has decided to investigate to which extent implementing an authentication system based on EEG can be built using current technologies, including software and hardware available on the market today. Thus, we are not proposing a new hardware design for an EEG headset specialized in measuring specific features for authentication purposes.

Furthermore, as this project is focusing on the technical and practical capabilities of EEG rather than the various medical aspects, we will not cover in depth how conditions of subject persons influence EEG measurements for authentication purposes. As we will see later in this report, conditions like drowsiness, hunger or stress all influence EEG signals, but a comprehensive test of these circumstances is out of the scope of this report.

## 1.6 Structure of the Report

This report is organized in the following way:

Chapter 1: Introduction – introduces and explains the purpose of the project, presents the problem formulation and methodology, and similar works.

Chapter 2: Background – presents theory and background information about EEG and authentication systems.

Chapter 3: Theory and Analysis – shows how EEG signals can be processed in order to find unique features, explains the setup of the experiments carried out and shows the results from interviews with an expert in the EEG field.

Chapter 4: Practical System Implementation – describes how the prototype system is

technically implemented and assesses different available technologies.

Chapter 5: System Usage – provides an analysis of in which scenarios the system can be used, presents important security aspects and describes possible further improvements of the developed system.

Chapter 6: Conclusions – presents and discusses the primary outcomes of the project, and concludes, elaborates and analyzes the results achieved during the work on the project.

# 2 Background

This chapter is presenting background information about brain biometrics and authentication systems in general.

## 2.1 Brain Biometrics

The brain is a highly complex and continuously active organ that receives and processes signals from the body and the environment, generates responses accordingly and recalls the stored information when it is needed. It is a known fact, that our brains represent both behavioural and physiological information at the same time [13] [14] and therefore reveal a big potential value for biometric purposes.

### 2.1.1 Brain Activity Registration

The brain activity produces several types of signals, including electrical, magnetic and metabolic signals [15, p. 87]. This activity can be registered using different approaches, which are usually classified as invasive and noninvasive. The invasive methods require surgical intervention for installing permanent implant devices in the brain, which raises several serious risks and therefore is not feasible for particle biometric applications. The most common noninvasive methods, which do not involve any physical damage, include magnetoencephalography (MEG), functional magnetic resonance imaging (fMRI), Functional near-infrared spectroscopy (NIRS), positron emission tomography (PET), Single-photon emission computed tomography (SPECT), optical imaging, and electroencephalography (EEG), which nowadays are mainly used for medical applications [16, p. 163] [17]. EEG is recognized as a direct and the simplest noninvasive method to record brain electrical activity, represented as voltage fluctuations resulting from ionic current flows within the neurons of the brain [18, pp. 18–19], while other methods record changes in blood flow (e.g., SPECT, fMRI) or metabolic activity (e.g., PET, NIRS), which are indirect markers of brain electrical activity. Electroencephalogram (EEG) waves can be represented as a signal over time, registered by the electrode placed on the scalp over the brain. In this way it is possible to detect and record the electric field that reaches the scalp and that partly reflects the underlying brain activity [18, p. 167]. The main advantage of EEG is that it can detect changes over milliseconds, which is excellent considering that an action potential takes approximately 0.5-130 milliseconds to propagate across a single neuron, depending on the type of neuron [19, p. 17]. Thus, apart from other techniques, which require more sophisticated and expensive devices as well as relatively long measuring time (e.g., PET and fMRI have time resolution between seconds and minutes), EEG is more practical, portable and faster to use.

EEG can be used simultaneously with fMRI so that high-temporal-resolution data can be recorded at the same time as high-spatial-resolution data, however, since the data derived from each system occurs over a different time course, the data sets do not necessarily represent exactly the same brain activity. EEG can also be used simultaneously with NIRS without major technical difficulties, and a combined measurement can give useful information about electrical activity of the brain.

### 2.1.2 Biometrics

Biometrics is the science of automatically identifying individuals based on their unique physiological or behavioural characteristics [20], and the EEG signal represents both of them [14, p. 3]. These characteristics are also called biometric identifiers and they must be *distinctive* and *measurable* in order to identify individuals [21].

Examples of biometric traits include fingerprint, face, iris, palm-print, retina, hand geometry, voice, signature, gait characteristics, and brain-waves (EEG) [20, p. 3] [22, p. 7]. The EEG use for person authentication is still the least explored possibility of all previously mentioned approaches.

As we have settled on a person biometric authentication system based on EEG recordings in this thesis, we should clarify the underlying characteristics which can be extracted from EEG signals.

### 2.1.3 EEG Characteristics

In this section we introduce the main characteristics of EEG signals.

The EEG is a measure of voltage as a function of time. The voltage of the EEG determines its amplitude (measured from peak to peak). EEG amplitudes in the cortex range from 500-1500 μV, however, the amplitudes of the scalp EEG range between 10 and 100 μV [16, pp. 11–12]. The attenuation is due to the poor electrical conductivity of brain tissues, skull and scalp. In general, EEG signals represent the combination of waveforms, and are generally classified according to their:

a) frequency (speed);

b) amplitude (power);

c) wave morphology (shape);

d) spatial distribution (topography);

e) reactivity (behavioural state);

EEG characteristics are highly dependent on the degree of activity of the cerebral cortex [23, pp. 2–5], which represents a very complex neural wiring, and therefore are unique for each person [24, p. 18]. The following illustration shows EEG measurements of 5 seconds:

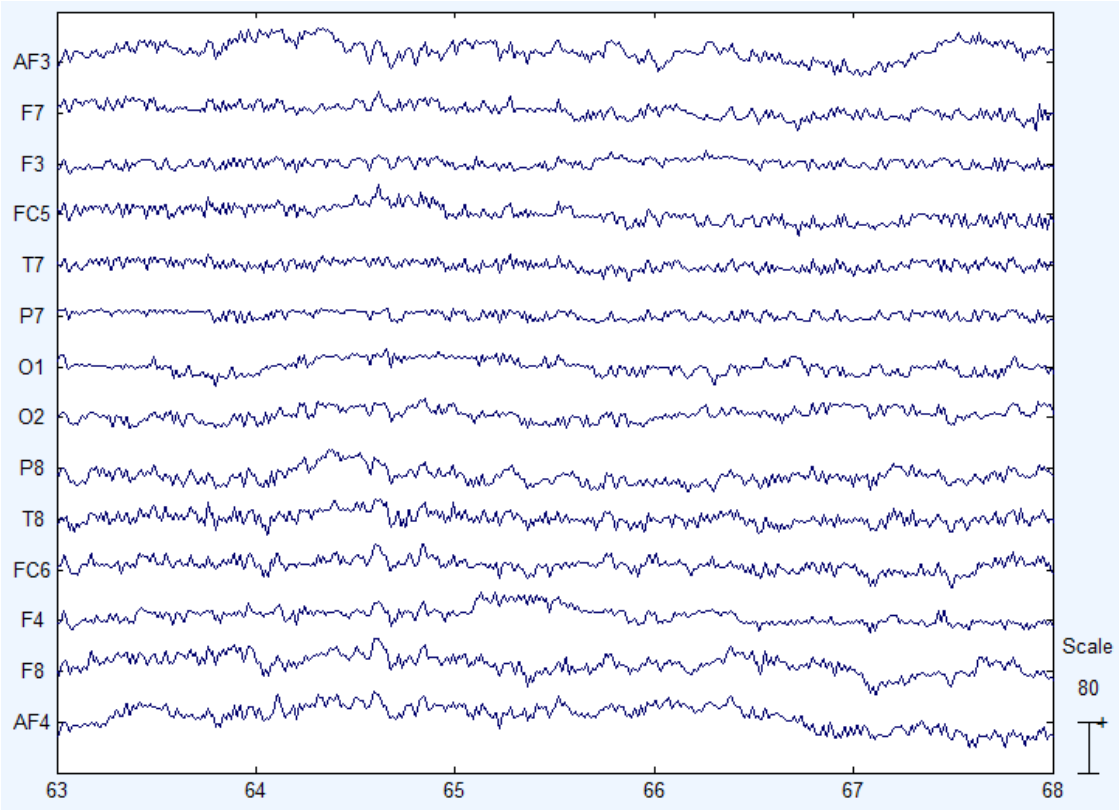


*Figure 1: Raw EEG data without the baseline, amplitude scale is set to 80 μV. The horizontal axis shows the timeline in seconds and the vertical axis corresponds to fluctuations in μV measured from different positions of the scalp, according to the International 10-20 system [60].*

### *Frequency bands*

The most familiar classification uses EEG waveform frequency bands (alpha, beta, theta, delta and gamma waves) [25, p. 211] which can be decomposed using different mathematical approaches, and the most common method is Fast Fourier Transform (FFT), however the most efficient approach to our knowledge is Wavelet Transform [26] described in the Theory and Analysis chapter later in this thesis. These waveforms are essential tools for analysing human brain activity.

The five frequency bands are therefore briefly described in the following list:

- **Alpha (α) waves:** are typically divided into low α and high α waves. Low alpha are those between 8 and 9 Hz and high alpha are approximately between 11 to 13 Hz, and the average frequency of alpha waves is ranging between 10 Hz. A typical healthy adult has stable alpha waves, which means that the frequency

varies not more than 1 Hz (e.g., 9 ~ 10 or 10 ~ 11 Hz), with the power ranging between 10 to 20 μV amplitudes. Alpha waves arise from synchronous and coherent (in phase) electrical activity of large groups of neurons in the human brain. Alpha waves are periodically found to originate from the occipital lobe during periods of relaxation, with eyes closed but still awake. Conversely alpha waves are attenuated with open eyes as well as by drowsiness and sleep. It was also proved that the activity of alpha rhythm reflects the vision functions of a person [18, p. 125].

- **Beta (ß) waves:** (similarly to α waves) are divided into low ß (14 – 20 Hz) and high ß (20 – 30 Hz) waves. The power of these waves has < 10 μV amplitudes. Comparing with α waves, not much is known about ß waves, due to their irregular activity. Beta waves are usually associated with normal waking consciousness, often active, busy, or anxious thinking and active concentration. Rhythmic beta with a dominant set of frequencies may be associated with various pathologies and drug effects. Beta waves are usually detected on both sides of the brain in symmetrical distribution and are most evident frontally. It may be absent or reduced in areas of cortical damage [27, p. 2].

- **Tetha (θ) waves:** Theta wave activity has a frequency of approximately of 4 to 8 Hz, and it can also be divided into low $\theta$ waves (of 4 – 5 Hz) and high υ waves (of 6 – 8 Hz). The amplitude is relatively high, normally < 100 μV. Theta waves are thought to involve many neurons firing synchronously. Theta rhythms are observed during some states of sleep, and in states of quiet focus, such as meditation. They are also manifest during some short term memory tasks, and during memory retrieval. Theta waves seem to communicate between the hippocampus and cortex in memory encoding and retrieval [28]. As an interesting fact, it was proved that υ rhythm plays a significant role in analysing processes and in learning procedures [27, p. 3].

- **Delta (δ) waves:** are the slowest EEG waves, which are normally detected during the deep and unconscious sleep. Their frequency is lower than 4 Hz, and similar to EEG frequencies that appear in epileptic seizures and loss of consciousness, as well as some comatose states. It is therefore thought to reflect the brain of an unconscious person. If the frequency is lower than 1 Hz, then such waves are identified as *subdeltha*, which are heavily pathological waves. The amplitude is relatively high, and measured in < 100 μV. Delta waves increase in relation to our decreasing awareness of the physical world. Thus, during the cognitive processes, the delta waves have relatively small amplitudes.

- **Gamma (γ) waves:** have approximately 40 Hz frequency, and it can vary between 26 to 70 Hz. These waves have very low amplitudes of < 2 μV of power. Gamma waves are thought to signal active exchange of information between cortical and subcortical regions. Gamma waves mainly indicate which areas are most active. It is seen during the conscious waking state and in REM dreams (Rapid Eye Movement sleep) or during anaesthesia. In fact, gamma and beta activity may overlap in time [27, p. 5].

### *EEG artifacts and their prevention*

Unfortunately, EEG is often contaminated by signals that have non-cerebral origin and they are called artifacts, which are caused by eye movement, eye blink, electrode movement, muscle activity, movements of the head, sweating, breathing, heart beat, electrical line noise and so on. This is one of the reasons why it takes considerable experience to interpret EEG clinically, because artifacts might mimic cognitive or pathological activity and therefore distort the analysis or completely overwhelm the EEG waves and make the analysis impossible. However, some artifacts can be informative as unique biometric identifiers.

All EEG artifacts can be divided in two main groups [27]:

1. Physical world (technological) artifacts:
   a. Movement of the EEG sensors
   b. 50/60 Hz AC power sources
   c. Fluctuations in electrical resistance
   d. Contact and wire quality
   e. Dirt
   f. Low battery of the headset
2. Artifacts of a user’s physiological origin:
   a. User’s heart rate and innervation (can be used as a biometric identifier)
   b. Physical movements (can be used as a biometric identifier)
   c. Eye movements (can be used as a biometric identifier)
   d. Sweating

Usually, for a clearer analysis it is necessary to eliminate the causes of artifacts before EEG measurement procedures as well as to reduce the remaining artifact signals by applying appropriate filters.

Figure 2 shows the main brain parts, which are further explained in terms of what

information can be derived from each of them.

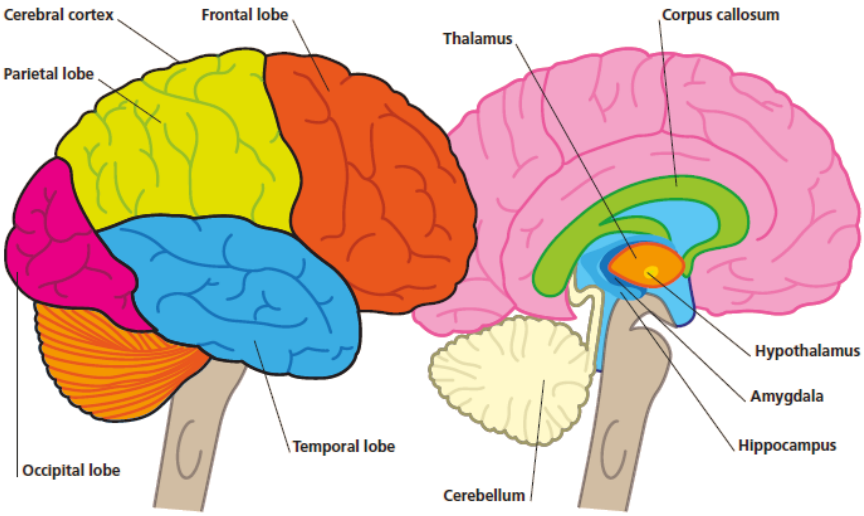


*Figure 2: The structure of the brain [76, p. 14]*

The main human brain part cerebrum is divided into the left and right hemispheres. They are linked by a central processing unit called the corpus callosum. Cerebellum is responsible for the balance and muscular co-ordination, but it's activity cannot be measured by available EEG headsets.

Each hemisphere is split into four more compartments:

1) Occipital lobe (back part of the brain) is responsible for the visual imagination and responds to visual stimuli. This part is the most efficient for biometric purposes. This part is recognized as the most effective in terms of extracting biometric data [29].

2) Temporal lobe is involved in the organization of sound, memory, speech, and emotional responses.

3) Parietal lobe handles sensations, such as touch, body awareness, pain, pressure, and body temperature, as well as processes spatial orientation tasks.

4) Frontal lobe is considered the home of our personality. The highest part of the frontal lobe is involved in solving problems, activating spontaneous responses, retrieving memories, applying judgement, and controlling impulses. It also controls our social and sexual behaviour [30, p. 14]. It has already been proved that some of the EEG parameters extracted from the frontal lobe are highly personal-dependent [31].

A more thorough discussion on EEG characteristics can be found in our previous study

[6, pp. 14–19], where we also discussed the EEG data source and different frequency bands in more detail.

## 2.2 Authentication Systems

Since the main objective of this project is to validate whether it is possible to build an authentication system based on EEG, it is important to clarify the different definitions and terms related to authentication systems. In security terms, three different concepts are essential. Those are the concepts of identification, authentication and authorization [32]. It is easy to confuse these concepts with one another, even though they are quite different and represent different approaches related to security systems. The three concepts are therefore briefly described in the following list:

- **Identification:** Identification is the simplest of the three concepts, and is simply a claim of an identity, with a goal of identifying one particular person from a group of persons. Basically it is a matter of not knowing anything about a particular subject person before trying to identify him or her, and verify a linkage between the known and unknown. The known about a subject is called an identifier, and must be unique within the identification scope.

- **Authentication:** Authentication systems tries to verify the claim a user gives about his or her identity by answering the question “Is the user really who he or she claims?”. Compared to a computer requiring login credentials, the system could authenticate the user by asking for a password.

- **Authorization:** When a user has successfully been authenticated into a system, the last step is to find out what the user can do with the system, or is allowed to do. This is basically the concept of authorization. A computer system can be designed with different user roles, where some users might have access to (or are authorized to) edit various resources, while others only have access to read them. As this project is centered on an authentication system, we will not go in depth with authorization.

It is important to note that there is a clear difference between identification and authentication, even though though they are dependent on each other. Identification cannot be carried out without some authentication [33]. The same applies in biometric terms. The main goal of biometric person identification is to identify an individual from a group of persons by matching the biometric features of one person against all the records in a database, while the goal of biometric person authentication is to confirm or deny an identity claim by a particular individual [31].

Stephen Downes defines identification as the act of claiming an identity, where an identity is a set of one or more signs signifying a distinct entity, and authentication is the act of verifying that identity, where verification consists in establishing, to the satisfaction of the verifier, that the sign signifies the entity [33, p. 4].

Figure 3 below illustrates how the three possible results of identification, “OK” for a positive result, “Not OK” for a negative result or “I don't know” for an uncertain result, are linked to different levels of confidence in a person's identity. Between each step there is a threshold that is surpassed when either the confidence or result of identification raises.

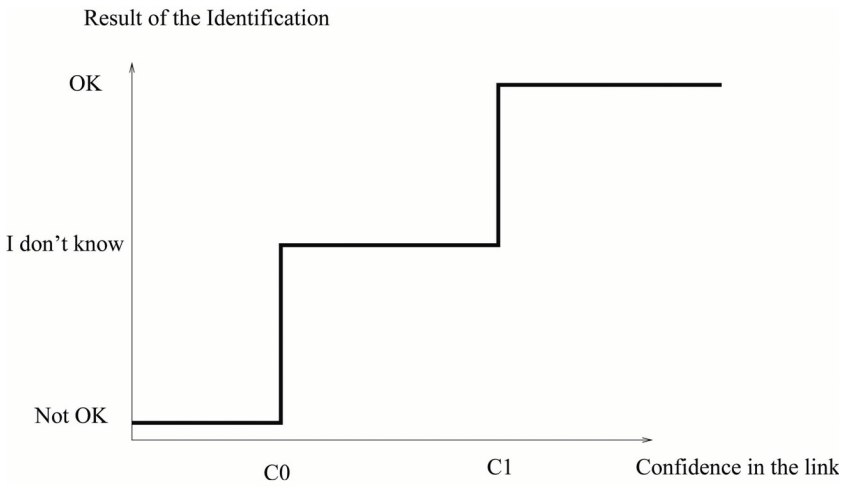


*Figure 3: The three cases of identification and corresponding confidences in a person's identity [34, p. 8].*

Authentication systems are in general based on three fundamental classes, “something you know”, “something you have” and “something you are”. Sometimes even a fourth one, “something you do”, is used [34]. For authenticating a person, at least one of these approaches must be used. Each of the classes authenticates a person in different ways:

- **Something you know:** Could for instance be a textual password. The overall idea is that you have a secret that only you know. Textual passwords are one of the most common kinds of authentication, but unfortunately there are a number of problems associated with the use of them. Passwords are easy to forget, and therefore they must be relatively simple so that the human brain can remember them. Simple passwords that can be found in a dictionary are vulnerable to computer attacks though [35, p. 2], forcing users to select more complicated and hard-to-remember passwords. This also poses the risk that the person writes the password down on a piece of paper in order to remember it, and thereby undermining the *something you know* class, since the only thing an attacker

needs to gain access is to obtain this paper. Also, if textual passwords are typed into the authentication system through a keyboard, they are vulnerable to "shoulder surfing attacks", meaning that someone could be standing behind the person typing in the password lurking what he or she writes [36, p. 1]. The same kind of vulnerability applies, if the attacker succeeds in installing a keylogger on the target machine, which can send whatever the person writes on the keyboard to the attacker.

- **Something you have:** Could for instance be a smart card. The overall idea is that the person authenticating into a system must have some kind of object to do so. This removes the problems with textual passwords, but on the other hand the object must be carried along every time the person wants to be authenticated. Also there is a risk that the object gets stolen. Therefore the *something you have* class is often combined with the *something you know* class, creating a 2-factor authentication with two independent steps that must be completed in order to authenticate. An attacker would in addition to stealing the object also need to know a secret for successfully authenticating.

  Smart cards are a typical example of the *something you have* class. A smart card can be capable of performing some kind of cryptographic calculation. An ID card or credit card with a magnetic strip or chip is another example.

- **Something you are:** Could for instance be a fingerprint. The overall idea is to base the authentication on something "built-in" in the person trying to authenticate. A number of biometric characteristics makes it possible for a machine to distinguish people from one another. Besides fingerprints, other biometric characteristics can also be used to identify people from one another, including iris scans, voice recognition, DNA, ear, face, signature among others [37, p. 5]. To implement a biometric authentication system, a representation of the biometric characteristics in question is stored in the system. When a person wants to authenticate, the biometric characteristics are measured and compared to the ones stored. If the two are equal enough, the person can successfully be authenticated.
  Biometric authentication characteristics have one major drawback though - they cannot easily be changed and are impossible to replace if they are stolen [38, p. 335]. If referring to a webmail account analogy, biometric characteristics can be considered as usernames or e-mail addresses, and not passwords. In other words information that is available to everyone. This is comparable to biometrics in terms of publicity, and not replacability. The same applies to fingerprints. A fingerprint is public, since we place it everywhere every time we touch

something. For an attacker to exploit a fingerprint based authentication system, the fingerprint or even the finger of the subject person should be stolen.

It has been shown, that the more of the three classes, something you know, have and are, that can be verified in an authentication system, the better the system is from a security point of view [39, p. 7]. At least two classes, and preferably all three should be used. Authentication systems based on multiple classes are harder for an attacker to compromise.

The fourth class mentioned above, “something you do”, proposed by Anrig et al. [34], is a class external to the person trying to authenticate. The idea behind it is, that there is a difference between a real physical person and a virtual person. Virtual persons are defined as a kind of mask, that someone or something is sitting behind. This someone or something can either be a physical person, an animal or even a computer program or a legal person (again there's a difference between a real physical person and a legal person, which is defined in our laws). According to Anrig et al., virtual persons can be defined by roles and acquisitions. The roles are defined as “something you are” and “something you do”, while the acquisitions are defined as “something you know” and “something you have”. Figure 4 shows the relationships between the authentication classes and roles and acquisitions in general.

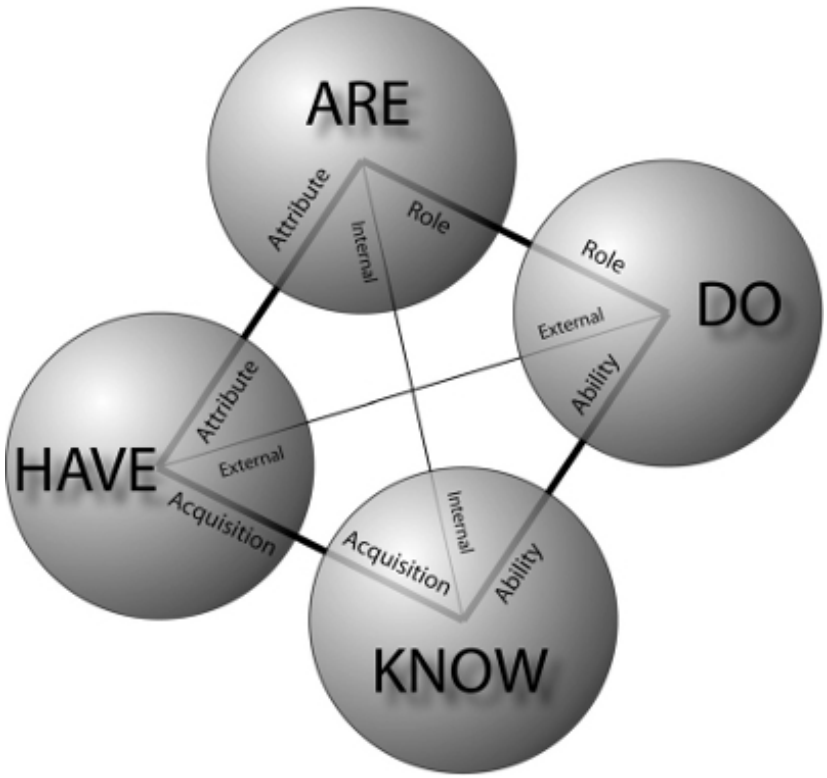


*Figure 4: Relations between authentication technologies [34, p. 4]. Besides showing the relationships between classes, roles and acquisitions, the figure also shows relations between the classes and the two other categories 'attributes' and 'abilities' and the types 'internal' and 'external'.*

Given this figure, a virtual person defined with the “something you do” class could for instance be the person who is having his or her brain-waves recorded (both examples combining the role and ability categories). Brain-waves are in general an internal attribute belonging to a subject, i.e. “something you are”. The virtual person defined as the person who *is* in possession of a particular set of brain-waves is therefore not necessarily the same one as the virtual person measuring his or her brain-waves. It is important to note that brainwaves can be interpreted as “something you are” as well as “something you have” at the same time. In the system proposed in this project, the latter virtual person claims to be the other one, and it is up to the system to decide based on the level of confidence whether the real physical person can gain access to the protected material.

### 2.2.1 Challenge Response

In the traditional sense, challenge/response is an authentication method where a person is prompted some kind of challenge in order to give back some kind of information (the response). Systems can either ask the user a question such as asking for the mother's maiden name or provide a numerical code (the challenge) which the user must enter in a smart card. The smart card can then display a new code (the response) which the user must type into the system in order to authenticate [40]. Traditionally, a challenge/response system follows a client-server architecture, with the server providing a challenge, which the client must respond to.

A practical example of challenge/response in action, which doesn't require direct user involvement, is to use one-way hash functions to avoid secrets such as textual passwords to be transmitted in clear-text over a network. When a client connects to a server, the server will compute a random text string, which will be sent directly back to the client. The client then concatenates this random text string and the password required by the system, and computes a one-way hash value of this new string (common cryptographic hash functions include MD5[1] or SHA-1[2]). The computed hash value is then sent to the server, which will likewise compute a hash value of the random text string and the server-side stored password. If the two computed hash values are exactly the same, the client can be granted access. As an example the secure socket layer protocol works in exactly the same way [41].

In general, the same applies to challenge/response in authentication systems based on biometry, but there is an important addition that applies in this case. Here identification of a subject person is confirmed by getting some kind of direct response from the

1 RFC 1321: http://tools.ietf.org/html/rfc1321
2 RFC 3174: http://tools.ietf.org/html/rfc3174

person. This response can either be voluntary or involuntary. The difference between the two is that in a voluntary response, the user will consciously react to the challenge the system presents, whereas in in an involuntary response, the user's body will automatically react to some kind of stimuli [42, p. 6].

### 2.2.2 Assurance Levels

In general, authentication systems operate with multiple levels of security. In technical terms, these levels are defined as assurance levels, and The American Office of Management and Budget (OMB) describes four levels of assurance for authentication systems with technical requirements described by the National Institute of Standards and Technology (NIST), with Level 1 being the lowest level of assurance, and Level 4 the highest [43, p. 4] [44, pp. 41–48]. Each of these assurance levels describes the degree of confidence that the user is who he or she claims to be. The following list summarizes the technical requirements for these four assurance levels:

- **Level 1 – Little confidence in the identity's validity**: No identity proofing or cryptographic techniques are required at this level.

  The use of assurance level 1 especially appropriate when there is very little or no negative consequences of an erroneous authentication. Websites requiring registration for access to protected content is an example of assurance level 1 security. This kind of registration usually provides some assurance about the subject person's identity, even though it is not a requirement that such assurance level 1 accounts must be created with a person's real name, and therefore information like e-mail addresses can be used as identifiers. The OpenID standard for decentralized authentication has been approved for assurance level 1 by the Federal Identity, Credentialing, and Access Management (ICAM) [45, p. 6].

- **Level 2 – Some confidence in the identity's validity**: The subject person must prove through a secure protocol that he/she is in control of the primary token. Identity proofing is required at this level, cryptographic techniques are not.

  Assurance level 2 obviously requires more confidence in the subject person's identity than assurance level 1, and the consequences of an erroneous authentication are considered moderate. Examples of assurance level 2 security includes self-service solutions on the websites of telecom companies, insurance providers, public authorities or the like, where people can sign up or use some kind of service using their civil registration number. Such services need some level of certainty about the users identity, to make sure that the provided

identifier is actually the user's. If such a service is misused by providing a wrong identifier, it is just inconvenient at worst, since official papers, notices about payment, etc. are sent to the user's registered postal address.

- **Level 3 – High confidence in the identity's validity**: Besides that the subject person must prove through a secure protocol that he/she is in control of the primary token, this level requires cryptographic strength that protects the primary authentication token against compromise. In order to comply to this assurance level, multi-factor authentication must be used (at least two factors).

  Examples of systems requiring assurance level 3 include web applications that send one-time passwords to the user's mobile phone after performing a sign up process. This one-time password must be entered in the web application in order to complete the sign up. This is basically an out-of-band authentication channel, and gives a higher degree of trust in the user's identity, since it is possible to verify that the user in question is actually is in possession of the phone, whose phone number has been provided.

- **Level 4 – Very high confidence in the identity's validity:** Requires cryptographic authentication of all parties and all data transfers between parties involved over a secure protocol based on cryptographic methods. The only difference between level 3 and 4 is, that only hard cryptographic tokens are accepted.

  As level 4 is the highest assurance level defined, it is appropriate for systems requiring very high confidence in a person's identity. Such cases could for example be transactions involving huge multi-million money transfers. Also, this level could be required when someone wants access to a law enforcement database containing criminal records of a person. Such access should only be granted to authorized personnel, as unauthorized access is associated with privacy issues.

Which assurance level to choose for a given authentication system depends on the risk associated with the impact of unauthorized access to protected material. The more important it is to secure the protected material, the higher assurance level must be picked. 4G Americas (previously 3G Americas) defines this risk as a function of the two factors potential harm or impact and the likelihood of such harm or impact [46, p. 33]. Examples of harm and impact include unauthorized release of sensitive information, financial loss, harm to personal safety services, among others.

The eligibility of the four assurance levels lies in, that they provide an in-depth

descriptions of technical requirements for different kind of authentication systems. After completing a risk assessment, identified risks can provide a basis for decision of an appropriate assurance level to pick, and technologies matching the chosen assurance level can be selected. Even though the assurance levels are described by an American department of The White House primarily targeted American governmental agencies [43, p. 1], the concepts are still valid in other respects, and can serve as a foundation when implementing any kind of authentication system. Later in the report we describe how EEG and authentication systems fits with these assurance levels.

## 2.3 Objective of EEG Based Authentication

In this chapter we have presented the state of the art regarding electroencephalography (EEG) and authentication systems in general. By putting these two concepts together, we are aiming to develop a new multiple-factor authentication procedure tailored for systems that require very high security. The cornerstone of our proposed procedure is authentication based on EEG in view of current authentication concepts.

# 3 Theory and Analysis

In this section we represent our review of the EEG-based biometric authentication perspective and the most feasible EEG features which are most likely to be unique for each subject based on the literature and the suggestions from EEG and digital signal processing (DSP) professionals. We also investigated feature extraction computational approaches, which can further be implemented into the EEG-based authentication system.

## 3.1 Interview

To get an expert's view on how EEG can be used for authentication purposes, we conducted a couple of interview sessions throughout the project period with neurologist and EEG expert dr. Jesper Rønager, previously employed at the national hospital of Denmark, Rigshospitalet in Copenhagen, and currently working as a consultant at the Danish company Biochronos. The primary interview took place at Aalborg University Copenhagen on the 8th of March 2012 [47]. The outcome of the interview will be described in detail in this section. Besides Jesper Rønager and the project group, several other persons were present at the meeting, including staff members from Aalborg University's Center for Communication, Media and Information Technologies (CMI). An audio recording of the interview can be found on the attached DVD disk in MP3 format. This file is named *jesper-roenager-interview-2012-03-08.mp3*.

### 3.1.1 Possibility of Using EEG for Authentication

In a previous project we also conducted an interview with Jesper [6, pp. 21–25], which aroused the interest to continue with this project. This meeting was focused on EEG in general, and covered several aspects of EEG. At this first meeting we asked Jesper if it is possible to use EEG equipment for biometric identification. Jesper confirmed this, and added that EEG is unique from person to person. He put it in the following way:

> *"None of us has the same EEG. Furthermore, EEG is a biometric phenomenon and it could in principle be used to detect some specific waves, but again it depends on the number and placement of sensors."*

Several literature sources serve as a strong confirmation of this fact [48, p. 133] [38, pp. 335–336], and some authors propose even stronger statements: *"every single individual has a unique and unchanging baseline brain-wave pattern"*, proposed first time by Lawson in 2002 [49]. At this meeting, Jesper also mentioned that the visual cortex area (occipital lobe) on the back side of the brain is the most informative for finding picture recall thought patterns, i.e. the brain-wave patterns when a person is

looking at something.

With this information in mind, we arranged this new meeting to find out more about how EEG can be used for biometric authentication. We presented our preliminary idea about using photographs of known faces as stimuli for recording brain-waves. Jesper Rønager replied, that in principle you could show any kind of image, since they would all stimulate the visual cortex, but when asked if there could be a difference between for example showing a relatively harmless image of a flower compared to an image of a close relative, Jesper said

> *"That might be true. It might be a clearer signal if it is a relative. I believe so."*

Even though we cannot distinguish directly between images using EEG alone, this means we can use a set of images of people known to most people, or one could imagine that the user of an EEG-based authentication system could use his or her own photo for brain-wave stimuli. Thus, the chosen image will not be kept secret, and will not serve as a "personal password image" as Thorpe et al. proposes [9], but will be public known. As brain-waves are unique, the system can still be used for authentication purposes, and additionally the images will not be vulnerable to shoulder surfing attacks as if they were used as normal textual passwords [36, pp. 1–2]. As a default, the system could let the user choose an image from a pool of photos of famous people, or let the user upload his or her own image.

### 3.1.2 Finding Unique Features

One of the most important questions was to ask how the process of finding unique features for the purpose of authentication could look like. Jesper Rønager replied to this question in the following way:

> *"Well, the state of the art is like you're making a band pass filter in the start and make a Fourier [transform]. And you can make this Fourier much better really. Who says you only need to work in the four bands [delta, theta, alpha and beta]? You can do more. And the more you have, the better it will be. And then you can use statistical correlations and feature extraction to see what does this correlate with when you are showing a picture of something. And it could be a known person. That wouldn't be a bad stimulus."*

Besides confirming that the approach of using photos of known people is definitely a way to go, Jesper also suggested to look into additional frequency bands than just the usual four (alpha, beta, delta and theta), because they will provide even more information.

In our initial experiments we sampled for 5 seconds while recording brain-waves, and asked Jesper if this was enough, or maybe even too much due to relevant signals fading away after a few moments. Jesper confirmed that five seconds of recording should be enough, because the relevant signals will be present very fast. It is a matter of a few seconds.

### 3.1.3 Relevance of Other Human Senses

We also asked Jesper if other of the five senses than just the visual one (hearing, taste, smell and touch) could play a role in such an authentication system. Jesper emphasized that visual stimuli gives the strongest EEG signals, but added this:

> *"You can't record the smell signals because those are not easily accessible. Those are hidden behind the temporal lobe so it is hard to get them. You should be able to get [signals from] homunculus. There are several of them. One for each kind of sense. One is dedicated to cold and hot, one to vibration and one to touch and one alone is dedicated to pain. So you can give a subject person an electric shock in the finger and get a significant signal."*

Even though the last part of this sentence is said in a humorous way, it tells us that other senses than just the visual one could be taken into consideration when implementing an EEG based authentication system. In fact, a simple touch helps lowering the alpha waves, which will lead to the subject person being more focused. For a mobile EEG authentication system, we can take advantage of this by using the built-in vibrator to vibrate the phone before showing an image and recording the brain-waves. This way the mobile device is used as a kind of tactile feedback to the user, implicitly telling the user "Now you should be ready to focus on an image". Also, this kind of tactile feedback can be used in an alternative version of the authentication system aimed for e.g. blind people that obviously cannot benefit from a visual based system.

### 3.1.4 Importance of Sensor Placement

Another topic we wanted to cover was the issue of how important placement of the electrode sensors actually is. This problem is especially important if an EEG based authentication system will be accepted for widespread use. As such a system requires a brand new hardware component (the EEG headset), users must learn how to properly put on the headset. Therefore, it is relevant to address exactly how important sensor placement is in terms of achieving reliable EEG recordings. Jesper Rønager replied that of course the sensors should be placed approximately at the same location each time a recording is made. When asked if a person wear the headset, takes it off, and put it on

again, so the sensors might not be placed millimeter-precise, he replied that it shouldn't really be a problem.

### 3.1.5 Ageing of EEG Signals

In continuation of the question about sensor placement, we discussed if EEG signals change over time. This is relevant because the final system might not be used on an everyday basis, and there could be large time gaps between usages, e.g. several years. The natural question is then, if an EEG authentication system working for one person today, will work the same way for the same person in a year or two. Jesper Rønager provides the following information about the extent to which ageing of EEG plays a role:

> *"I think the problem could be with children and young people, not older people. I think that will be nearly the same for 50 years. But if you are taking a baby, you would not expect to find the same signals after two years. I don't think so. […] EEG shows no changes from the age of 18 until a very old age. But a doctor can match the age of an EEG within 1 and 2 years."*

Thus, it is clear that the system should be tailored for grown up people, and exclude persons less than 18 years of age. But an important thing to add according to Jesper is that the EEG field is rather new, and according to his knowledge, nobody has tried doing consecutive EEG recordings and then making feature extraction.

### 3.1.6 Condition of Subject Persons

We already know that the conditions of the subject person would affect EEG recordings in various ways [6, p. 23]. We wanted to get Jesper's opinion on how conditions like hunger, drunken state, drowsiness, emotional and stress states influence EEG signals. Jesper's immediate reply was that all of the listed conditions will affect the EEG, and mentioned as an example how hunger and low blood sugar affect it:

> *"If the blood sugar is low, then you will see something happen. There will be a lot of low frequencies, delta and even sharp waves. […] So, low blood sugar will give an abnormal EEG, and if you have such patients at a hospital, you'll feed them and do it again."*

The importance of this question was aroused from an imagined abuse scenario of an EEG based authentication system, where intruders might attempt to threaten an authorized user to log in to the system for them. For example by pointing a gun to the user's head to try forcing him to authenticate. Jesper thought this was a good point, and suggested that the authentication system should be based on relaxed records, cause as

he said “I believe you cannot be relaxed if you have a gun pointed to your head”.

### 3.1.7 Summarization of Interview

To summarize, the main outcomes of the interview are:

- The system should be based on visual stimuli using photographs of known faces.
- Brain-wave recordings of five seconds are enough.
- Vibration can be used as tactile feedback and as an alternative authentication mechanism for blind people.
- The problem with sensor placement is just a minor issue with the hardware available.
- The subject persons should be over 18 years old.

## 3.2 EEG Signal Preprocessing

This section describes the necessary algorithms for EEG signal preprocessing, by which means the raw EEG data is prepared for the further analysis and feature extraction. The preparation usually consists of the following steps: bandpass filtering, baseline removal, detrending, artifact removal and finally enhancing the useful EEG data using Independent Component Analysis.

One of the most basic and efficient approaches is the signal moving average technique.

### 3.2.1 Moving Average Computation

A moving average is a rolling mean function, which is a subclass of a finite impulse response filter used to analyse a set of points by creating a series of averages of different periods of the full data set [50].

The simple moving average (SMA) is represented as $y[j]$ of the given signal value (in our case the measurement of one sensor $x$ in the current point $j$ is calculated as a mean value of the signal in a certain period n. In this way the resulting signal y is made from the summation of all measurements $x_i$ divided by the number of points in this period, as shown in the following formula:

$$y[j] = \frac{\sum_{i=l+1}^{l+n} x[i]}{n}$$

*Formula 3.1: Simple moving average*

The value of a new signal $y[i]$ represents the aligned function's value in the current point $j$. By adjusting the value $l$ we can manipulate with the aligning interval which represents the delay of the mean of the given signal. In order to generate the mean of a signal without any delay or overtake, so that the aligned signal is fitting the raw signal, it is necessary to generate a *centred moving average (CMA)*, as presented further.

If $n$ is an odd number ($n = 2h + 1$), $l = j - h - 1$, $j - h >= 0$ *and* $j + h <= m$, then we get the following formula represented below, which is called as *centred moving average* (the delay will be equal to the overtake – this ensures the best fit of the aligned signal to it's original raw signal, therefore is the best choice for the EEG signal alignment).

$$y[j] = \frac{\sum_{i=j-h}^{j+h} x[i]}{n}$$

*Formula 3.2: Centred moving average*

Figure 5 below represents the one dimensional signal of the raw EEG recording from one sensor (blue line) and it's centred moving average representation (green line).

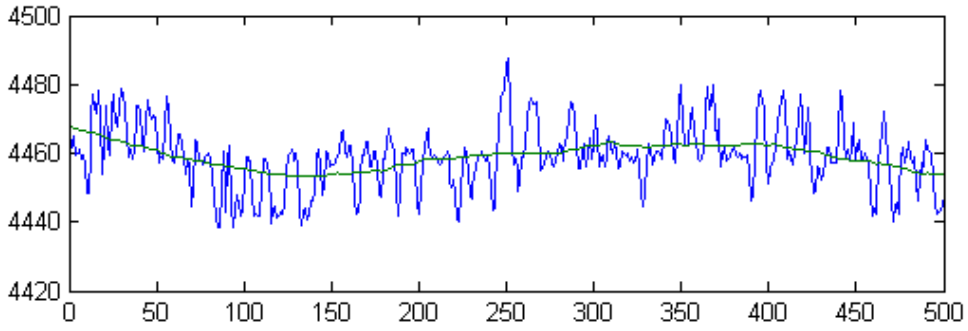


*Figure 5: The raw EEG signal of 500 samples from one sensor and it's centered moving average of 128 samples as the baseline*

Subtracting the above function from the raw EEG signal will ensure the de-trending and the baseline removal from the given EEG signal at once, therefore the computation is relatively efficient. The value of a new signal $z[i] = x[i] - y[i]$ represents the detrended function's value which is computed for each signal point $i$, where $x[i]$ is a raw EEG signal and $y[i]$ is it's centered moving average function. Figure 6 below represents the detrended EEG signal $z[i]$ distributed around 0 value which is a result of the green line subtraction from the blue line (see Figure 5 above).

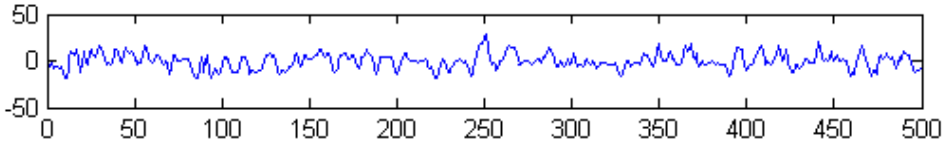


*Figure 6: Detrended EEG signal distributed across 0 value*

In case we need to apply this formula for a real-time EEG signal, we have to transform it to a recursive form, which means that each sequential alignment value $y[i]$ is derived from the previous one $y[j-1]$ and therefore ensures that the complexity (computational time) of the algorithm is significantly lower.

$$y[j] = y[j-1] + \frac{1}{n}\left(x[j] - x[j-n]\right)$$

*Formula 3.3: Recursive form of the left-sided simple moving average function*

In many cases there will be a need to calculate the moving average from the already existing moving average values $y[1]$, $y[2]$ ..., $y[j-1]$, which will lead to a higher level of a signal alignment. This approach is called as a *modified moving average – MMA* and can be calculated in the following way:

$$y[j] = \frac{1}{n}\left(\sum_{i=j-n+1}^{j-1} y[i] + x[j]\right)$$

*Formula 3.4: Recursive form of the modified moving average function*

Many other moving average calculation approaches exist to the current knowledge, such as cumulative moving average, weighted moving average [51], exponential moving average [52], but these approaches are not useful for our problem. The significance of EEG data measurements does not change over time, therefore we should not adjust weights for each data point.

### 3.2.2 Independent Component Analysis

As it is assumed in general, that EEG recordings are linear mixtures (combinations) of the underlying brain sources [53], it might be beneficial to extract the sources by employing blind source separation (BSS) techniques for our authentication approach. Among BSS techniques, Independent Components analysis (ICA) has been investigated for EEG analysis to derive mutually independent sources from highly correlated scalp EEG recordings. The main goal of ICA is to remove the influences of the sources on each other.

The idea behind is derived from the “cocktail party problem” [54], when it is possible

to use several microphones to filter out useless audio sound from surroundings and to amplify speech from specific persons in the conversation, but in our case there would be signals from the EEG sensors. In the perfect case, it is necessary to know the exact location of the signals we are looking for, so very often magnetic resonance imaging techniques are beneficial for scanning the structure of the brain.

A classical EEG generation and acquisition model is presented in Figure 7, conceptually representing how several underlying signals are mixed and captured via EEG sensors.

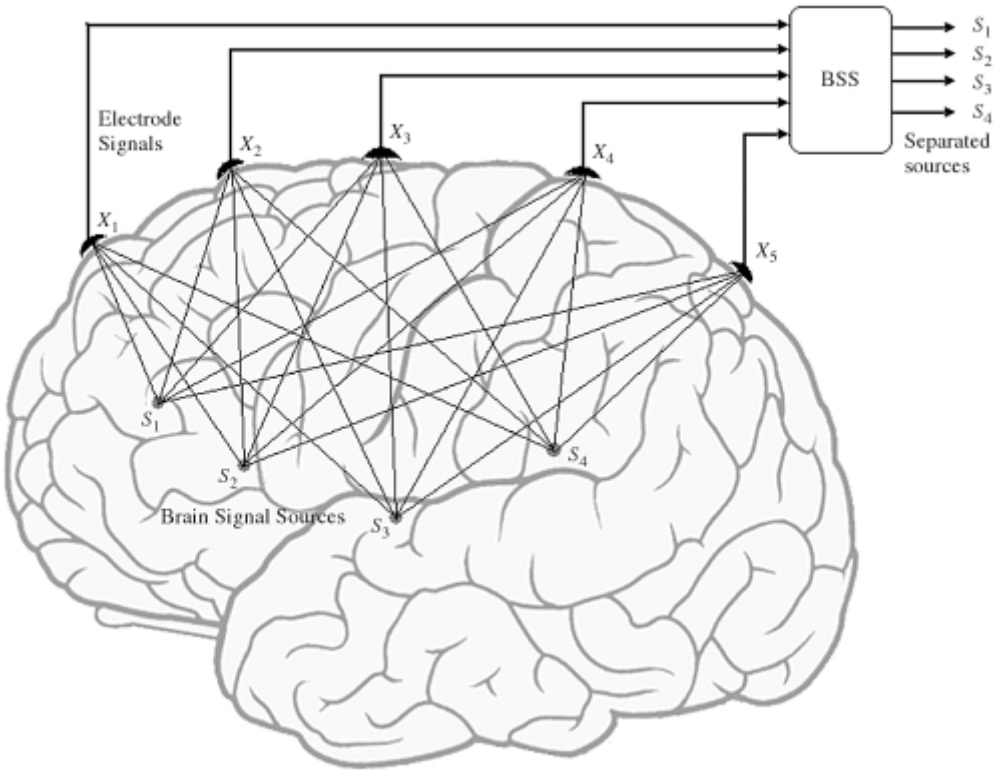


*Figure 7: BSS concept: EEG linear mixture model (of four signal sources) and blind separation of the underlying EEG signals [16, p. 87]*

Subsequently, the EEG mixture can be written as X = AS, where X are the observations (electrodes), A is the mixing system (anatomical structure) and S are the original sources.

When the independence assumption is correct, blind ICA separation of a mixed signal gives very good results. It is also used for signals that are not supposed to be generated by a mixing for analysis purposes. A simple application of ICA is the "cocktail party problem", where the underlying speech signals are separated from a sample data consisting of people talking simultaneously in a room. Usually the problem is simplified by assuming no time delays or echoes. An important note to consider is that

if N sources are present, at least N observations (e.g. microphones) are needed to get the original signals.

## 3.3 EEG-based Feature Extraction Algorithms

This section describes the potentially unique EEG features that can be used for the EEG-based biometric authentication system.

### 3.3.1 Zero-Crossing Rate

As suggested by DSP expert Per Lynggaard, a first potential unique feature could be zero-crossing rate of a detrended raw EEG signal with a certain period of time. The zero-crossing rate is the rate of sign-changes along a signal, i.e. the rate at which the signal changes from positive to negative or back. This feature has been used heavily in both speech recognition and music information retrieval, being a key feature to classify percussive sounds [55, pp. 146–147].

ZCR can be calculated as follows:

$$ZCR = \frac{1}{(T-1)} \sum_{t=1}^{T-1} I\{x(t)\,x(t-1) < 0\}$$

*Formula 3.5: Zero-crossing rate of a signal period T*

With the formula above we can calculate the total number of signal crossings of zero value for a certain period *T*. The indicator function $I\{x(t)x(t-1)<0\}$ is equal to 1, if the current x(t) value is below zero and the previous $x(t-1)$ value is over zero or the current x(t) value is over zero and the previous $x(t-1)$ value is below zero. Otherwise the indicator function is equal to 0. The most optimized approach is to count "positive-going" or "negative-going" crossings, rather than all the crossings, since, logically, between a pair of adjacent positive zero-crossings there must be one and only one negative zero-crossing.

### 3.3.2 Power Spectral Density

Power spectral density (PSD) is a positive real function of a frequency variable associated with a stationary stochastic process [16, p. 55], representing the measure of the power strength at each frequency (be showing at which frequencies variations are strong and at which frequencies variations are weak). The unit of PSD is energy per frequency (width). Computation of PSD can be done directly by the method of Fast Fourier Transform (FFT) or computing auto-correlation function and then transforming it.

### 3.3.3 Coherence

Coherence is a linear correlation measure between two signals represented as a frequency function. It uncovers the correlation between two signals at different frequencies and is often applied for the EEG signal analysis at hospitals [56, p. 12]. Usually it is used for analysing the condition of different cognitive disorders [56, p. 46]. It has already been proved that EEG-based coherence analysis can be used in biometrics [57, p. 51]. The formula below represents the magnitude of the squared coherence estimate, which is a frequency function with values ranging from 0 to 1, quantizes how well *x* corresponds to *y* at each frequency. The coherence $C_{xy}(f)$ is a function of the power spectral density $P_{xx}$ and $P_{yy}$ of x and y and the cross-power spectral density $P_{xy}$ of x and y, as defined in Formula 3.6 below:

$$Cxy(f) = \frac{(|(Pxy(f))|)^2}{(Pxx(f)\,Pyy(f))}$$

*Formula 3.6: Coherence between two EEG sensors computation*

In our case, the EEG feature is represented by a set of points of the coherence function. The values x and y are de-trended and filtered raw EEG values in microvolts (μ) from two different electrodes. This function should be applied to all pairs of the data from EEG electrodes. Thus, if the number of electrodes exceeds, the size of the feature table exceeds exponentially. So we must keep in mind that we have to limit the number of sensors for the coherence analysis.

### 3.3.4 Cross-Correlation

The cross-correlation (CC) function represents the similarity of two signals as a function of a time-lag applied to one of them. It is also known as sliding dot product. Usually it is used to find occurrences of a known signal's sequence in an unknown one. For example, consider two real valued time sequences x and y that differ only by a time shift. We can calculate the cross-correlation to investigate how much y must be shifted to make it identical to x, as shown in Formula 3.7 below:

$$CCxy(\tau) = \frac{1}{(N-\tau)} \sum_{t=1}^{N-\tau} x(t+\tau)\,y(t)$$

*Formula 3.7: Cross-correlation between two signals x and y*

The EEG signals from two different sensors x and y should be detrended and

normalized (zero mean and unit variance), N is the number of the observations and τ is the delay. $CC_{xy}$ must be within the range [-1, 1]. If C < 0 then the correlation is inverse and both signals tend having similar absolute values but with opposite signs and C > 0 implies a direct correlation and a tendency of both signals having similar values with the same sign. If C = 0, then it indicates the lack of the linear dependency between two signals. In our case, the EEG feature can be represented by the set of points of the cross correlation function. To minimize the feature size, we can use the mean feature value of a certain recorded EEG signal period.

### 3.3.5 Wavelet Transform

Wavelet transform is a tool that converts a signal into a different form revealing the characteristics hidden in the original signal. The wavelet is a small wave that has an oscillating wavelike characteristic and has its energy concentrated in time. Wavelet transform enables variable window sizes in analysing different frequency components within a signal. In Figure 8 below we represent the wavelet coefficient extraction as a graphical representation:

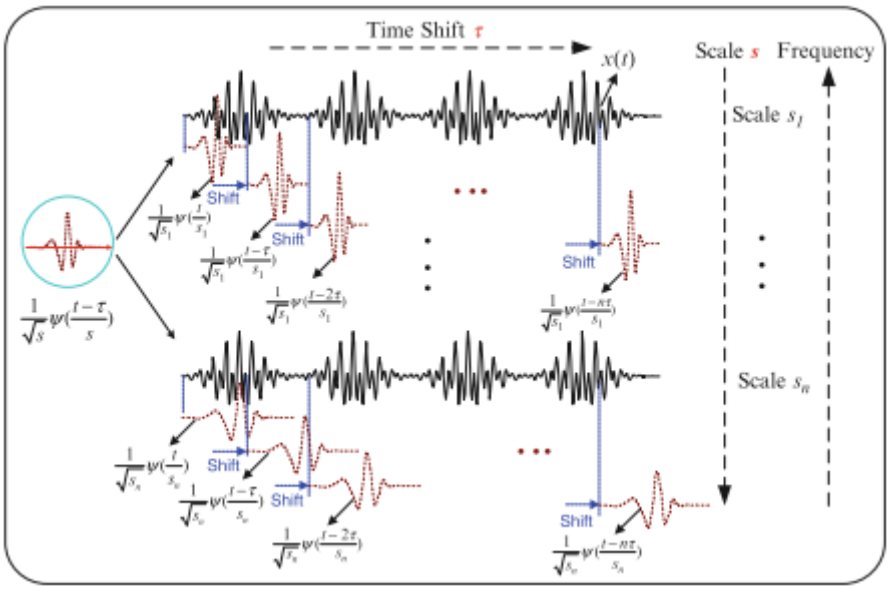


*Figure 8: Representation of the Wavelet transform by comparing the signal (black oscillations) with a set of functions obtained from the scaling and shift of a base wavelet*

The best waveforms (template functions) for the EEG data analysis are the Ricker (Mexican hat) and Morlet (Gabor) wavelets [58, p. 69], as illustrated in Figure 9:

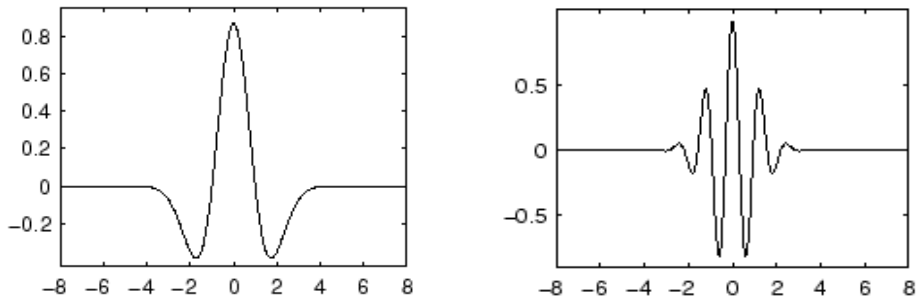


*Figure 9: Ricker (Mexican hat) wavelet on the left, Morlet (Gabor) wavelet on the right*

To extract unique dominating frequencies from signals and reveal the underlying dynamics that corresponds to these signals, a wavelet analysis technique is needed. Typically, the process of signal processing transforms a time domain signal into another domain since the characteristic information embedded within the time domain is not readily observable in its original form. Mathematically, this can be achieved by representing the time domain signal as a series of coefficients, based on a comparison between the signal x(t) and template functions $\{\Psi_n(t)\}$, as represented in Formula 3.8 below:

$$c_n = \int_{-\infty}^{\infty} x(t)\Psi_n^*(t)\,dt$$

*Formula 3.8: Time-domain wavelet signal coefficients*

The inner product between the functions x(t) and $\Psi_n(t)$ is represented in Formula 3.9 below:

$$(x, \Psi_n) = \int x(t)\Psi_n^*(t)\,dt$$

*Formula 3.9: The inner product between the given signal x and the template function (base wavelet)*

The inner product describes an operation of comparing the similarity between the signal and the template function, i.e. the degree of closeness between the two functions.

## 3.4 Experiments

Based on our gained experience from the literature review and the interviews, we have settled on the following procedure (see Figure 10 below) for the EEG measurement experiments and the analysis of the collected data.

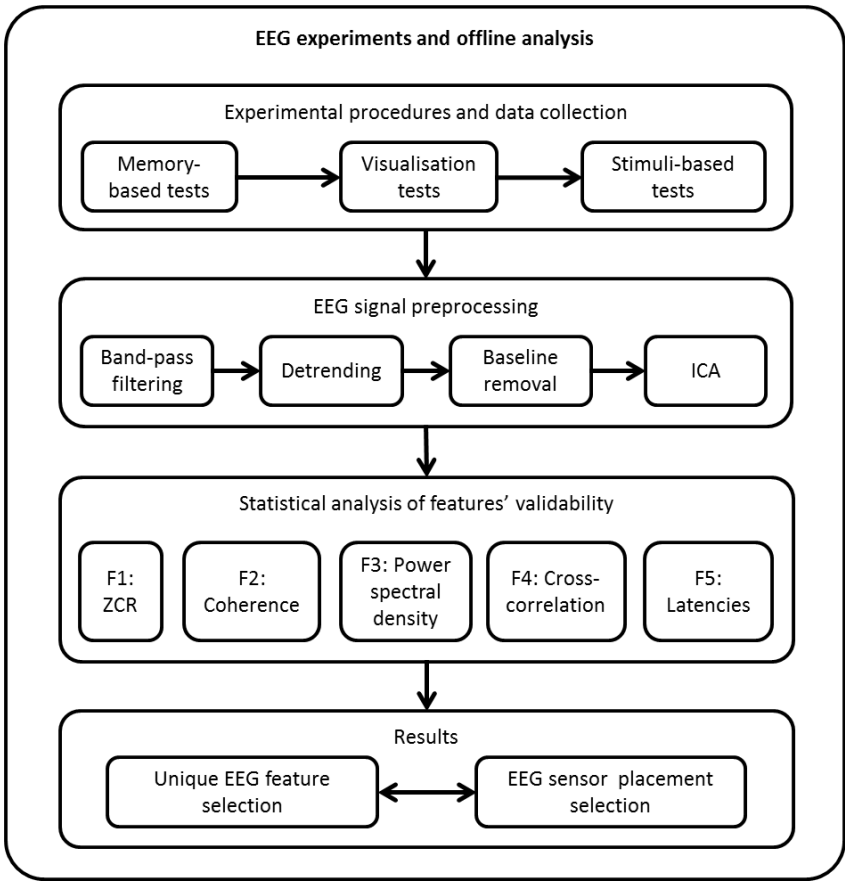


*Figure 10: Organization of the experiments and analysis of collected data*

The above figure illustrates the four main sequential steps of the experimental study intended for obtaining the sufficient knowledge needed for the further prototype design and development.

### 3.4.1 Experimental Goal

This study was performed with three main goals in mind. The first goal was to understand if it is possible to differentiate between several subject persons based only on their EEG measurements. The second goal was to find what is the most efficient mental task or stimulator (memory-based thought, visualisation, or stimuli-based brain reaction) for capturing brain-waves for authentication purpose. Finally, the third goal was to analyse whether it is feasible to distinguish between different *pass-thoughts* [9] of one individual, so that he or she can use a specific *thought* as a password in order to authenticate in a system. Such option is interesting because it covers the "something you know" authentication class (see 2.2 Authentication Systems on page 18), which would raise the security level of the system in general.

### 3.4.2 Experimental Setup

This section describes the technical setup and the ambient environment of the experiments.

The EEG measurements were obtained based on the Emotiv EPOC research EEG neuroheadset: a 14 channel (plus CMS/DRL references, P3/P4 locations) high resolution, neuro-signal acquisition and processing wireless neuroheadset [59]. Channel names based on the International 10-20 locations [60] are: AF3, AF4, F3, F4, F7, F8, FC5, FC6, P7, P8, T7, T8, O1, O2. The sampling rate of the Emotiv EEG headset is 128 Hz on the output (to ensure the precise output values, the Emotiv headset has the internal sampling rate of 2048 Hz frequency) with 1.95μV least significant bit (LSB) voltage resolution, therefore it is possible to detect VEPs (which can be beneficial to deduce latencies of electrical impulse exchange representing uniqueness of neural-wiring of subjects' brains), since average amplitude for VEP waves usually falls between 5 and 10 microvolts [61, p. 153].

The actual sensor placement is shown in the figure below:

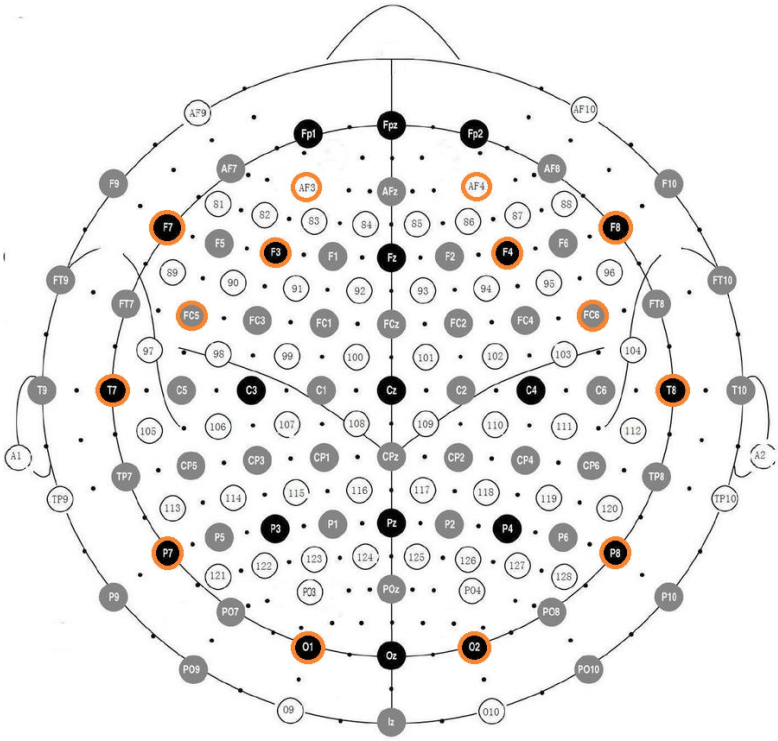


*Figure 11: The map of the International 10-20 EEG sensor locations. [77] The sensor placements of the Emotiv EPOC EEG headset are marked in orange color. The EEG data recorded from these locations were used for analysis.*

To establish a good connection between the scalp and EEG electrodes, the saline liquid solution was put on every electrode before each experiment. However, several times it

was necessary to redo the experimental procedures, after checking if the EEG data is valid or not for the further analysis. The below figure shows the example raw EEG data (with removed baseline) of 10 seconds from the marked sensors of the Emotiv EPOC EEG headset, which we had to reject due to the heart rate artifact appearance:

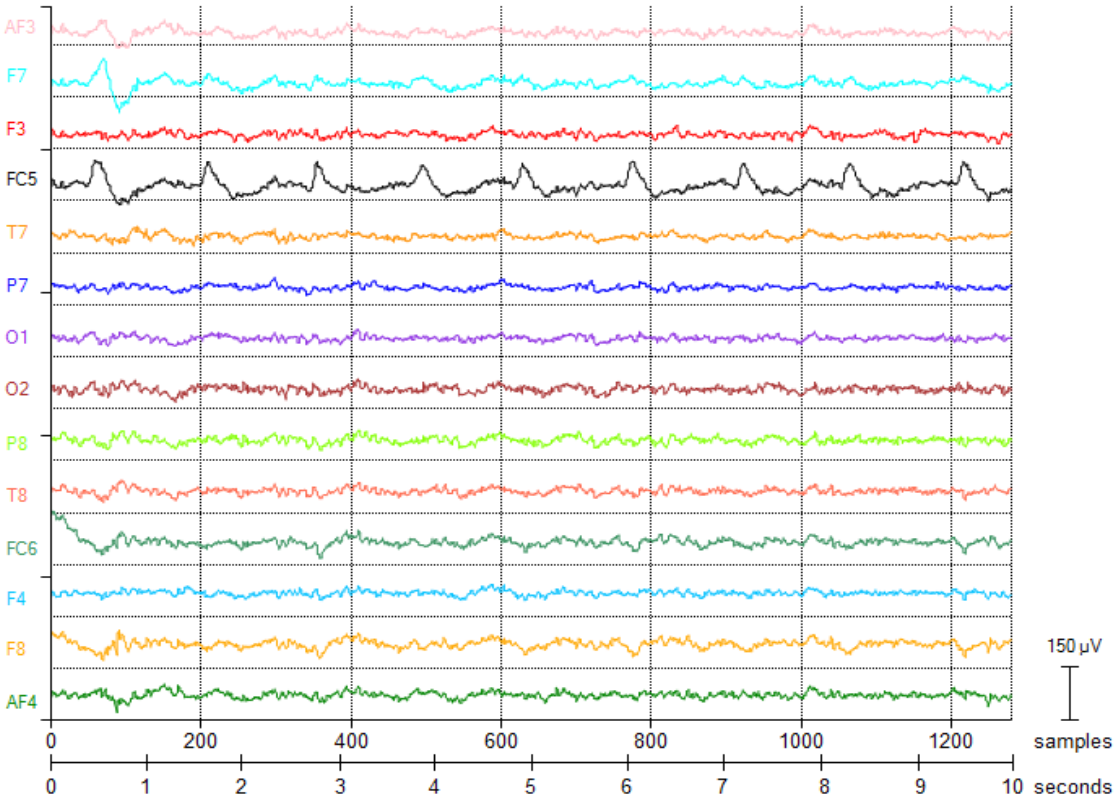


*Figure 12: Example of detrended EEG data received from one test person with the Emotiv EPOC headset. The data received from FC5 sensor (black line) contains heart rate artifacts (9 peaks with approximately 1 second interval), because it's location coincided with the blood vessel on the subject's head. Thus it was necessary to readjust the headset and to ensure symmetry of sensor placement.*

We used the TestBench™ research software packet included in the Emotiv Research Edition SDK which provided the recording option of the EEG data files in binary EEGLAB format.

For the experiment we have synchronized the visual output of pictures with an EEG data recording. Real-time emotional data was also extracted at the same time based on the Emotiv Control Panel. When the emotion models are used in real-time, the system performs self-scaling. In such a way it is able to adapt to the base point and range of emotions of the current subject. A study proves that the Emotiv EEG headset is a valid device for measuring EEG and evaluating the subjective emotional parameters of subjects and has a high level of reliability [62]. We considered this as contextual information which can later be beneficial for a more thorough analysis, e.g. how emotional states can influence the uniqueness of the subject's brain-waves.

### 3.4.3 Experimental Procedures

In order to identify what are the most efficient EEG feature stimulations, we have conducted several tests with healthy subjects, who are older than 18 years old – as suggested from the interview.

As mentioned in the 3.4.1 Experimental Goal section on page 38, the main aim of the EEG measurement experiments was to reveal unique EEG features of each subject and to investigate, whether the subject has a unique brain activity during different mental tasks. Therefore, we conducted 3 separated experimental sessions (3 different days) with healthy subjects. The experiment took place in a quiet closed room with covered windows. We asked our subjects to sit in a normal office chair, with relaxed arms lying on their legs. We divided our test in two different approaches: imagination based tests (first part) and tests based on visual stimuli (second and third part). According to the interview with Jesper Rønager [47], we have settled on visual oriented experiments explained further. Therefore, we will focus mainly on the four sensors on the back of the head, specifically O1, O2, P7, P8, as illustrated in Figure 11 on page 39.

First, the imagination based tests consisted of the following experimental tasks with closed eyes. The tests lasted 10 seconds each with approximately 30 seconds break and repeated 10 times per subject:

1) Imagination of red capital letter “A”;
2) Imagination of red capital letter “B”;
3) Imagination of running brown Labrador dog;
4) Imagination of waving the right arm.

In the second part of our experiments, we recorded the subjects' brain-waves while they were looking at 3 different images, which were changing sequentially. These images were following:

1) Image 01: Green grass (chosen by Subject No. 1);
2) Image 02: Boxer with blood (chosen by Subject No. 2);
3) Image 03: Jumping man (randomly chosen).

In the third part of our experiments, we recorded the subjects' brain-waves while they were looking at 5 different famous face images, which were changing randomly. These images were following:

1) Barack Obama;

2) Elvis Presley;

3) Albert Einstein;

4) Angelina Jolie;

5) Chuck Norris.

As we already know, the time-frequency analysis can distort the signal at both ends of the recording. Therefore we must make sure we do not lose important data and that the baseline recording is still long enough after cutting off the affected portions. The affected recording length depends on the frequency in an inverse manner. In the final system, the recording should not be too long nevertheless; the longer it is the bigger the risk that an artifact appears.

### 3.4.4 Software Tools Used for Analysis

This section briefly presents the various software tools used for experimental analysis.

#### *MATLAB*

MATLAB[3] is a high level technical computing language and graphical interface used for intensive mathematically computations. It is designed to be more efficient and more accurate than typical programming languages like C++ and Java. It provides users with various tools for data analysis and visualization, and will be the primary tool used in this project for accessing the effectiveness and sensitivity of any developed algorithms. The software also provides various toolboxes designed specifically for use in Bioinformatics.

#### *EEGLAB*

EEGLAB[4] is a MATLAB toolbox distributed under the free GNU GPL license for processing data from electroencephalography (EEG), magnetoencephalography (MEG), and other electrophysiological signals. Along with all the basic processing tools, EEGLAB implements independent component analysis (ICA), time-frequency analysis, artifact rejection, and several modes of data visualization. EEGLAB allows importing electrophysiological data in about 20 binary file formats, to pre-process the data, to visualize activity in single trials, and to perform ICA. This is a useful feature of the software, because the artifactual ICA components may be subtracted from the data, which serves as a data enhancing technique.

3 http://www.matlab.com
4 http://www.eeglab.org

### *OpenVIBE*

OpenVIBE[5] is a software platform dedicated to designing, testing and using brain-computer interfaces, intended for real-time processing of brain signals. It can be used to acquire, filter, process, classify and visualize brain signals in real time.

OpenViBE is free and open source multi-platform software. OpenViBE can use a vast selection of hardware EEG devices, including the Emotiv EPOC headset, which is used as the main EEG data measurement device in our project.

### *Emotiv Research SDK*

The Emotiv's Research Edition SDK[6] is a single user license program for independent researchers intended to conduct EEG research leveraging the Emotiv EEG technology. We have used the TestBench™ software included in the Research Edition SDK which provided us the following option we used for the measurements: recording EEG data files in the binary EEGLAB (.edf) format. Command line file converter included to produce .csv format.

## 3.4.5 Results and Discussion

In this section we present the main findings of EEG signal analysis, presenting the EEG characteristics as unique biometric identifiers.

The statistical analysis revealed the significant differences between different subject persons (but not between different mental-tasks or visual stimuli within one person) in terms of the present waveforms and powers of electrical bio-potential differences (as mean μV values and corresponding histograms, as seen in Figure 13 and Figure 14).

5 http://openvibe.inria.fr
6 http://emotiv.com/store/sdk/bci/research-edition-sdk/

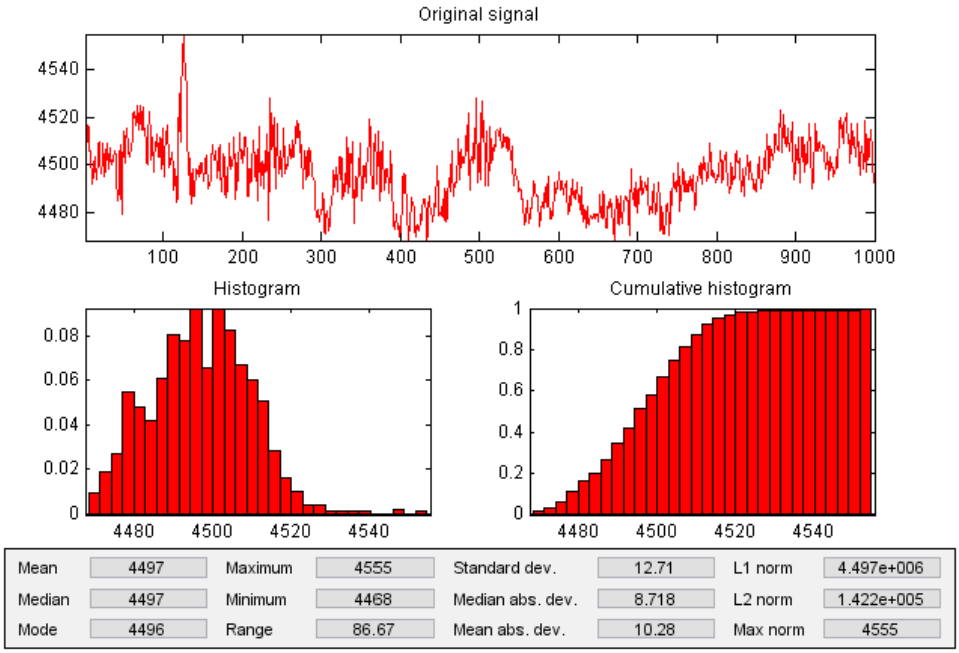


*Figure 13: Statistical analysis of the mean EEG powers of subject Nr. 1*

The below figure represents the statistical EEG data of the same mental task but conducted from the different subject:

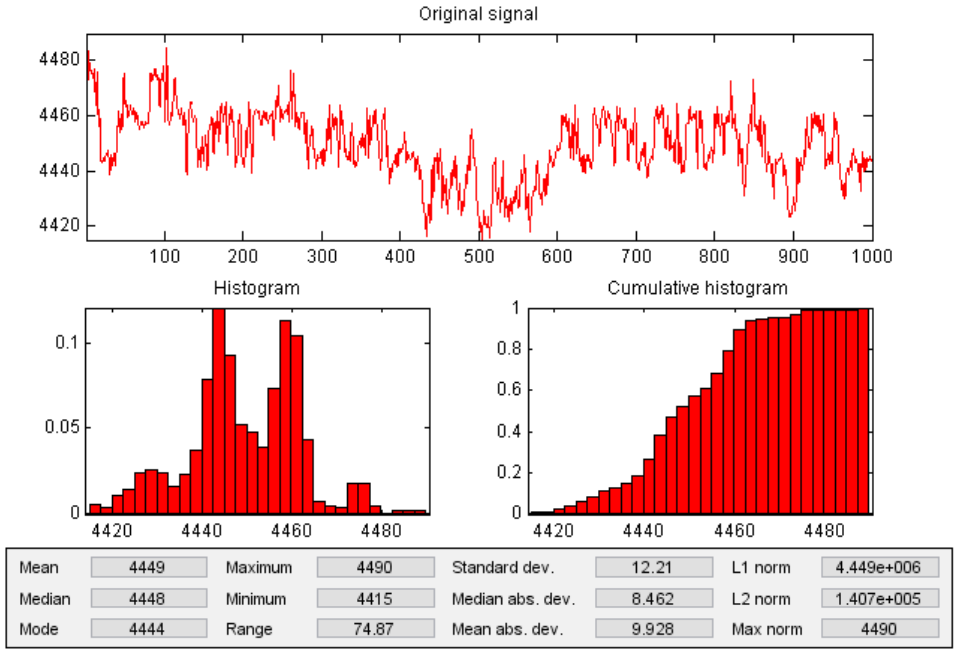


*Figure 14: Statistical analysis of the mean EEG powers of subject Nr. 2 (within the same mental task as in Figure 13 above)*

We found that the Power Spectral Density also reveal unique patterns for each subject, and the difference is obvious in the figure below (See Spectrogram differences). For statistical analysis we have computed the mean values of histograms from the power spectral densities, to mark the dominating frequencies in EEG signals during visual

stimulations of each subject. The most significant differences were found in signals obtained from the sensors O1, O2, P7, P8, which confirms the suggestion of Jesper Rønager, to base the system mainly on visual cortex area. Figure 15 below represents the example of processed EEG data from these four sensors and corresponding spectrograms.

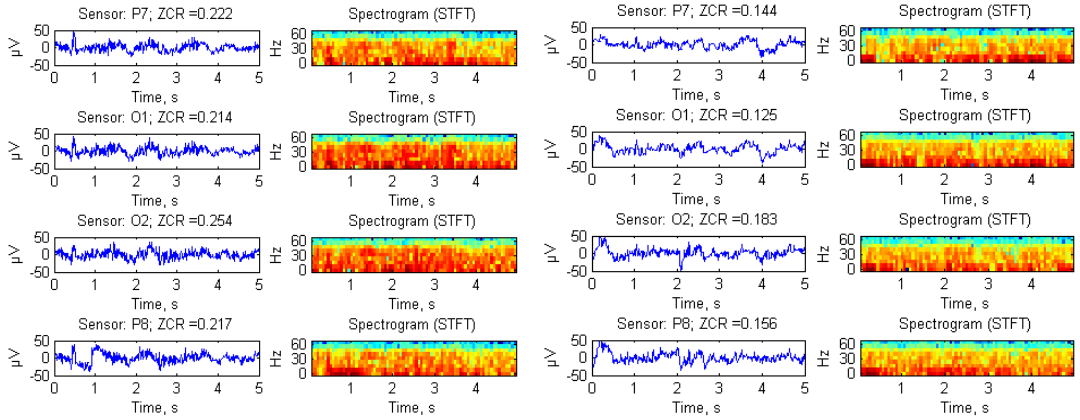


*Figure 15: Detrended EEG data from O1, O2, P7, P8 sensors and it's zero crossing rates (ZCR) values of 5 s period, and corresponding Power Spectral Density illustrations (as a spectrogram computed based on STFT). The two columns on the left corresponds to subject Nr.1, and two columns on the right corresponds to subject Nr.2.*

From the visual representation of power spectral densities (see Spectrograms in Figure 15) it is relatively hard to distinguish differences between the subjects by just looking at them. However, this helped us to select the most significant frequency range which revealed the highest differences of PSD values among subjects, but remained relatively similar within one individual's values. We present the mean values of the ZCR feature intended for biometric authentication application in Figure 16.

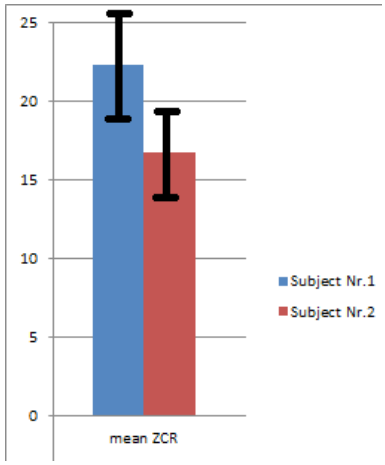


*Figure 16: Mean zero crossing rate feature of two subjects with a black marker indicating standard deviation (SD) of each subject*

As these results show, the ZCR of the detrended and denoised EEG signal from the four sensors can also serve as a unique biometric feature.

Furthermore we have decomposed the EEG signals with the 8-level discrete wavelet transform (DWT), and the Mexican hat wavelet showed the most reliable results of detecting the moment, when the famous person image appeared on the smartphone screen and was shown to the subject instantly. This moment is detected in the O1 and O2 sensor measurements with a delay of approximately 120 milliseconds after the stimuli appearance and can be detected as an overrun of 8 μV amplitude high-frequency bursts (see figure below, marked with a red square on the component $d_1$, representing the highest frequencies and the lowest amplitudes of the signal). The burst size and structure is different from subject to subject and can be beneficial for usage as a unique identifier.

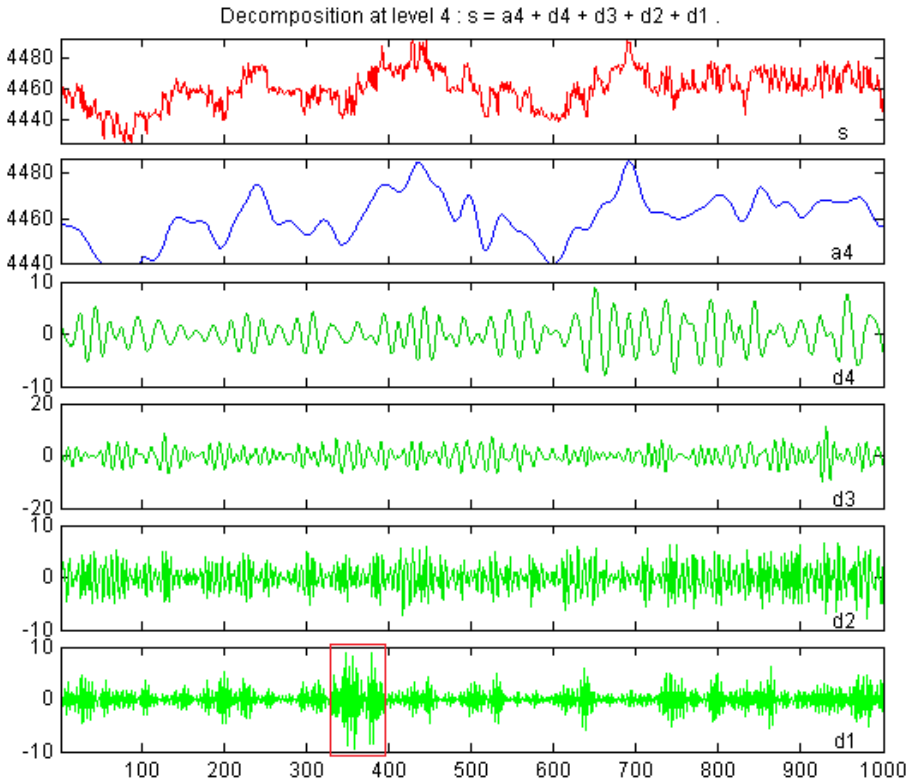


*Figure 17: Four-level Mexican hat wavelet decomposition of the original signal obtained from the O1 sensor (red color), with a trend component (blue color) and four-level wavelet components (green color). Red indicator shows the visual stimuli related burst, detected in approx. 120 ms after the appearance of a famous person face picture on the smartphone screen.*

For the development of the prototype, this information is useful for extracting the latencies of how fast electrical signals are travelling among the neural wiring. Since we can extract the exact time-stamp of the moment when the password picture is shown to the user, we are can calculate the latency time from the moment of picture appearance to the moment, when the visual stimuli signal is reached the occipital cortex and is registered by the sensors O1 and O2. To improve the precision of the detection, higher level of the DWT decomposition (using Mexican hat template wavelet) can be used.

# 4 Practical System Implementation

This chapter describes how the prototype system is implemented and the various decision and design considerations are explained in depth. In general the prototype is divided into two major parts (in addition to the EEG headset); a front-end part located on an Android smartphone responsible for user interaction and a back-end part located on a remote server responsible for processing EEG data and handling the authentication algorithms. The overall architecture is a client-server model, and in the following sections we will refer to the client as front-end, and the server as back-end. This chapter starts off with introducing the requirement specification for the system, followed by an overview of the system architecture, followed by in-depth description of the front-end and then the back-end, and finally the exchange protocol used for communication between the two is described.

## 4.1 Requirement Specification

In this section, the requirement specification for the system is presented. Each requirement consists of a unique ID, a description and a priority. Furthermore, it is indicated whether the requirements are functional (F) or non-functional (NF). The priorities are expressed using the MoSCoW prioritization method [63]. In this project, the capital letters in MoSCoW are interpreted as follows:

- **M**ust: this requirement must be fulfilled.
- **S**hould: this requirement should be fulfilled, but it is not critical.
- **C**ould: this requirement is not mandatory, and less critical.
- **W**on't: this requirement will not be fulfilled, but would be nice to have in a future implementation.

| ID | Requirement | Priority | F/NF |
|---|---|---|---|
| R1 | The system shall use an EEG headset to measure brain-waves. | M | NF |
| R2 | The system shall be tailored to a smartphone device. | M | NF |
| R3 | The system shall be based on visual stimuli using photographs of known faces. | M | NF |
| R4 | The system shall record brain-waves from the sensors P7, P8, O1 and O2 (defined by the international 10–20 system of electrode placement [18, p. 140]). | M | NF |
| R5 | The system shall use 5 seconds brain-wave recordings as basis for authentication processing. | M | F |
| R6 | The system shall ensure that users are over 18 years old. | C | F |
| R7 | The system shall ensure that the user is not moving while recording brain-waves. | S | F |
| R8 | The system shall use the smartphone's built-in camera to detect if there's a face in front of the smartphone while recording brain-waves. | S | F |
| R9 | The system shall use a face recognition algorithm to detect if the right user is in front of the camera. | W | F |
| R10 | The system shall use the smartphone's vibrator to give tactile feedback to the user, indicating that the authentication process is starting. | C | F |
| R11 | The system shall process recorded brain-waves on a remote server, containing user information. | M | F |

*Table 1: Requirement specification for the system.*

The majority of the requirements are derived from our literature study about how EEG can be used for authentication purposes as well as from the suggestions from Jesper Rønager [47]. The requirements are not necessarily saying anything about exactly which technologies and hardware devices that should be used. The remainder of this chapter will deal with these decisions and design considerations, and present different possible approaches and explain the choices made.

## 4.2 System Architecture

The overall system architecture from the hardware and communication perspective is illustrated in Figure 18 below.

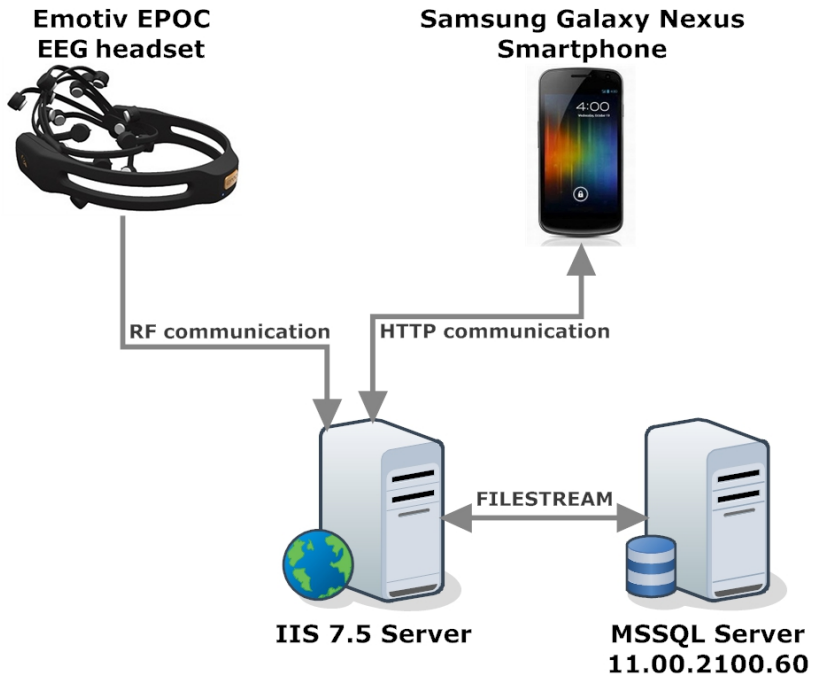


*Figure 18: System architecture diagram.*
*The Emotiv EPOC headset is responsible for EEG signal transmission. The Samsung Galaxy Nexus Smartphone is runnig the front-end part, which communicates with an IIS 7.5 server running the back-end part responsible for data exchange with a MSSQL database.*

### 4.2.1 Smartphone Device

As the system is tailored for mobile use, it is necessary to implement it in a modern smartphone environment with access to various context triggers like web, camera and accelerometer among others. According to the information technology research and advisory firm Gartner Inc., the worldwide market share of smartphone systems in the fourth quarter of 2011 is dominated by the Android system from Google (50.9 %), iOS from Apple (23.8 %) and Symbian from Nokia (11.7 %) [64]. Besides having the biggest market share, the Android system is also relatively easily accessible from a development point of view, since a Software Development Kit is provided free of charge and the system itself is open source [65].

These circumstances formed the decision to base the front-end part of the prototype on the Android platform. Specifically, a Samsung Galaxy Nexus smartphone running Android version 4.0.4 (Ice Cream Sandwich) is used as the main testing device. This device features a 1.3 megapixel front camera as well as a 5 megapixel rear camera. The front camera can be used to unlock the phone using facial recognition software, which is built in natively in the new Android 4.0 version. Besides that, the device also includes support for the wireless communication technology Near Field Communication (NFC), capable of establishing a radio connection between the device and an item or endpoint with a RFID tag.

### 4.2.2 EEG Headset

After analysing currently available EEG headsets on the market [6] we decided to use the Emotiv EPOC Developer neuroheadset to use for development of the prototype solution. The Emotiv EPOC EEG headset has 14 saline electrodes with two reference sensors and is recognized as a high-fidelity EEG device designed for practical consumer applications [59]. As all incoming data from the Emotiv EPOC headset are encrypted, it must first be decrypted before applying further digital signal processing techniques.

## 4.3 Technical Front-end Setup

The front-end side of the prototype is implemented as a native Android application aimed for minimum API level 14 (Android 4.0 and upwards). Even tough the application is developed as a native Android application (thus written in Java with user interface files written in XML), a significant part of the app is written in standard web technologies like HTML, CSS and JavaScript. This is accomplished by using the Android WebView class, which is an Android View (essentially a piece of code controlling the look and appearance of an Android application) capable of displaying web pages with the Webkit rendering engine (the same rendering engine used in the default Android web browser).

The web code is built on top of jQuery Mobile[7], which is a framework optimized for mobile devices with touch interfaces, it is in itself based on the jQuery framework. In short, jQuery Mobile is optimized for most mobile platforms, and is restyling most normal web page elements like headers, links, lists and form elements including text inputs, buttons and checkboxes to a mobile-optimized version appearing the same across various platforms. A screenshot of the frontpage styled with jQuery Mobile can be seen in Figure 19.

7 http://jquerymobile.com/

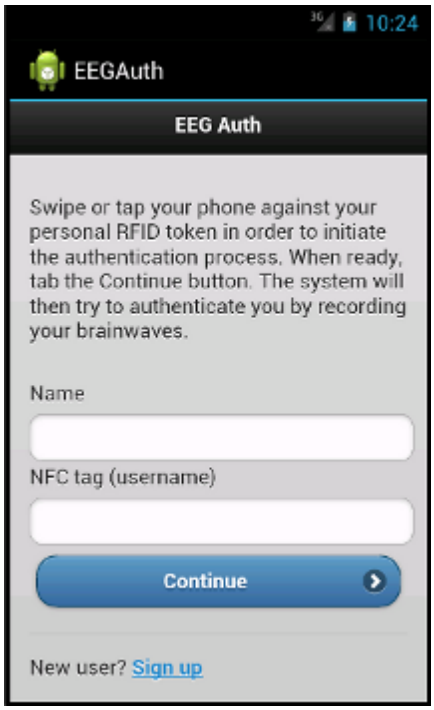


*Figure 19: Screenshot of the EEGAuth frontpage styled with jQuery Mobile.*

The reason for choosing to implement most of the graphical user interface with web technologies is the rapid prototype capabilities of current web technologies. Also, it makes the code more portable, if one should decide to implement the system on a different platform.

On the other hand, the reason for not fully implementing the app as a web application instead of a native app, is because of the necessary integration with hardware like camera, accelerometer and vibrator. To use the camera, the application needs to communicate closely with the core system. This is not (yet) possible to achieve directly from a web interface, and therefore this bridge between a Java and JavaScript environment has been implemented.

There are initiatives though, which strive to create a framework for developing mobile apps in HTML5 and offer access to the phone's various context triggers. Examples of such frameworks are Phonegap[8] or Titanium from Appcelerator[9]. Whilst these frameworks have come a long way, none of them are perfect, and it will take some time before an HTML5 based framework can offer the same functionality as any native mobile platform.

8 http://phonegap.com/
9 http://www.appcelerator.com/

### 4.3.1 Front-end System Flow

Prior to recording the user's brain-waves in order to authenticate him or her, several steps must be carried out. Since the prototype system is an authentication system whose sole purpose is to give an answer to the question "Is the user actually who he or she claims to be?" the system must begin with allowing users to make such claim. As explained earlier, the more of the three classes, something you know, have or are, a system can incorporate, the more secure the system is. The something you have class can be put into practice in this case by demanding that the user verifies his or her identity with an item containing a chip the system can read. Such an item could be a smart card, ID card or even a wristband or finger ring containing an electronic chip. By taking advantage of the NFC technology built into the Android device, the user must swipe his or her personal item containing an RFID tag against the device in order to initiate the authentication process. Besides knowing other significant credential's of the user, an intruder also has to steal this item in order to bypass the authentication system. In the System Usage chapter later in this report, the various security matters of the system including description of assurance levels will be analyzed in depth.

The entire front-end system flow from the perspective of the user is illustrated in Figure 20 below.

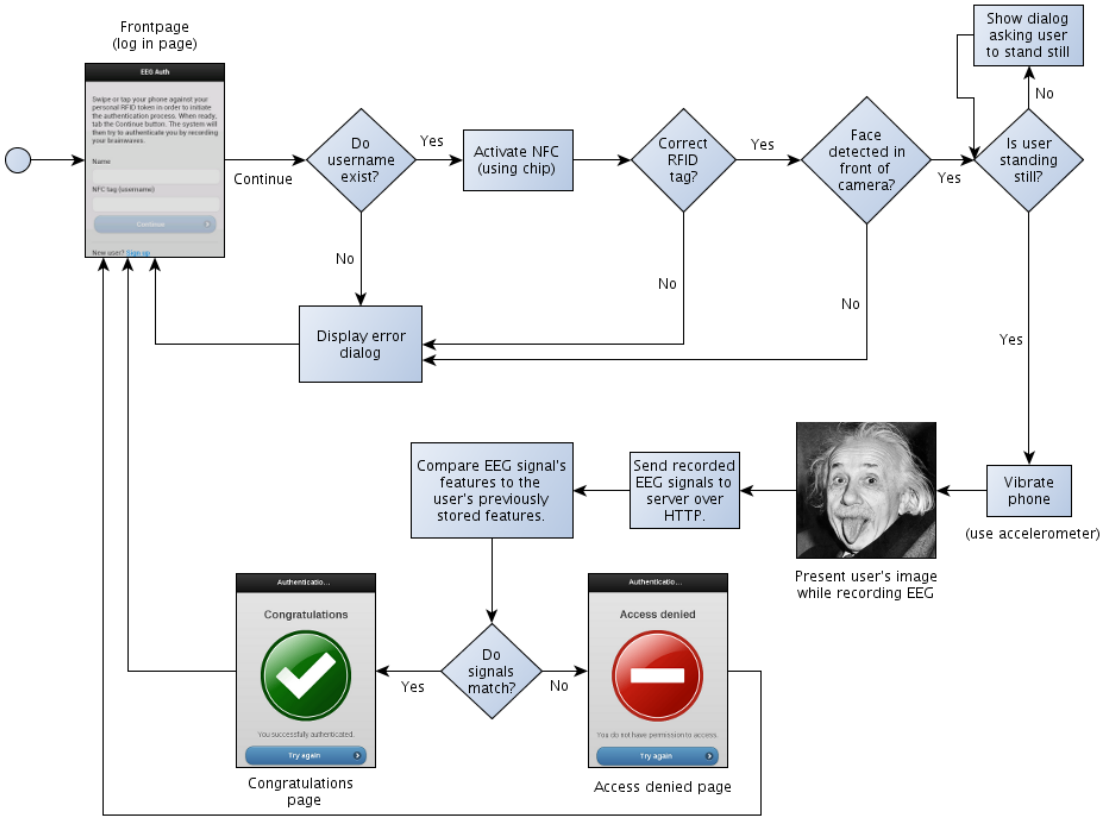


*Figure 20: Flowchart representing the authentication steps in the front-end. The diagram centers around a frontpage, and shows how the user can try to authenticate using an existing user profile.*

The illustration doesn't directly show what is happening on the back-end side, as it is described in depth in the back-end section, but behind the scenes the front-end will establish a connection to the back-end server when decisions important for the authentication process must be taken.

To start the authentication process, the user must swipe an RFID tag against the phone. The front-end will then ask the back-end whether a user profile matching this RFID tag exists. This is synonymous to making a claim about a user identity. If a user profile exists, the process continues, otherwise it stops here with an error dialog. Assuming we are dealing with a valid RFID tag that corresponds to a known user, the systems proceeds with face and motion detection flows, in order to validate if there's actually a user in front of the camera standing relatively still. More about that shortly. The remainder of Figure 20 shows the flow for authenticating the user with EEG.

Figure 21 shows the flow of creating a new user. This flow is not fully implemented in the prototype system, but implemented visually to give an idea about the whole concept. Hence a user will not actually be created if completing this part of the flow. Instead the prototype as it is presented here operates with a set of defined user profiles.

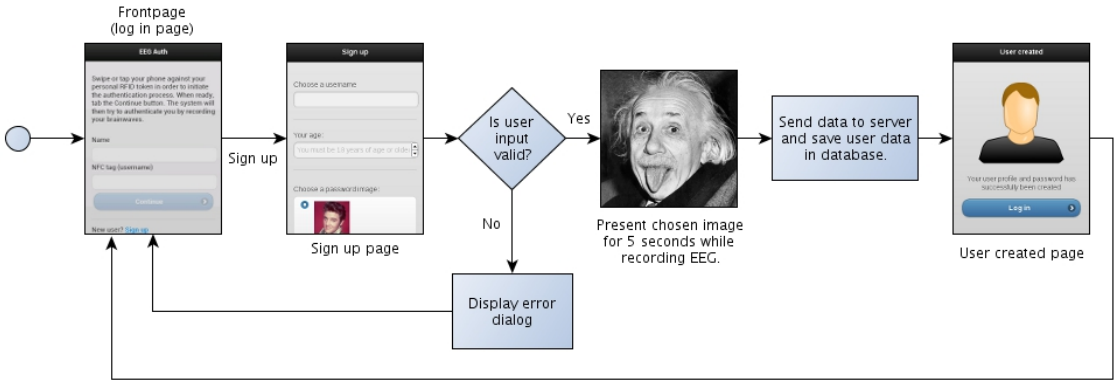


*Figure 21: Flow chart showing the user creation process in the front-end. The purpose of this scenario is to store user information in a database for later use, and create an initial recording of brain-wave data while the user is looking at a chosen image. This recording is the one any future recordings will be compared to in order to decide whether the user can be authenticated or not.*

These two main scenarios, user authentication and user creation are implemented as two separate use cases. The use case specifications can be seen in the appendices in Appendix 3 - Use Case Specifications on page 82.

### 4.3.2 Face Detection

The next couple of steps are implemented to make sure that the optimal circumstances and conditions of the user are met when recording EEG data from the headset. As Jesper Rønager explained, to get optimal EEG recordings tailored for authentication

purposes, the subject person should sit in a comfortable and relaxed position, stay relatively still, and concentrate his or her mind about a photograph of a person [47]. Therefore it is obvious to take advantage of the camera built into the smartphone to detect whether there's a person in front of the display or not. The Samsung Galaxy Nexus smartphone contains a front camera in addition to the traditional rear camera found on most smartphone devices. More and more smartphone models are shipped with a front camera [66], and we believe that this functionality could be more common on smartphone devices in the near future, if the right services or applications taking advantage of it prove their value. In the prototype, the system will therefore use the Face Detection functionality in Android 4.0 to detect if there is a face in front of the device [67]. Specifically, the system will show a page containing a live camera preview stream alongside with a text asking the user to place his or her face in front of the camera. The system will continuously scan the camera preview for faces, and in the moment exactly one face is detected, the user will be redirected to a new page where the authentication process continues.

One could argue that instead of showing the camera preview, the system could just indicate whether a face is detected with, say, a green button for a positive result, and a red for a negative. The reason why it is implemented with a camera preview in the prototype is due to limitations in the Android system, which requires that a camera preview must be active in order to detect a face. As this is only a software limitation, the concept of using a green/red face indicator is still valid.

Another inappropriateness of this limitation is that the system only ensures that there is a face in front of the display at the beginning of the authentication process, but if the user moves his or her face away from the display later, the system will not detect it. Optimally, the system should silently detect if there is a face in front of the display throughout the whole authentication process, and kindly ask the user to adjust if that is not the case.

In addition to detect a face, the camera could also be used for logging purposes in the authentication part of the system. The system could capture a picture of the person in front of the camera when someone tries to authenticate. This photo could be used in case of disputes or when an intruder is trying to gain unauthorized access after theft of an RFID token, further improving the overall security of the system.

### 4.3.3 Motion Detection

When a face has successfully been detected, it is time to check if the user is standing relatively still. As mentioned earlier, the best EEG data are measured from subject

persons who are standing still [47]. Thus the prototype system uses the built-in accelerometer to detect the movement level of the smartphone. The idea behind is that it should not be possible to continue with the authentication process, if the phone (and, consequently, the headset) is shaken too much or if the user is currently moving from one spot to another.

The Android system offers accelerometer data as three values indicating the position of the phone in a three-dimensional space. We name these values X, Y and Z. Android doesn't directly offer a kind of motion indicator, thus a custom algorithm is implemented in the prototype to detect movement of the phone. The three accelerometer values are read twice every second, saving the last measured values as well as the second-last measured values for further calculcations (giving six values in total). The calculated shake value, ω, is given by the following formula, which is implemented in the front-end:

$$\omega = \frac{\frac{|X_a - X_b|}{max(X_a, X_b)} + \frac{|Y_a - Y_b|}{max(Y_a, Y_b)} + \frac{|Z_a - Z_b|}{max(Z_a, Z_b)}}{3}$$

*Formula 4.1: Formula for the shake value ω, where $X_a$, $Y_a$ and $Z_a$ are the current accelerometer values, and $X_b$, $Y_b$ and $Z_b$ are the previous accelerometer values.*

The greater ω is, the more the phone is shaken. If ω exceeds a certain threshold value (in the prototype system set to 0.25) the system will indicate that the phone is currently being shaken, and display a text message in red asking the user to stand still. If ω is below the threshold, it means the user is standing still enough to proceed with the application flow, thus enabling a proceed button.

The prototype's motion detection functionality suffers from the same inappropriateness as the face detection functionality; Movement detection is only carried out once in one particular page, while it optimally should silently detect the motion level throughout the whole authentication flow in a background process, and shortly interrupt with a warning message if the motion level is too high.

### 4.3.4 Authentication Process

When the NFC-, face detection- and motion detection-steps are completed it is time for the actual authentication process. The back-end server will provide a photograph showing a person, which will stimulate the user's visual cortex while recording brain-waves. Before showing the photo to the user, the system should vibrate the smartphone for a short period of time to further prepare the user for paying attention to the shown

image. By sensing this “touch” from the phone, the alpha waves will be lowered, setting the user in a ready-state [47].

The image will be shown for a total of five seconds, and when five seconds have passed the front-end will immediately prompt the back-end server for a result of the authentication. Based on the answer from the back-end, the front-end will either show a 'Congratulations' page if the authentication was successful or an 'Access denied' page if it wasn't (as illustrated in Figure 20).

From these two pages it is possible to return to the frontpage and try again. The prototype doesn't actually protect anything but the 'Congratulations' page itself.

### 4.3.5 System Flow Considerations

The process of authentication as it is pictured in Figure 20 and described in the last previous sections is the end result of a number of iterations including changes and improvements to the flow and system design. Originally, the plan was to develop a system based on secret password images for EEG authentication as Thorpe et al. proposed [9]. In this setup each user would choose their own personal password image. This image would be shown to the user when authenticating, and the measured EEG signals would be analysed in order to confirm that the user is who he or she claims to be *and* currently looking at the correct password image. This is different from the final setup, where the images are only used for visual stimulation, and what they are depicting is not essential for the authentication decisioning. In other words, the most crucial in the final prototype is that some image depicting a known face will be shown to the user while authenticating, but it is not essential that the image is kept secret or belonging to the user in question. The reason to change to this approach, was because of advises from Jesper Rønager and how EEG functions. EEG is not a tool to read the exact thoughts of a brain, but can outline the results of certain tasks from within the brain. The spatial resolution of EEG is relatively low and the most informative signals that contains data necessary to build an authentication system based on thought images, is carried out by gamma waves, which are filtered out in the brain tissues. The electrical activity of the brain sources is propagated through the anatomical structures and the resulting EEG is a linear mixture (with unknown or difficult to model parameters) of brain sources and other electro-physiological disturbances, often with a low signal to noise ratio (SNR) [53].

If brain-waves should be interpreted, it would be necessary to conduct a Structural MRI (Magnetic resonance imaging) and Functional MRI at the same time of measuring EEG, which would be way costlier than the proposed system, because of the need for

new hardware.

Taking these circumstances into account, it is still possible to identify a subject person using visual based EEG, but the process cannot stand alone for authentication purposes. Therefore there was a need to incorporate an additional step that the user must carry out in order to successfully authenticate. We chose to add the RFID validation step, hence making a two-factor system by requiring something you have in addition to something you are (the EEG).

The face and motion detection steps and vibration of the phone are not by themselves improving the security of the systems, but were added to take advantage of the most relevant context triggers on the phone, that could help ensure that the person trying to authenticate is as relaxed as possible and ready to concentrate.

## 4.4 Technical Back-end Setup

Based on our previous investigation [6, p. 46], we proposed that the system should be able to carry out heavy DSP calculations on a server side, which ensures lowering the smartphone's processor load as well as giving several benefits in terms of security and scalability of the system. For this purpose, we set up an IIS 7.5 server which operates the back-end part intended for processing the EEG data packages and extracting unique user features for the purpose of authentication. The back-end is also responsible for communication between the server and the EEG headset, as well as it responds to the front-end requests, and finally it exchanges the user specific data with the SQL database. The XML-based web interface is written in ASP.NET, and functionality is implemented with C# .NET, and for the data storage we use a Microsoft SQL 2012 server[10], which enables a cloud-ready information platform.

### 4.4.1 Back-end System Flow

The back-end part consists of two main modules: 1) the Signal Acquisition and Preprocessing module and 2) the Feature Extraction and Classification module. The advantage of such division is that the system can adopt to any EEG hardware by adjusting only the Signal Acquisition and Preprocessing module. The main purpose of this module is to deliver the selected raw EEG data in a compact and organized form to the Feature Extraction and Classification module, which is responsible for calculating and delivering the final authentication results to the front-end.

The entire back-end system flow from the perspective of the EEG signal handling is illustrated in Figure 22 below.

10 https://www.microsoft.com/sql/

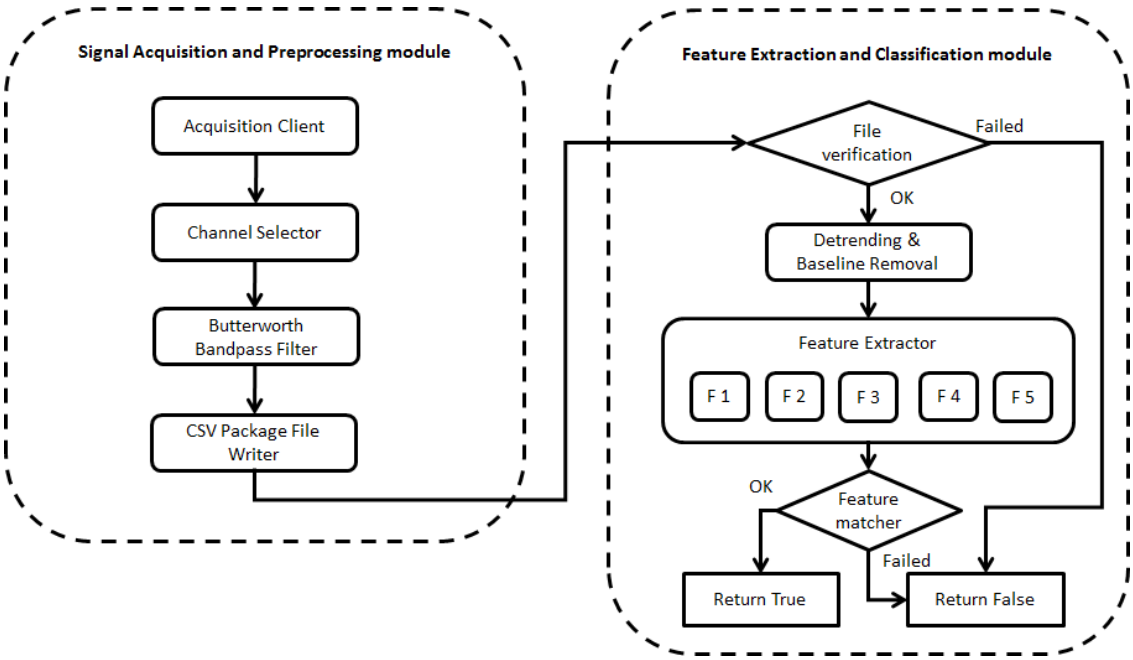


*Figure 22: Flowchart representing the EEG signal handling steps divided in two main modules. The first module represents the actual signal acquisition module which should be implemented on the particular environment connected directly to the EEG measuring device. The second part is responsible for feature extraction and matching the extracted features to the database records on the server side.*

The Signal Acquisition and Preprocessing module is built with a help from the OpenVIBE[11] software platform, which is dedicated to designing, testing and using brain-computer interfaces. The OpenVIBE software can be used to acquire, filter, process, classify and visualize brain signals in real time.

As our prototype system is based on the Emotiv EPOC headset, the Acquisition Client must also decrypt the encrypted raw EEG data stream from the Emotiv EPOC headset. For this purpose, we had to use the 32 byte encryption key linked to the ID number of the Emotiv EPOC headset together with several DLLs intended for the raw EEG signal decryption available from the Emotiv Research SDK. Based on the experiment results (see Experiment results) and the literature review [68] [22] [10], the most significant features can be extracted from the visual parietal-occipital cortex of the brain. Therefore the Channel Selector is created and is set to obtain the data from the following four EEG sensor locations: P7, P8, O1, O2, based on the international 10-20 system [18, p. 140]. The Butterworth Bandpass Filter was applied in order to avoid frequencies which are lower than 0.5 Hz and higher than 40 Hz, because these frequences were not informative enough for further feature extraction (see Experiment results). The CSV Package File Writer is responsible for generating an EEG data

11 http://openvibe.inria.fr/

package by the request of the front-end.

### 4.4.2 EEG Data Packages

The decrypted and filtered raw EEG data is packed in a text file with one reading at each line, with each line starting with a timestamp. The numeric EEG measurement values are separated by commas, thus using a Comma Separated Value (CSV) syntax. The following table shows an example of the contents of the compact package as a text file:

| **Time (s),** | **P7,** | **O1,** | **O2,** | **P8,** | **Sampling Rate** |
|---|---|---|---|---|---|
| 0.000000, | 4614.358887, | 3870.769287, | 4448.205078, | 4300.512695, | 128 |
| 0.007813, | 4621.025879, | 3871.794922, | 4457.436035, | 4304.102539, | |
| 0.015625, | 4626.153809, | 3862.051270, | 4449.743652, | 4295.897461, | |
| 0.023438, | 4614.358887, | 3861.025635, | 4447.692383, | 4295.384766, | |
| 0.031250, | 4608.205078, | 3861.538574, | 4448.717773, | 4295.384766, | |
| 0.039063, | 4620.000000, | 3861.538574, | 4446.153809, | 4288.717773, | |
| 0.046875, | 4627.179688, | 3872.307617, | 4458.461426, | 4298.974121, | |
| […] | | | | | |

*Table 2: Generated raw EEG data package.*

As further explained in the 4.5 Front-end-Back-end Communication Protocol section, there are two main requests to the back-end from the front-end part: first, when the application verifies the user NFC tag and provides the password image of a registered user; and second, when the application requests to start measuring the brain-waves. It is required that the user adjusts the EEG headset before using the application, so that the signal can be correctly acquired when the application starts.

### 4.4.3 File Verification

The package file verification procedure is necessary to ensure that the signal is acquired correctly and that it can be further used for the extraction of unique biometric features. First of all it checks that the package exists and that it contains non-zero content, which is formatted correctly. This subsection also reveals one of the reasons, why the Detrending and Baseline Removal part is not applied in the Signal Acquisition and Preprocessing module. In our system, the baseline itself is used to verify the package data, thus it is stored in a temporary buffer. For example, if there is a high fluctuation of the baseline, which exceeds the 100 μV value, it means that the EEG signal is too noisy and is not reliable for further feature extraction. This will happen if the subject person is not adjusted the EEG headset properly, or if he or she is on-the-go for example. So if it happens, the back-end will automatically respond with *false* to the front-end request, so that the user will not be authenticated and will be asked to retry the authentication procedure.

### 4.4.4 Detrending and the Baseline Removal

For easier feature extraction, it is necessary to remove the baseline of the raw EEG dataset for each electrode measurements individually, which means to remove the mean of the recording. This step ensures that the signal will be distributed around 0. For this purpose, a buffer has been used to remove the mean of the closest 128 samples to the current point – 64 from the past and 64 from the further data (which equals to one second) instead of the baseline of the whole recording of five seconds. As the moving average was used for the baseline removal, it automatically detrends the signal, leaving the 1Hz to 40 Hz frequency signal for the further processing.

Another reason, why this step was not applied in the Signal Acquisition and Preprocessing module, is that the baseline itself can potentially represent a unique biometric feature [69, p. 2], as it represents micro voltage values of the scalp. Therefore, it might be necessary to store the baseline of a 5-second-long EEG signal in the database as an extra component for further feature extraction.

### 4.4.5 Database Design

In Figure 23 below the structure of the MSSQL database can be seen.

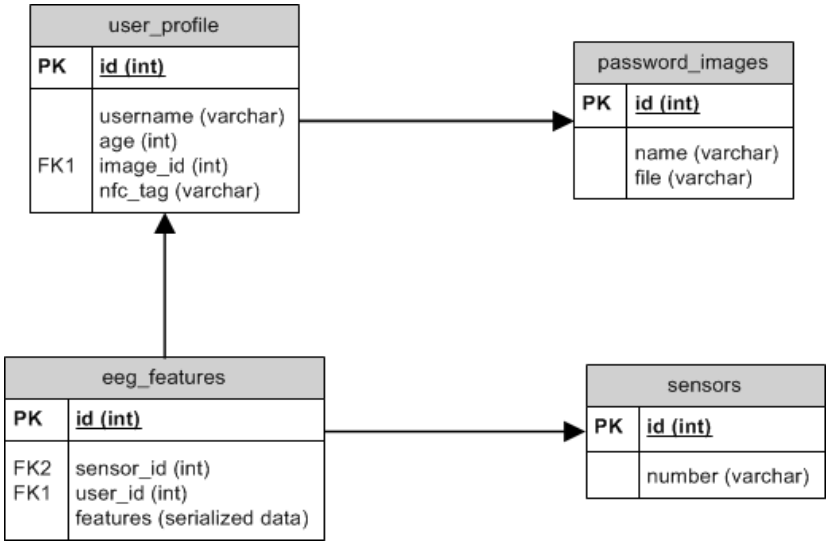


*Figure 23: Entity-relationship diagram representing the database model.*

The database consists of 4 main tables: 'user_profile', 'password_images', 'eeg_features' and 'sensors'. The user_profile table stores the personal information of the registered users, specifically their ID numbers, NFC tag numbers of their ID cards, their usernames, years of age, and finally the password-image ID numbers. The 'eeg_features' table is responsible for storing the unique subjects' EEG features which are used as biometric identifiers for classifying the individual. The mean base-line

values, ZCR measures, Cross-correlation, coherence values, PSD histograms, and finally latency values are stored in this table. However, the latencies are not yet used for classification of the subject persons, however these measures are considered useful for future improvements of the prototype. Since we know the exact time-stamp of the moment when the password picture is shown to the user, we are can extract the latency time from the moment of picture appearance to the moment, when the visual stimuli signal is reached the occipital cortex and is registered by the sensors O1 and O2. This is based on the DWT method (using Mexican hat template wavelet) of the 4-th level of decomposition, when the amplitude is exceeding 8 microvolts amplitude.

## 4.5 Front-end-Back-end Communication Protocol

The front-end and back-end communicate with each other by means of a RESTful web interface. Simply put, REST (Representational state transfer) is an architectural style where data is exchanged over HTTP, for example in a client-server model [70]. In the prototype the front-end and back-end communicate over a WiFi connection, with the front-end querying data from the back-end by sending HTTP requests with additional GET parameters. The back-end will in return respond with data in XML format. As the front-end is simply a web application built with HTML, CSS and JavaScript, communication with the back-end server is done through AJAX calls using the JavaScript `XMLHttpRequest` API. Figure 24 below illustrates the flow of data in the exchange protocol.

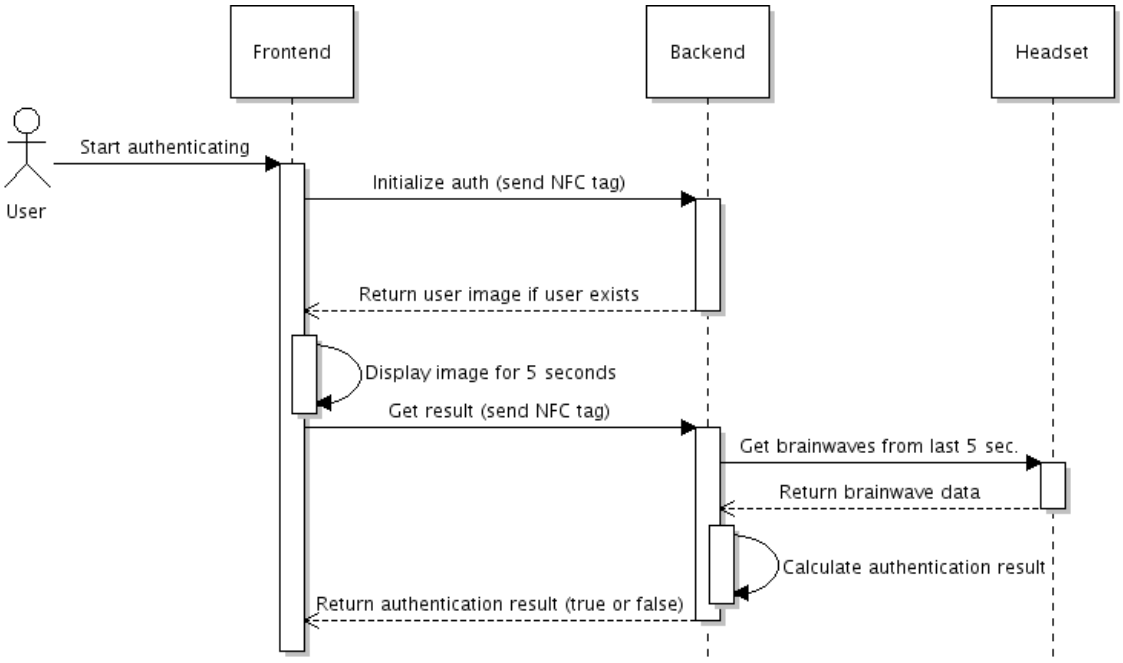


*Figure 24: Sequence diagram showing interaction between front-end, back-end and headset. Communication between front-end and back-end is carried out in a RESTful approach, with the front-end querying the back-end with GET parameters, and the back-end server responding with XML files.*

As it can be seen in the figure, the communication between front-end and back-end is initiated after the user has swiped a NFC tag against the smartphone, and the face- and motion-detection steps has been completed. The front-end will then send a request to the back-end containing the NFC tag as a GET parameter. If the NFC tag matches an existing user profile, the back-end responds with an XML file containing an image path. The front-end displays this image to the user while recording his or her brain-waves, and when the 5 seconds have elapsed, the front-end will send a new HTTP request to the server (sending the NFC tag as a GET parameter once more, as the exchange protocol is stateless). The intention of this second request is to get the result of the authentication process, and once calculated by the back-end server, it will be returned to the front-end in a simple XML file containing either true (for a positive authentication result) or false (for a negative authentication result).

# 5 System Usage

Even though something is achievable in theory, it is also important to evaluate whether it is actually useful. So far we have assessed whether it is possible to create a biometric EEG based authentication system, and presented how such a system can be implemented. In this section we will analyze and evaluate the usefulness of EEG based authentication systems, and assess different potential use case scenarios where it could be put to use. To set the scene, this section starts with a brief introduction to the various concepts and principles regarding identity management and digital identities.

## 5.1 Digital Identities

Digital identities play a massive role in the modern world. When operating in a web based environment it is necessary for a user to prove his or her identity to a number of identity providers. In general, identity providers are responsible for verifying a user or client identities. Furthermore, they are issuing security tokens that can be further accepted by some service providers, letting the user to access some service. In addition to the identity providers and subject users, the identity metasystem also consists of relying parties, i.e. services that uses identities offered by other parties [71, p. 3]. In 2005, Kim Cameron penned the Seven Laws of Identity, which describes a set of rules about how identity and privacy works on the Internet [72]. These laws says, among other things, that a digital identity system must only reveal user information with the user's consent, only as little identifying information as possible should be disclosed, only authorized persons can get access to identity information and that humans are the key component in identity systems, etc. The fifth law, entitled Pluralism of Operators and Technologies, says that a universal identity metasystem must support multiple identity technologies run by multiple identity providers.

In the physical world it is much easier to prove the identity of a subject person than in the digital world. Often users are giving away too much information about themselves on the Internet, which results in loss of privacy. The typical identity information used in systems nowadays is name, address, gender, nationality or the like. People do not worry much about giving away that kind of information, and these circumstances forms Kim Cameron's proposal to implement a special identity layer for the Internet.

These concepts are relevant in the digital world with digital subjects making claims about their identity to identity providers. The same counts for an EEG based authentication system, which is essentially a new technology fitting into the overall picture of identity management. Such a system can support already existing and well-defined identity management systems and services, and additionally it can improve

privacy in some cases, as it can avoid the use of typical identity information attributes like name and address etc.

## 5.2 Biometric Identification Requirements

According to Jain et al., biometric identification system has four fundamental requirements [21, p. 3]:

1. **Universality**, which refers to, that all people should be able to use the system.
2. **Uniqueness**, which refers to, that the system should be able to differentiate between individuals.
3. **Constancy**, which refers to, that the biometric characteristic should be relatively constant for a long period of time.
4. **Collectability**, which refers to, that biometric data should be easy to collect without causing discomfort.

These requirements are a good indication of whether a given biometric based authentication system is reliable and useful in reality.

Considering the first requirement about universality, the proposed prototype system obviously wouldn't work for blind people or people with severe visual impairments, since the cornerstone in the authentication process is processing brain-waves evoked from visual stimuli. We believe though, that since this is a relatively limited number of people compared to the ones who can see, the system still has its merits. As mentioned earlier in this report, alternative versions of the system could be deployed for people with visual impairments; e.g. using tactile feedback or sound stimuli.

Regarding the second requirement about uniqueness, we have showed how to clearly differentiate between individual's brain-waves, by implementing a robust feature extraction and classification system used for processing incoming brain-waves and authenticating people.

When talking about constancy, the third requirement in the list above, there is still some uncertainty about what happens to EEG signals over time. As we saw earlier in this report, according to Jesper Rønager EEG shows no difference over a fifty year period, but it is important to point out that this is a rather new field, and more investigation needs to be done concerning this matter.

Considering the fourth requirement about collectability, there are still a number of problems to address regarding the presented prototype system. The most obvious one

being the use of the EEG headset itself, which must be used in order to authenticate. The sensors must be placed approximately in the same position each time a recording is done, which will require training the end users. Furthermore, the headset is not so comfortable to wear for a longer period of time. We believe that these problems are solvable, and shouldn't be a barrier to develop and improve EEG based authentication systems.

## 5.3 Usage Scenarios

There are several possible and potential usage scenarios where a mobile EEG based authentication system could be used. An important detail to remember about the system as it's presented in this project is that it's “mobile”. This means that it has an advantage in scenarios, where there is a sudden or unexpected need to prove an identity and grant access to a specific resource. But obviously the system is not limited to mobile use, and could as well be used in more static environments. The system is using various context triggers like camera and accelerometer from a smartphone to support the EEG authentication procedure, but the main function of the smartphone, the telephone with dial-up functionality, is not used and not so important in this context. One could therefore argue that the term “smart device” or simply just mobile device is more precise in this case.

One of the smart things about the system is, that is constructed of standard products already existing. Furthermore, EEG has some advantages over other biometric characteristics like fingerprints or iris scans, since EEG cannot easily be duplicated. On the other hand, as we just saw the biggest disadvantage of the system is the need for an EEG headset, which must be placed properly on the scalp for optimal recordings. Development it this area is very fast, and some of the inconveniences associated with current EEG headsets might be overcome in the nearby future. For example, the American company Quasar is developing a prototype EEG headset with dry electrodes, which does not need to be moistened before use [73].

As the system is working now with an EEG headset, it would be most useful in scenarios, where a high security level is required and it is important to know that the subject person in question is really who he or she claims to be. Given these assumptions, it is imaginable that EEG-based authentication could be used with automatic teller machines (ATM's), or when trying to grant access to open a door which is securing something. Both of these examples represent a static environment, since neither an ATM or a door (usually) move around. In that case the person trying to authenticate must have a personal token with a NFC tag (built into a finger ring, wristband or ID card) in order to proceed. The mobile device itself is not so important

in this case, and its functionality could just as well be be taken over by the ATM or secured door.

Instead, the mobile feature has its strength when it comes to another type of usage scenarios. It could be in case of a sudden need to perform an unplanned payment with high security involved. That case is not necessarily tied to one particular location, thus taking advantage of the mobile capabilities of the system.

Additionally, the system might serve as an alternative for people that are not good at remembering passwords. As mentioned earlier in this report, normal textual passwords suffer from a number of problems. People tend to select passwords that are easy to remember, and therefore easy to guess or lookup in a dictionary. On the other hand, if passwords are hard to guess, they are also hard to remember, and if maintaining a too strict password policy, there's a risk that people store their passwords in clear text another place in order to remember them (e.g. on a piece of paper).

Research has been trying to assess whether using graphical passwords has an advantage or is just as secure as textual passwords [36, p. 2]. The findings of this research do not yet give an unambiguous answer to those questions, since the vulnerabilities of graphical passwords are still not fully understood. Even though the EEG authentication system shares the graphical aspect with such systems because of the images of well-known faces, it does not use true graphical passwords. People who are not good at remembering passwords, for one reason or another, might therefore be able to benefit from a system that puts less emphasis on the *something you know* factor (textual passwords), and instead weights the *something you are* factor (the brain-waves) higher.

## 5.4 Security Matters and Assurance Levels

One of the main reasons to introduce an authentication system based on EEG on the market in the first place, should be that it offers something that current authentication systems are not capable of in terms of security. The EEG feature extraction and classification part of the system does not by itself serve as an authentication system, but is used as an *identifier,* that together with the NFC, camera and accelerometer functionalities forms a complete authentication system.

The decision to base the authentication process on EEG recordings from relaxed subject persons has other implications than just making it easier to process the incoming data. This decision also influences the security aspects of the system, since it will be very hard for e.g. a stressed person to successfully authenticate. In the interview with Jesper Rønager, we presented a scenario where an intruder might try to gain access to a secured system by forcing an authorized subject person to authenticate [47].

If the system is based on relaxed recordings, and the intruder is acting in a threatening manner, thus stressing the subject person, it will be much harder to successfully authenticate. The same counts for basically any kind of environmental change when recording the brain-waves. The system requires approximately the same conditions at each authentication event as the initial EEG recording.

As with many other authentication systems, the EEG system presented in this project is not immune to phishing attacks. Intruders could create a fake variant of the system, with the sole purpose of trick users into giving away their login credentials together with their brain-waves. If the system is used to protect intangible goods, the fake system could even be constructed so that it'll give the intruders access to the real data in real-time, and thus serve something looking like the real protected data to the unaware user.
To make it more resistant to phishing attacks, the system could be constructed so that it will refuse to accept two identical EEG recordings. This strategy takes advantage of the fact, that two EEG recordings are never exactly the same point by point, even though the conditions of the subject person and the surrounding environment seem to be comparable. It is unpredictable how artifacts will influence the EEG recordings. If the system can furthermore continuously store these changes in recordings from one authentication attempt to another, it could as well address the aforementioned eventual problem about aging of EEG signals, that might change over time (see Interviews section).
In a future version of the system, it might be possible to construct some kind of challenge-response system, asking the user to solve a small task while recording his or her brain-waves, where the results will be evaluated in order to decide whether the user can gain access or not. This may further assist in avoiding phishing attacks.

### 5.4.1 EEG and Assurance Levels

In terms of the assurance levels as described by OMB (see 2.2.2 Assurance Levels), the proposed EEG authentication system is intended to be placed in the higher end tailored for systems that require very high security. In the case required use of hard tokens in assurance level 4, this is solved by using an NFC tags in the prototype. As the system presented here is just a prototype, it is out of the scope of the project to comply with all the technical requirements of assurance level 4. Hence, for example, cryptographic technologies are not implemented.

Technically it would be possible to implement an authentication system in assurance level 4, with all the necessary cryptographic technologies, secure protocols and hard tokens required, and in addition to this add EEG based authentication. In other words,

if all the requirements for assurance level 4 is met in a particular system, and a layer of EEG based authentication is added on top of that, we claim that it will further improve the overall security of the system.

### 5.4.2 Continuous Authentication Process

Since in the current prototype system the EEG data are captured continuously, there is a potential possibility to continuously requesting the authentication results in order to make sure, that the same person is using the system. This can eliminate the potential risk of a situation, when a successfully authenticated user forget to log-off from the system and a criminal is trying to access the system. In such case, the system can automatically log-out the user in the following (and not limited to) example cases:

1) if the user took-off the EEG measuring headset;
2) if the user is on-the-go, so that the EEG data will become too noisy;
3) if the user's mental state changes significantly (e.g. become stressed, drowsy);
4) if the user's face is not in front of a smartphone anymore.

## 5.5 Further Improvements and Alternatives

In this section we present different possible further improvements and alternatives to the system as it is presented. These are included to give an indication of the opportunities of EEG based authentication systems and present natural steps for future work on the topic.

### 5.5.1 Face Recognition

In chapter 4 we showed how the prototype uses face detection algorithms to detect whether there's a person in front of the smartphone camera. As this functionality only *detects* faces in the camera's field of view, it could be relevant to improve it so that it would also *recognize* faces. This means, that in addition to store the user's brain-waves, the system should also store a photograph of the user's face (taken with the samrtphone's camera), and continuously compare this face to a new snapshot of the user currently trying to authenticate. There are plenty of algorithms and approaches available capable of recognizing faces. Some analyzes the relative position between eyes, nose, jaws, etc., while others normalize a gallery of face images in order to recognize a particular face. Especially three algorithms are described in depth in face recognition literature. These are named Principal Components Analysis (PCA), Linear Discriminant Analysis (LDA), and Elastic Bunch Graph Matching (EBGM) [74, pp. 2–4].

This addition could assist in improving the overall security of the system, since it would require a positive face recognition match to authenticate. It is not so important that the chosen face recognition algorithm is 100 % perfect, as the security factors (the EEG authentication process, requirement of a hard token, etc.) will still ensure a reliable authentication system. Say, if the system is easily fooled if the intruder is using a photograph of the person he is trying to identify himself as instead of showing his own face to the camera, resulting in a false positive, it is only a minor issue security-wise, as face recognition should not be the cornerstone in the authentication system anyway.

To overcome this issue, the face recognition functionality could take advantage of the fact, that facial expressions can be measured with the Emotiv Epoc EEG headset used for the prototype system. These measurable facial expressions include eyelid and eyebrow positions, clenching teeth, smiling and laughing. The system could after recognizing the face in front of the camera, setup a simple challenge-response asking the user to either smile, clench teeth or maybe blink his or her eyes. This way the system can validate if it is a real human being in front of the camera, by synchronizing input from the EEG headset with the live camera preview, and check that the provided input is not perhaps a photograph or video sequence of a face. In this case it is a prerequisite, that the user doesn't know in advance which challenge to complete.

In order to accomplish this technically, the video data from the camera and the EEG recordings must be synchronized and processed for further feature extraction. Only if the unique features extracted from the facial recognition and from the EEG recordings corresponds to the actual person in the correct order (of the replicated facial expressions), the system will generate a positive authentication result.

### 5.5.2 Eye Blinking

The prototype system presented in this report shows how an EEG based authentication system *could* be implemented, but our investigations made throughout this project also shows that basing the system on relaxed EEG recordings from subject persons focusing on images of known faces, thus stimulating their visual cortex, is not the only way to achieve the desired result. Other similar approaches might give just as good authentication mechanisms, and can be tailored for different usage scenarios. According to Jesper Rønager [75], visual stimulus is not the only characteristic which results in unique brain-waves. Jesper puts it this way:

> *"You could use the eye artifacts. Those are also distinct. Every face is unique and if you just blink the eyes there will be very large signals from most of the*

*electrodes that will be unique for that person."*

If eye blinking artifacts signals are just as unique as signals evoked from visual stimuli, one could imagine an alternative authentication system based on the sequence of eye blinks. This way, a particular user could select his or her own private eye blinking sequence (for example, blink once with the right eye, then twice with the left eye and finally once more with the right eye), which could be used to authenticate into the system. Just as with the current system, this eye blinking sequence will be evaluated in order to decide whether the subject is who he or she claims to be. The user will have to make an initial recording of eye blinks when signing up in the system, that will be stored and compared to future recordings, when the user wants to authenticate. The greatest benefit of this approach is that it automatically adds a *something you know* class to the evaluation of EEG recordings (the personal eye blinking sequence), meanwhile the EEG still represents *something you are*. There are plenty of entropy in this *something you know* class, thus substituting normal textual passwords. In principle, such an eye blinking sequence can be infinitely long.

Furthermore, if intruders succeed in harvesting this recording of eye blinks, and attempt to abuse it, it would be relatively easy to change the eye blinking sequence to a new one, hence making the old one useless in terms of authentication. Just as if a textual password is stolen and needs to be replaced with a new one.

By using eye blinks as the contextual trigger for authentication, it is possible to create a system slightly different from the one presented in this report.

# 6 Conclusions

In the last few years, many different projects have focused on specific EEG authentication tasks, as well as innovative interaction techniques, applications, studies and tools. However, so far there has been no comprehensive overview about this field discussing the different brain-smartphone interaction techniques, their characteristics and their implementations. Furthermore, very little research regarding the development process of such applications is reported with the exception of just a few existing tools that only focus on the support of one specific technique – in our case a mobile EEG-based biometric authentication. The overall goal of this work was to fill the gap between mobile web technologies and wireless EEG devices and to develop a new authentication technique and a feasible application.

The risk analysis we made supported us throughout the project process in identifying potential harm and impacts associated with the project.

## 6.1 EEG-based Authentication

Based on the gained experience from the literature investigation and several interviews conducted with EEG and DSP professionals, it is clear that a EEG-based authentication system is feasible, and our prototype system is a proof of this claim. We introduced how the short EEG recordings can be transformed to represent unique biometric identifiers, including both: behavioural and physiological characteristics. Obviously, the major problems involved in EEG-based authentication are the large feature size (which are computed from the scalp EEG signals) and the poor reliability of EEG signals (due to the noise, subject's activity and condition). Our main contribution was to find exact and relatively reliable unique features, which combination can maximize the reliability of the EEG-based biometric authentication system. Sensor condition and adjustments of the EEG headset were critically important for successful system usage, however, the exact sensor positioning was not so crucial.

We have analyzed in which contexts a mobile EEG based authentication system could be put to use, and identified and assessed various possible usage scenarios. It has been shown that EEG authentication can support already existing well-defined identity management systems, and can have some advantages in terms of privacy since typical identity information attributes like name, address and the like doesn't necessarily have to be used.

As the system presented in this project is mobile based, it is especially suited for scenarios, where there is a sudden or unexpected need to prove an identity or authenticate, but that doesn't prevent it from being used more statically. Such static

environments could be ATM's or the need to open a door that is protecting something. The mobile functionality of the system gives some other opportunities, like solving the problem of suddenly making an unexpected money payment with high security involved. Additionally, the system could act as an alternative to already existing authentication solutions that for one reason or another is insufficient in their current context. Examples includes using such a system for people that are not good at remembering passwords, or when authentication is happening so rarely, that it is hard for anyone using the system to remember their password.

## 6.2 System Implementation

In order to prove the feasibility of using EEG for biometric authentication, we have implemented a mobile prototype system, capable to authenticate a user. For the prototype development, we used an Android Samsung Galaxy Nexus smartphone (because it is the most open platform) and an Emotiv EPOC EEG headset (because of our previous experience, the wireless interface and the hardware reliability). Based on our experimental results and suggestions from EEG expert Jesper Rønager, the best possible implementation approach was to use visual stimuli (specifically, faces of famous persons) in order to extract unique features from the four preselected EEG sensors: P7, P8, O1, O2.

The system implementation was divided in two major parts: a back-end and a front-end part. The main aim of the back-end part, running on a cloud-ready server, was to handle the heavy DSP calculations of EEG feature extraction and classification for authentication decision making. The front-end was responsible for managing the interaction between the user and the smartphone. We decided to build the front-end with standard web technologies because of the rapid prototype capabilities of these. The communication of the front-end and back-end was realised as an XML-based RESTful web interface, with a protocol describing data exchange.

Since the main system interface from the perspective of the user is a smartphone device, there are various context triggers available that can support the authentication procedure. We decided to tailor the prototype system on relaxed subject persons in order to get optimal conditions for capturing their brain-waves. We decided to use the smartphone's built-in camera to detect whether there's a face in front of the screen before the user should focus on an image. Likewise, we used the accelerometer to control if the user is standing still while authenticating. This step was added to make sure that the user is relatively calm, and not on-the-go, since this could influence the EEG measurements. As alpha waves are lowered as a result of touch, thus making a person ready to concentrate, the built-in vibrator can give some tactile feedback to the

user before the image containing a known face is shown.

All of these functionalities taking advantage of the hardware components of the smartphone were implemented to support the authentication procedure, but are not essential for the authentication result itself.

### 6.2.1 Practicability of the System

Despite the fact that an EEG headset is a non-invasive system and does not require any surgical involvement, the comfortability level of an EEG headset should still be high enough for bringing it to everyday use. Based on our experience and feedback from the subjects we have tested, the comfortability of the Emotiv EPOC neuroheadset varies from subject to subject and some people finds it relatively uncomfortable to wear for a longer period of time. As our proposed system requires wearing the EEG headset for only a few seconds, this problem does not apply to our prototype. However, it might take relatively long time (up to approximately 10 minutes) for adjusting procedures of the Emotiv EPOC headset, which potentially makes the EEG authentication service impractical. These procedures are moisturising the EEG sensors and adjusting sensors on the correct locations by avoiding hair. The individuals with bushy hair have more problems in adjusting the sensors. To solve this issue, it is necessary to investigate further how the EEG hardware should be build, and as mentioned before, the dry sensor electrodes might be more appropriate and reliable. Finally, our proposed system requires only sensors, which are placed on a subject's scalp over the parental and occipital lobes, thus eliminating other sensors might partly solve the issue.

## 6.3 Feature Extraction

We have revised and tested several EEG feature extraction techniques, which were suggested by EEG and DSP professionals as well as found in the literature as potentially unique. Before the feature extraction procedures, it was necessary to prepare signals and to enhance the signal-to-noise ratio (by applying band-pass filters and ICA). One of the simplest features, which proved the uniqueness from subject to subject was zero-crossing rate, however it was not efficient enough to rely the whole authentication decision making on this one method only. To improve the system reliability, several more complicated techniques were employed, such as power spectral density and Wavelet analysis (based on Morlet and “Mexican hat” wavelet), where the feature output was multidimensional coefficient matrices. Therefore, it was relatively hard to distinguish differences between subjects from a large set of extracted data and at the same time to present the stationary of these features. From the power spectral

density we were able to find the similarities in the histogram of the spectrogram image, and the wavelet analysis was beneficial to measure latencies of visual-evoked potentials at the occipital lobe area. This is a valuable finding for biometric authentication application, since these measures are more likely unique for a larger number of subjects, since nobody has the same neural-wiring of the brain. Finally, as a potentially beneficial feature for biometric authentication, we proposed to use eye artifact related signals and facial expressions.

## 6.4 Security Aspects

We have evaluated the various security aspects associated with the presented prototype authentication system. We have seen a positive side-effect security-wise of basing the system on brain-wave recordings from relaxed subject persons, since it makes it impossible for an intruder to directly force a user to authenticate. Stress signals will be present in the measured brain-waves, thus resulting in a denial of access. The same counts for almost any kind of environmental change when authenticating, as the conditions should be as close as possible to the original recordings.

The presented system is, just as many other authentication systems, not immune to phishing attacks. The problems regarding phishing attacks can be addressed by incorporating a challenge/response mechanism to the authentication procedure or by not accepting two identical brain-wave recordings at any time, taking advantage of the fact that no EEG recordings are 100 % identical.

The assurance levels defined by The American Office of Management and Budget have been presented to show how different degrees of trust and confidence in an identity can be described. When implementing a new system, one can identify the risks associated with misuse of the system, and use those as a basis for picking an appropriate assurance level to match the risks, and choose technologies to prevent misuse.

According to these assurance levels, the presented EEG authentication system is intended to be placed in a higher level tailored for systems that require very high confidence in an identity's validity. As the system is just a prototype, all the technical requirements of e.g. assurance level 4 are not met, but could be implemented in a real-life system.

As the system is obtaining brain-waves from users trying to authenticate, one of the most obvious questions raised is if it's possible for someone to steal this stream of thoughts and use them to authenticate, or even worse from an ethical point of view, interpret what the brain-waves *mean*. However, the EEG signals have a very high network effect and signals from the deeper parts of the brain are not readable by EEG

headsets [53], therefore there is no risk of reading and interpreting the actual thoughts of the user.

## 6.5 Future Work

We have proposed a number of alternatives to the system and additional functionality, which can benefit the biometric authentication process. These include the combination of facial recognition and EEG-based authentication, as well as using eye artifacts and facial expressions as extra context data.

In a future version of the system, it would be relevant to use more unique features, which are complementary to each other, and cover all of the five EEG characteristics (frequencies, amplitudes, wave morphology, spatial distribution, reactivity), so that behavioural and physiological data is covered for authentication reasoning. Furthermore, we suggest using emotional states (which can be extracted from the Emotiv research package) as extra context, in order to avoid emotional states influencing the authentication result, by adjusting features accordingly.

# Bibliography


[1] R.J. Wilkus, “The EEG as confirmatory evidence of brain death: Previous and current approaches,” *Journal of Medical Humanities*, vol. 2, Mar. 1980, pp. 39–45.

[2] S. Akben, A. Subasi, and D. Tuncel, “Analysis of EEG Signals Under Flash Stimulation for Migraine and Epileptic Patients,” *Journal of Medical Systems*, vol. 35, Jun. 2011, pp. 437–443.

[3] L. Jameson and T. Sloan, “Using EEG to monitor anesthesia drug effects during surgery,” *Journal of Clinical Monitoring and Computing*, vol. 20, Dec. 2006, pp. 445–472.

[4] Q. Zhao, H. Peng, B. Hu, Q. Liu, L. Liu, Y. Qi, and L. Li, “Improving Individual Identification in Security Check with an EEG Based Biometric Solution,” *Brain Informatics*, Y. Yao, R. Sun, T. Poggio, J. Liu, N. Zhong, and J. Huang, eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 145–155, Available online: http://www.springerlink.com.zorac.aub.aau.dk/content/g53n47235k5u5542/, (Accessed: January 31, 2012).

[5] J. Ales, T. Carney, and S.A. Klein, “The folding fingerprint of visual cortex reveals the timing of human V1 and V2,” *NeuroImage*, vol. 49, Feb. 2010, pp. 2494–2502.

[6] J. Kļonovs and C.K. Petersen, *Mobile Mind State Detection Services*, Denmark: Aalborg University Copenhagen, 2011.

[7] Yubico, “Yubico Sees 90 Percent Customer Growth and Geographically Expanded Adoption of Two-Factor Authentication Technology in 2011 - Yubico,” Jan. 2012 Available online: http://www.yubico.com/90-Percent-Customer-Growth-2011, (Accessed: June 5, 2012).

[8] J. Arlow and I. Neustadt, *UML 2 and the Unified Process: Practical Object-Oriented Analysis and Design*, Addison-Wesley Professional, 2005.

[9] J. Thorpe, P.C. van Oorschot, and A. Somayaji, “Pass-thoughts: authenticating with our minds,” *Proceedings of the 2005 workshop on New security paradigms*, New York, NY, USA: ACM, 2005, pp. 45–56, Available online: http://doi.acm.org/10.1145/1146269.1146282, (Accessed: May 18, 2012).

[10] A. Zúquete, B. Quintela, and J.P.S. Cunha, “Biometric Authentication using Brain Responses to Visual Stimuli.,” *BIOSIGNALS*, Aveiro, Portugal: Institute of Electronics and Telematics Engineering of Aveiro (IEETA), 2010, pp. 103–112, Available online: http://www.ieeta.pt/~avz/pubs/BIOSIGNALS10.pdf, (Accessed: February 22, 2012).

[11] J.G. Snodgrass and M. Vanderwart, “A standardized set of 260 pictures: norms for name agreement, image agreement, familiarity, and visual complexity,” *Journal of Experimental Psychology. Human Learning and Memory*, vol. 6, Mar. 1980, pp. 174–215.

[12] C. Ashby, A. Bhatia, F. Tenore, and J. Vogelstein, “Low-cost electroencephalogram (EEG) based authentication,” *2011 5th International IEEE/EMBS Conference on Neural Engineering (NER)*, IEEE, 2011, pp. 442–445.

[13] “Agroscope - Simultaneous measurement of brain activity, physiology & behavior in large animals” Available online: http://www.agroscope.admin.ch/publikationen/einzelpublikation/index.html?lang=en&aid=22334&pid=22962, (Accessed: May 31, 2012).

[14] A.F. Mirsky and P.V. Cardon Jr., “A comparison of the behavioral and physiological changes accompanying sleep deprivation and chlorpromazine administration in man,” *Electroencephalography and Clinical Neurophysiology*, vol. 14, Feb. 1962, pp. 1–10.

[15] K. Li, V. Narayan Raju, R. Sankar, Y. Arbel, and E. Donchin, “Advances and Challenges in Signal Analysis for Single Trial P300-BCI,” *Foundations of Augmented Cognition. Directing the Future of Adaptive Systems*, D. Schmorrow and C. Fidopiastis, eds., Springer Berlin / Heidelberg, 2011, pp. 87–94, Available online: http://www.springerlink.com/content/n1302838231852x2/abstract/, (Accessed: June 3, 2012).

[16] S. Sanei and J. Chambers, *EEG Signal Processing*, John Wiley & Sons, 2007.

[17] G.J. Gillen, *Single Photon Emission Computed Tomography: Performance Assessment, Development and Clinical Applications*, University of Glasgow, 1990.

[18] E. Niedermeyer and F.L. da Silva, eds., *Electroencephalography: Basic Principles, Clinical Applications, and Related Fields*, Lippincott Williams & Wilkins, 2004.

[19] J. Anderson, *Cognitive Psychology and Its Implications*, Worth Publishers, 2009.

[20] A.K. Jain, A.A. Ross, and K. Nandakumar, “Introduction to Biometrics,” *Handbook of Biometrics*, Springer, 2011, pp. 1–22.
[21] A. Jain, L. Hong, and S. Pankanti, “Biometric identification,” *Commun. ACM*, vol. 43, Feb. 2000, pp. 90–98.
[22] A. Zúquete, B. Quintela, and J.P.S. Cunha, “Biometric Authentication with Electroencephalograms: Evaluation of Its Suitability Using Visual Evoked Potentials,” *Biomedical Engineering Systems and Technologies*, A. Fred, J. Filipe, and H. Gamboa, eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 290–306, Available online: http://www.springerlink.com.zorac.aub.aau.dk/content/g6878412401753n5/, (Accessed: January 31, 2012).
[23] E.G. Jones, “Cortical and Subcortical Contributions to Activity-Dependent Plasticity in Primate Somatosensory Cortex,” *Annual Review of Neuroscience*, vol. 23, 2000, pp. 1–37.
[24] L. Graziano Breuning, “How Your Brain Wires Itself,” *Meet Your Happy Chemicals: Dopamine, Endorphin, Oxytocin, Serotonin*, CreateSpace, 2012, p. 210.
[25] E. Ackerman and L.C. Gatewood, *Mathematical Models in the Health Sciences: A Computer-Aided Approach*, University of Minnesota Press, 1979.
[26] A. Prochazka, J. Kukal, and O. Vysata, “Wavelet transform use for feature extraction and EEG signal segments classification,” *3rd International Symposium on Communications, Control and Signal Processing, 2008. ISCCSP 2008*, IEEE, 2008, pp. 719–722.
[27] Н. Л.А., “Электроэнцефалография и ее использование для изучения функционального состояния мозга,” *Естественнонаучные основы психологии*, May. 1978, pp. 155–177.
[28] F. Stella and A. Treves, “Associative Memory Storage and Retrieval: Involvement of Theta Oscillations in Hippocampal Information Processing,” *Neural Plasticity*, vol. 2011, 2011, pp. 1–15.
[29] J. Šťastný and P. Vrchota, “EEG-based biometric person identification : 18-th International Eurasip Conference Biosignal 2006. Measurement and interpretation of physiological signals,” *Analysis of biomedical signals and images : .. international Eurasip conference : Biosignal .. : proceedings*, 2006, pp. 76–77, Available online: http://www.medvik.cz/link/bmc08003843, (Accessed: June 4, 2012).
[30] J. Harrison and M. Hobbs, *Brain training : the complete visual program*, New York, N.Y.: DK, 2010.
[31] Tran, A. Craig, and P. Mcisaac, “Extraversion–introversion and 8–13 Hz waves in frontal cortical regions,” *Personality and Individual Differences*, vol. 30, 2001, pp. 205–215.
[32] J. Harper, *Identity Crisis: How Identification is Overused and Misunderstood*, Cato Institute, 2006.
[33] S. Downes, “Authentication and Identification,” *Instructional Technology and Distance Learning*, vol. 2, Oct. 2005, pp. 3–18.
[34] B. Anrig, E. Benoist, and D.-O. Jaquet-Chiffelle, “Virtual? Identity,” *FIDIS Deliverable 2.2: Set of use cases and scenarios*, 2005, pp. 22–34, Available online: www.fidis.net.
[35] D.V. Klein, “‘Foiling the cracker’: A survey of, and improvements to, password security,” *Proceedings of the 2nd USENIX Security Workshop*, 1990, pp. 5–14.
[36] A.H. Lashkari, S. Farmand, D.O.B. Zakaria, and D.R. Saleh, “Shoulder Surfing attack in graphical password authentication,” *arXiv:0912.0951*, Dec. 2009, Available online: http://arxiv.org/abs/0912.0951, (Accessed: May 12, 2012).
[37] A.K. Jain, A. Ross, and S. Prabhakar, “An introduction to biometric recognition,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, Jan. 2004, pp. 4– 20.
[38] M. Quigley, *Encyclopedia of Information Ethics and Security*, Idea Group Inc (IGI), 2008.
[39] Federal Financial Institutions Examination Council, “Authentication in an Internet Banking Environment,” Oct. 2005, Available online: http://www.ffiec.gov/pdf/authentication_guidance.pdf, (Accessed: March 12, 2012).
[40] N.K. Ratha, J.H. Connell, and R.M. Bolle, “Enhancing security and privacy in biometrics-based authentication systems,” *IBM Systems Journal*, vol. 40, 2001, pp. 614–634.
[41] A. Freier, P. Kocher, and P. Karlton, “The Secure Sockets Layer (SSL) Protocol Version 3.0” Available online: http://tools.ietf.org/html/rfc6101, (Accessed: June 7, 2012).
[42] National Science and Technology Council (NSTC), Committee on Technology, Committee on

Homeland and National Security, Subcommittee on Biometrics, “Biometrics Glossary,” Sep. 2006, Available online: http://www.biometrics.gov/Documents/Glossary.pdf, (Accessed: March 23, 2012).

[43] Office Of Management and Budget (OMB), “Memorandum on E-Authentication Guidance for Federal Agencies,” 2003, Available online: http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf.

[44] W.E. Burr, D.F. Dodson, and W. Timothy Polk, “NIST SP 800-63 Version 1.0.2, Electronic Authentication Guideline,” *National Institute of Standards and Technology*, 2006, Available online: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

[45] Federal Identity, Credentialing, and Access Management (ICAM), “ICAM OpenID 2.0 Profile,” Nov. 2009, Available online: http://www.idmanagement.gov/documents/ICAM_OpenID20Profile.pdf, (Accessed: June 1, 2012).

[46] 3G Americas, *Identity Management - Overview of Standards & Technologies for Mobile and Fixed Internet*, 2009, Available online: http://www.4gamericas.org/documents/3GAmericas_Unified_Identity_Management_Jan2009.pdf, (Accessed: February 13, 2012).

[47] J. Rønager, *Interview and Meeting about EEG and authentication.*, Aalborg University Copenhagen: 2012.

[48] J.D.W. (Jr.), N.M. Orlans, and P.T. Higgins, *Biometrics*, McGraw-Hill/Osborne, 2003.

[49] W.J. Lawson, “The New Wave ‘Biometric Access & Neural Control’,” *The International Center for Disability Resources on the Internet*, Apr. 2002 Available online: http://www.icdri.org/biometrics/new_wave.htm, (Accessed: May 3, 2012).

[50] E.W. Weisstein, “Moving Average -- from Wolfram MathWorld” Available online: http://mathworld.wolfram.com/MovingAverage.html, (Accessed: May 28, 2012).

[51] “Weighted Moving Averages: The Basics,” *Investopedia* Available online: http://www.investopedia.com/articles/technical/060401.asp, (Accessed: May 28, 2012).

[52] “Exponential Moving Average (EMA) Definition | Investopedia,” *Investopedia* Available online: http://www.investopedia.com/terms/e/ema.asp, (Accessed: May 28, 2012).

[53] D.M. Goldenholz, S.P. Ahlfors, M.S. Hämäläinen, D. Sharon, M. Ishitobi, L.M. Vaina, and S.M. Stufflebeam, “Mapping the Signal-To-Noise-Ratios of Cortical Sources in Magnetoencephalography and Electroencephalography,” *Human brain mapping*, vol. 30, Apr. 2009, pp. 1077–1086.

[54] T.-W. Lee, A. Ziehe, R. Orglmeister, and T. Sejnowski, “Combining time-delayed decorrelation and ICA: towards solving the cocktail party problem,” *Acoustics, Speech and Signal Processing, 1998. Proceedings of the 1998 IEEE International Conference on*, 1998, pp. 1249 –1252 vol.2.

[55] S. Stergiopoulos, ed., *Advanced Signal Processing Handbook: Theory and Implementation for Radar, Sonar, and Medical Imaging Real Time Systems*, CRC Press, 2000.

[56] “EEG Coherence: An Introduction : Journal of Clinical Neurophysiology” Available online: http://journals.lww.com/clinicalneurophys/Fulltext/1999/11000/EEG_Coherence__An_Introduction.1.aspx, (Accessed: May 28, 2012).

[57] Marsalek, V. Matousek, P. Mautner, M. Merta, and R. Moucek, “Coherence of EEG signals and biometric signals of handwriting under influence of nicotine, alcohol and light drugs,” *Neural Network World*, vol. 16, 2006, pp. 41–60.

[58] S. Tong and N.V. Thakor, *Quantitative EEG Analysis Methods and Clinical Applications*, Artech House, 2009.

[59] Emotiv, *Emotiv SDK Research Edition Specifications*, Available online: http://www.emotiv.com/upload/manual/sdk/Research%20Edition%20SDK.pdf, (Accessed: May 13, 2012).

[60] M.S. Myslobodsky, R. Coppola, J. Bar-Ziv, and D.R. Weinberger, “Adequacy of the International 10-20 electrode system for computed neurophysiologic topography,” *Journal of clinical neurophysiology: official publication of the American Electroencephalographic Society*, vol. 7, Oct. 1990, pp. 507–518.

[61] J.D. Trobe, *The Neurology of Vision*, Oxford University Press, 2001.

[62] D. Cernea, P.-S. Olech, A. Ebert, and A. Kerren, “EEG-Based Measurement of Subjective

Parameters in Evaluations," *HCI International 2011 – Posters' Extended Abstracts*, C. Stephanidis, ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 279–283, Available online: http://lnu.diva-portal.org/smash/record.jsf?pid=diva2:437169, (Accessed: June 4, 2012).

[63] L.M. Tierstein, "Managing a Designer / 2000 Project," 1997, Available online: http://www.wrsystems.com/whitepapers/managedes2k.pdf.

[64] Gartner, Inc, "Gartner Says Worldwide Smartphone Sales Soared in Fourth Quarter of 2011 With 47 Percent Growth," *Gartner.com*, Feb. 2012 Available online: http://www.gartner.com/it/page.jsp?id=1924314, (Accessed: May 3, 2012).

[65] Google Inc., "Philosophy and Goals," *Android Open Source* Available online: http://source.android.com/about/philosophy.html, (Accessed: May 3, 2012).

[66] Z. Shroff, "Top Smartphones With Front Facing Camera" Available online: http://www.zenilshroff.com/top-smartphones-with-front-facing-camera/, (Accessed: May 5, 2012).

[67] Google Inc., "Android - Introducing Ice Cream Sandwich," *Android.com*, 2011 Available online: http://www.android.com/about/ice-cream-sandwich/, (Accessed: May 23, 2012).

[68] J.-P. Lin, Y.-S. Chen, and L.-F. Chen, "Person Identification Using Electroencephalographic Signals Evoked by Visual Stimuli," *Neural Information Processing*, B.-L. Lu, L. Zhang, and J. Kwok, eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 684–691, Available online: http://www.springerlink.com.zorac.aub.aau.dk/content/80875w91474v4051/, (Accessed: January 31, 2012).

[69] I. Damousis, D. Tzovaras, and E. Bekiaris, "Unobtrusive Multimodal Biometric Authentication: The HUMABIO Project Concept," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, Jan. 2008, p. 265767.

[70] A. Rodriguez, "RESTful Web services: The basics," *IBM.com Developerworks page REST*, Nov. 2008 Available online: http://www.ibm.com/developerworks/webservices/library/ws-restful/, (Accessed: May 8, 2012).

[71] K. Cameron and M.B. Jones, "Design Rationale behind the Identity Metasystem Architecture," Jan. 2006, Available online: research.microsoft.com/~mbj/papers/Identity_Metasystem_Design_Rationale.pdf.

[72] K. Cameron, "The Laws Of Identity," *IdentityBlog*, May. 2005 Available online: http://www.identityblog.com/?p=352, (Accessed: May 16, 2012).

[73] Quasar USA, "EEG: DSI 10/20," *Quasar*, 2010 Available online: http://www.quasarusa.com/products_dsi.htm, (Accessed: May 16, 2012).

[74] K. Smith, *Face Recognition*, National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, 2006, Available online: http://www.biometrics.gov/Documents/facerec.pdf, (Accessed: May 25, 2012).

[75] J. Rønager, "Demonstration of prototype system and roundtable discussion," May. 2012.

[76] D.K. Publishing, *Brain Training: Boost memory, maximize mental agility, & awaken your inner genius*, DK ADULT, 2009.

[77] Emotiv Systems, "Emotiv EPOC," *Emotiv Wiki*, Jun. 2011 Available online: http://emotiv.wikia.com/wiki/Emotiv_EPOC, (Accessed: June 4, 2012).

# Appendices

## Appendix 1 - Glossary

| Abbreviation | Description |
|---|---|
| AJAX | Asynchronous JavaScript and XML |
| API | Application Programming Interface |
| ATM | Automatic Teller Machine |
| CC | Cross-correlation |
| CMA | Centred Moving Average |
| CMS | Common Mode Sense (active electrode) |
| CSS | Cascading Style Sheets |
| CSV | Comma Separated Value |
| DLL | Dynamic-Link Library (Microsoft file format for executables) |
| DNA | Deoxyribonucleic Acid |
| DRL | Driven Right Leg (passive electrode) |
| DSP | Digital Signal Processing |
| EEG | Electroencephalogram / Electroencephalography |
| fMRI | Functional Magnetic Resonance Imaging |
| GNU | GNU's Not Unix |
| GPL | General Public License |
| GPS | Global Positioning System |
| HTML | Hypertext Markup Language |
| HTTP | Hypertext Transfer Protocol |
| Hz | Hertz |
| ICA | Independent Component Analysis |
| ICAM | Federal Identity, Credentialing and Access Management |
| MEG | Magnetoencephalography |
| MMA | Modified Moving Average |
| NIST | National Institute of Standards and Technology (American agency) |
| OMB | The American Office of Management and Budget |
| PSD | Power Spectral Density |
| REST | Representational State Transfer |
| RFC | Request For Comments (Internet-related documents published by the Internet Engineering Task Force) |
| RFID | Radio-frequency identification |
| SDK | Software Development Kit |
| SMA | Simple Moving Average |
| SNR | Signal-to-noise Ratio |
| WiFi | Wireless Fidelity |
| XML | Extensible Markup Language |
| ZCR | Zero-crossing Rate |

# Appendix 2 - Project Work Organization

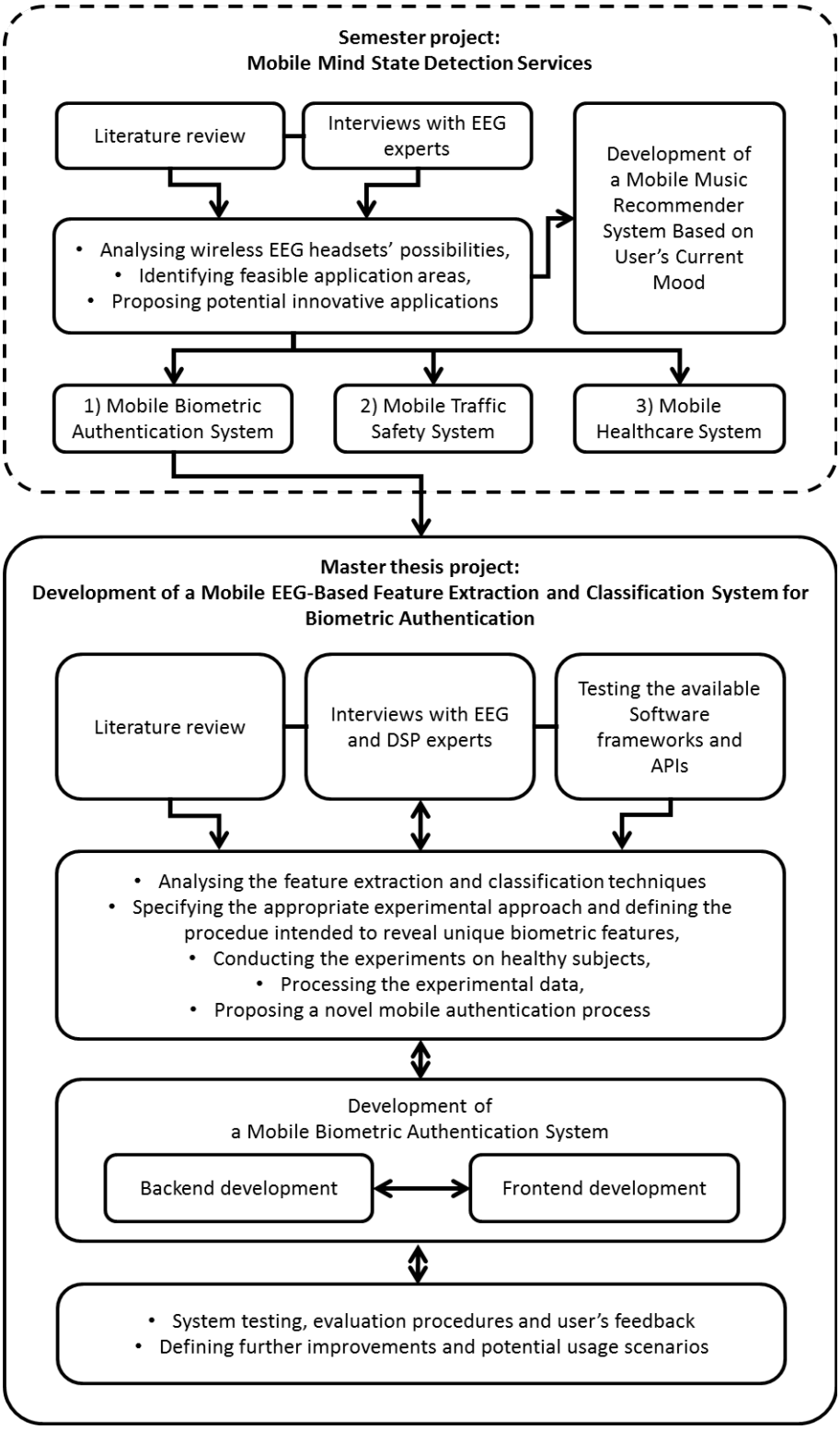


*Figure 25: Project work organization representing main sequential procedures*

## Appendix 3 - Use Case Specifications

| **Authenticate user** | |
|---|---|
| ID: | UC1 |
| Description: | This use case authenticates a user into the system by displaying an image with a known face while recording the user's brain-waves with EEG. |
| Purpose: | Authenticate a user into the system. |
| Primary actors: | User |
| Secondary actors: | None |
| Pre conditions: | The user must have created a user profile with a selected image as specified in UC2. |
| Main flow: | 1. User swipes his or her personal NFC tag against the phone.<br>2. If the system recognizes the user, the username will be displayed and the Continue button made clickable.<br>3. User clicks the Continue button.<br>4. The system shows the phone's camera preview and asks the user to place his or her face in front of the phone.<br>5. If the system detects a face in front of the camera, it will make the mobile phone vibrate to indicate that the user should be ready to record his or her brain-waves.<br>6. The system displays the user's image for five seconds while recording brain-waves.<br>7. The system checks whether the recorded brain-waves matches the pre-recorded ones.<br>8. If there's a positive match:<br>a) The user is successfully authenticated and the system displays a “Success” page.<br>9. Else:<br>a) The user cannot be authenticated and the system displays an “Access denied” page. |
| Post conditions: | User is either granted or denied access. |
| Alternative flow: | If the specified user/NFC tag/username doesn't exist, the login process must be discontinued. |

| **Create new user** | |
|---|---|
| ID: | UC2 |
| Description: | This use case creates a new user profile by letting the user type his or her credentials and select a password-image. |
| Purpose: | Creates a new user profile. |
| Primary actors: | User |
| Secondary actors: | None |
| Pre conditions: | The must wear the Emotiv Epoc EEG headset. |
| Main flow: | 1. User goes to the page “Create new user”.<br>2. User types desired username and age.<br>3. User selects a password-image from a system pre-defined pool of images.<br>4. User clicks the button “Create user”.<br>5. The system makes the mobile phone vibrate to indicate that the user should be ready to record his or her brain-waves.<br>6. The system displays the image chosen in step 3 for five seconds while recording and saving the brain-waves.<br>7. The system shows a 'User created' page. |
| Post conditions: | User profile is created. |
| Alternative flow: | None. |

## Appendix 4 - Risk Analysis

The project group has created the following risk analysis that identifies different risks associated with the project. The intention of the risk analysis to ensure that the project group is prepared to meet potential risks. The analysis touches upon both the project progress oriented parts of the project as well as the development oriented parts. All identified risks are listed, together with an estimate of how likely they are, what the consequences would be and what actions to take.

| Risk | Probability | Consequence | Action |
|---|---|---|---|
| EEG is not useful for authentication. | Low | High | Change outcome of project and develop identification system instead. |
| EEG is not useful for identification. | Low | High | Change outcome of project and develop eye blink system instead. |
| The Emotiv headset is not accurate enough for authentication. | Medium | High | Write intentions and potential solutions instead. Go as far with development as possible. |
| Prototype system only works as intended on few people. | Medium | Low | State this difference in report and analyze potential use cases. Optionally reveal why it only works on few people. |
| Sensor placement makes the system inaccurate. | Low | Low | Don't move sensors on test persons; write guide for correct sensor placement; |
| EEG features are changing over time, making the system inaccurate over time. | Medium | Low | Not enough knowledge to estimate probability, but doesn't influence project. Write about age influence on EEG. |
| Difficult to ensure same conditions of subject person. | Medium | High | Write how the system could react on this. Additional implementation for subject condition detection. |
| Lack of knowledge in processing data. | Medium | Medium | Ask Per Lynggaard for help, use existing sources. |
| Difficult to establish connection between mobile and headset. | High | Low | Use laptop as intermediate. |
| Loss of data. | Medium | Medium | Make backups, use version control systems. |
| The time schedule exceeds. | Medium | High | Planning, organize tasks in Gantt chart. |
| Agreements not respected. | Low | Medium | Daily follow-up, communication. |

## Appendix 5 - Project Plan and Task List

The following table shows an overview of the time plan made for this project divided into major milestones with their corresponding tasks.

| ID | Start date | Deadline | Task |
|---|---|---|---|
| | **01-02-2012** | **29-02-2012** | **Inception phase** |
| 1 | 01-02-2012 | 28-02-2012 | Literature study. |
| 2 | 06-02-2012 | 20-02-2012 | Arrange interview with Jesper Rønager. |
| 3 | 13-02-2012 | 14-02-2012 | Create Dropbox folder for sharing documents. |
| 4 | 15-02-2012 | 16-02-2012 | Create initial report with table of contents. |
| 5 | 13-02-2012 | 17-02-2012 | Carry out initial EEG experiments. |
| 6 | 20-02-2012 | 22-02-2012 | Arrange interview with Per Lynggaard regarding DSP. |
| 7 | 22-02-2012 | 22-02-2012 | Meeting with Per Lynggaard regarding DSP. |
| | **01-03-2012** | **31-03-2012** | **Elaboration phase** |
| 8 | 01-03-2012 | 06-03-2012 | Get software tools from Emotiv (ask Niels for credentials). |
| 9 | 08-03-2012 | 08-03-2012 | Meeting with Jesper Rønager. |
| 10 | 09-03-2012 | 12-03-2012 | Summarize outcomes of interview. |
| 11 | 12-03-2012 | 16-03-2012 | Create requirement specification. |
| 12 | 12-03-2012 | 16-03-2012 | Plan and carry out EEG experiments with visual stimuli. |
| 13 | 14-03-2012 | 16-03-2012 | Make risk analysis. |
| 14 | 19-03-2012 | 31-03-2012 | Write about authentication systems. |
| 15 | 23-03-2012 | 31-03-2012 | Write about challenge-response. |
| 16 | 27-03-2012 | 27-03-2012 | 2nd meeting with Per Lynggaard regarding DSP and wavelets. |
| | **01-04-2012** | **01-05-2012** | **Construction phase** |
| 17 | 02-04-2012 | 05-04-2012 | Create flow chart for authentication process. |
| 18 | 02-04-2012 | 30-04-2012 | Develop prototype system |
| 19 | 09-04-2012 | 13-04-2012 | Investigate Phonegap vs. phone hardware integration. |
| 20 | 02-04-2012 | 14-04-2012 | Implement front-end in jQuery Mobile. |
| 21 | 09-04-2012 | 20-04-2012 | Create face detection functionality in Android. |
| 22 | 16-04-2012 | 23-04-2012 | Implement motion detection algorithm using accelerometer. |
| 23 | 01-04-2012 | 09-04-2012 | Writing scripts in Matlab for EEG analysis. |

| ID | Start date | Deadline | Task |
|---|---|---|---|
| 24 | 09-04-2012 | 16-04-2012 | Analyse experiment data. |
| 25 | 16-04-2012 | 20-04-2012 | Selecting feature extraction techniques. |
| 26 | 20-04-2012 | 24-04-2012 | Setup EEG signal acquisition and preprocessing module for generating EEG data packages. |
| 27 | 24-04-2012 | 27-04-2012 | Implementing C# program for extracting selected features and matching them with subjects. |
| 28 | 27-04-2012 | 29-04-2012 | Setup IIS 7.5 backend server and MSSQL 2012 database. |
| 29 | 29-04-2012 | 30-04-2012 | Establish network connection between smartphone front-end and server back-end. |
| 30 | 01-05-2012 | 01-05-2012 | Demonstration of prototype and roundtable discussion (with Jesper Rønager). |
| | **02-05-2012** | **08-06-2012** | **Transition phase** |
| 31 | 02-05-2012 | 07-06-2012 | Report writing. |
| 32 | 02-05-2012 | 08-05-2012 | Write front-end + back-end part. |
| 33 | 08-05-2012 | 13-05-2012 | Write interviews and test/experiments. |
| 34 | 13-05-2012 | 18-05-2012 | Write EEG theory + System usage. |
| 35 | 18-05-2012 | 24-05-2012 | Write related work + analysis and theory. |
| 36 | 24-05-2012 | 01-06-2012 | Write introduction, create graphs, improve report. |
| 37 | 01-06-2012 | 04-06-2012 | Write conclusions. |