AALBORG UNIVERSITET
KØBENHAVN

Semester: 10th

Title:

Realizing the PSD2 open ecosystem utilizing Self-Sovereign Identity

Electronics and IT

Aalborg University Copenhagen

www.aau.dk

Project period:

01/06/22 – 02/06/22

Supervisor(s):

Henning Olesen

Members:

Camilla Schneider Bergman

20173808

Pages: 111

Finished: 01/06/22

Abstract

The increasing digitization presents new possibilities for innovating in established sectors. This entails an increasing demand in privacy and transparency to instil digital trust.

This thesis presents how established structures and ecosystems within the financial sector payment landscape and digital identity management systems could be changed due to the EU initiatives of PSD2 and eIDAS 2.0.

The thesis presents deployment proposals to illustrates how the Self-Sovereign Identity and Financial-grade API frameworks could be utilized for realizing the novel trust relationship among the entities within the payment landscape, while accommodating an increased demand in data privacy, transparency and trust.

Contents

List of abbreviations

2FA	Two-Factor Authentication
AISP	Account Information Service Provider
AML	Anti-money Laundering
API	Application Programme Interface
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
eIDAS	Electrict Identification, Authentication and trust Services
FAPI	Financial-grade API
GDPR	General Data Protection Regulation
IdP	Identity Provider
KYC	Know-Your-Customer
PISP	Payment Initiation Service Provider
PSD2	Payment Service Directive revised
RTS	Regulatory Technical Standards
SCA	Strong Customer Authentication
SSI	Self-sovereign Identity
TPP	Third Party Providers
VC	Verifiable Credentials

Chapter 1

Introduction

The financial sector consists of well-established structures and procedures for ensuring trust. The ecosystem of the sector has consisted of established trust relationships among the banking institution, its customers, as well as the entities involved with the payment transaction processes [25].

The Revised Payment Service Directive (PSD2) introduced by the European Union aims to liberalise the sector by lowering the barrier of entrance for new service providers [54], while enhancing security and strong customer protection [65]. The legislation aims to improve customer choice by enabling a broader environment for information sharing and payment initiation [44], by enabling third party service providers direct access to customers' banking data through open APIs [5].

The PSD2 is a shift from product-centric to user-centric [65], and ensures that third party service providers are subject to security requirements in order to establish trust with consumers [58]. This entails new challenges, and further increases the complex digital trust relationships that customers find themselves in among the entities handling personal identifiable data (PID) [44].

eIDAS 2.0 initiative addresses this issue by promoting the right for all individuals to have a digital identity, that enables citizens to share identification information in multiple contexts [52], and manage their provider trust relationships in a transparent manner that enables control and ownership [44]. This requires a digital identity and a verifiable credential

ecosystem, that provides the required transparency and trust in digital service providers [44].

1.0.1 The importance of trust

Opening up ecosystems entails a need to address the increasing demand for data privacy and trust, by enhancing the ability of digital identities to enable trust while preserving individual privacy [13]. Digital identity is defined as *the relationship of identity between a person at enrolment time, and a person at authentication time* [77]. This implies that digital identity is a process, that depends on several factors for ensuring the integrity of this process, respectively the reliability of the process of registration, verification and enrolment, the integrity of credentials used, and the strength of the verifiable link between the credentials and the person presenting them [77].

In order to innovate within the financial sector, third party service providers must build trust with its customers. Trust depends on the aspects of context, controls and consent [77], which implies the need for privacy and security of PID. Privacy is defined as *the ability of individuals to have control over how personal information in collected and used*, and focuses on the use and governance of individual data [56]. The contextual background of digital activities must be transparent for controls of how information is used can be governed, and consent provided, as the latter signifies knowledge of why information is disclosed and how it is processed [61].

1.0.2 Digital Identity

Identity is how we are recognized by our surroundings [77]. The evolution of digital identity management systems and digital identities have advanced through four stages from centralized identities based on hierarchy authorities [4], to federated identities where separate communities with several hierarchies corporate to share trusted digital identities [4]. This federated evolved into a user-centric identity-form developed by the OpenID Foundation [4]. Despite being user-centric, this form of identity issuance depends on centralised control, resulting in the lack of privacy for customers, as the identity provider is in control and aware of all activity [44].

Self-Sovereign Identities (SSI) constitutes the fourth stage of the digital identity evolution [13]. It takes a step towards true user control, as the digital identity is detached from the dependence of centralized hierarchies for managing authority [13]. Self-Sovereign Identity translates to *a person's identity that is neither dependent or subject to any other power or state* [61].

According to Enisa, the EU Agency for Cybersecurity, SSI provides an effective basis for digital identities for protecting the privacy of personal data [4] by not relying on a centralized authentication authority. Verifiable credentials are stored in a data wallet, and enables the separation of private attributes from the digital identity to ensure data minimization, which is achieved through selective data disclosure. This allows the user to only reveal the necessary attributes to a relying party. The Data Wallet enables the ability to hold multiple authentication keys in a wallet to separate identity documents from different controllers, which preserves data privacy by avoiding correlation among transactions.

In order to address the increased digitization and to develop the digital single market within the EU, The European Commission presents legislation and initiatives that aims to *break down obstacles and open up opportunities online* [74].

In order to achieve this, consumers must have more freedom and less dependency when engaging in digital transactions.

1.1 Motivation

The motivation for conducting this thesis stems in an interest in investigating the societal trend of data privacy and digital trust apparent today, and how novel legislation and initiatives changes the established trust relationships among the entities of the financial sector.

The well-established structures and ecosystems present today are challenged by novel technology frameworks, respectively Self-Sovereign Identity and Financial-grade APIs, which holds the potential of changing established ecosystem scenarios, by promoting more user empowerment in controlling identity information online, and ensuring the demanded transparency and data privacy by users.

Traditionally, banking data has been kept in data silos within the individual institution, and exchanged with entities of the existing ecosystem with whom there is an established trust relationship. Open ecosystems and the user-centric approach toward digital identities challenges the existing trust relationships, and if not handled properly, the data privacy and security of users might come at the expense of innovation.

This thesis sets out to investigate how innovation, competition and trust can be fostered in the financial sector, while protecting data privacy. The goal of the thesis is to present a potential outcome of how the trust of the established ecosystem is shifted, and how Self-Sovereign Identity framework and FAPI specification can support the deployment proposals.

1.2 Problem formulation

How can Self-Sovereign Identity support the implications of the liberalization of banking services that the PSD2 entails?

- How does PSD2 and open ecosystems affect the trust relationships within the financial sector?
- How can the assurance levels required for high-risk financial payment transactions be achieved through Self-Sovereign Identities?
- How does the evolution towards SSI shift the trust relationships?

1.3 Limitations

Digital services extends across borders globally, whereas legislation is narrowed down to apply within physical demarcated areas. This thesis is limited to investigate legislation applied within the European Union only, which concerns institutions and citizens who operate within the European Union and the European Economic Area.

The financial sector consists of a broad range of industries, that ranges from banks, real estate companies, investment and insurance companies. These firms provide a variety of services to its customers. This thesis solely focuses on the services that banks, credit card providers, payment intermediaries and commercial market actors of this nature offer its customers in the context of the PSD2.

Chapter 2

Methodology

The thesis sets out to investigate how initiatives from the EU, respectively the PSD2 and eIDAS 2.0, changes the established trust relationships within financial institutions and its ecosystem. The research approach applied for this thesis was deductive, as existing findings of previously conducted research has been analysed. The overall deductive approach is displayed in Figure 2.1, and outlines the steps involved, respectively the general focus, followed by analysis of collected data in order to synthesis the data for the purpose of presenting deployment proposals.

In order to investigate this area, and to address the problem formulation, a hybrid methodological approach incorporating both quantitative and qualitative methods has been applied. The research design is a combination of desktop research and semi-structured interviews.

The quantitative approach has been utilised to collect and analyse secondary data sources, the thesis builds upon combined data sources, respectively published scientific research, white papers, statistical data and grey literature, including online sources. The scientific articles analysed has been peer-reviewed and published in scientific journals. These have been obtained through the research portals accessible through the Aalborg University library, respectively Elsevier, ScientificDirect and SpringerLink. Articles have been selected based on the criteria of publication date. The scientific articles utilised are published in 2019 or later, technical reports utilised have are published in 2018 or later, and statistical data taken into consideration have been published in 2020 and later.

Due to the novelty of the research field, the process has consisted of on-going iterations. Figure 2.1 displays the process in a high level manner. As displayed, the process started with a general focus of societal trends and initiatives proposed by the EU. By analysing the collected data it became clear that in order to achieve the ambition of opening up opportunities online, technological frameworks must support these initiatives which changes traditional ecosystems. I have worked with the latest developments in Financial-grade APIs and the Self-Sovereign Identity framework, which is still under development, and tried to applied these in a specific area. As no standardized approach for neither SSI or FAPI has been agreed upon, the handling of some processes have not determined upon, which limits the scope of the research.

In order to investigate trust, privacy and how technologies can support legislation, I have interviewed three experts within the area. The qualitative method utilised was semi-structured interviews, and the experts were selected based on the criteria of representing different actors, respectively the area of trust in organisations, the area of identity and management systems and the area of financial services.

The basis for conducting these interviews, were to gain an in-depth understanding of the domain and to identify requirements for the deployment proposals. The diversity in the background of the participants provided a broad insight into the domain. The questions asked during the interview served as a guideline for the conversation, depending on the background and current position of each interviewee, the questions asked were decided based on these criteria.

The data sources collected and the interviews conducted are synthesized in order to present potential scenarios and deployment proposals for how the technologies can support the novel ecosystems that the paradigms entail.

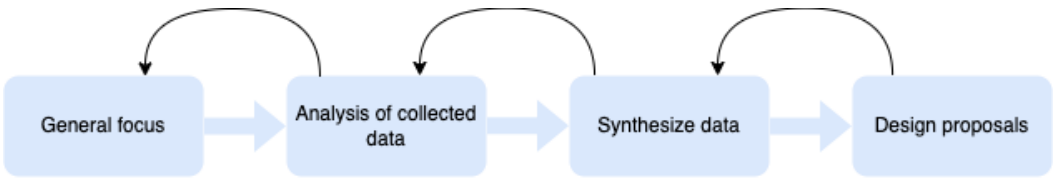

Figure 2.1: Methodological process

Chapter 3

Digital Identity

The following chapter presents the scope of digital identities, and how digital identity management systems have evolved. The EU initiative eIDAS 2.0 is presented, followed by the national Danish eID MitID. Furthermore, the recommendation of EUDI and the technological framework that Self-Sovereign Identity management consist of is presented.

The internet was built without an identity layer, as it was built to interconnect machines [61]. This exposes users to ever growing insecurities, as there is no inherent way of knowing who and what you are connecting to [61].

Digital identities serve as online representations of individuals, and refers to the information that applies to a natural person, including the information that might uniquely identify an individual [28]. Personal identifiable data (PID) is used to confirm an individual's legal identity, and is defined as *any information that relates to an identified or identifiable natural person* [28]. Data that is collected together and by that can lead to the identification of a particular person, does also constitute as personal data and must be protected as such [28]. Examples of PID include identifiers such as; name, email address, social security number, financial data, location data, cookie ID and an identification card number [28].

The bundle of information about the person it pertains to, is used to provide a certain level of trust in the identification of a natural person, respectively the Identification Assurance Level (IAL) [76] [52]. Identity proofing is the process concerned with identifying and verifying

the claims made about a natural person represented by a digital identity. It is the process of collecting identity attributes that supports the stated claims of identification of an individual through reliable identification means to establish trust in the identification process [76]. This process is typically handled by a Registration Authority, Attribute Provider or Credential Service Provider, which provides assertions to the claims [76]. Asserted claims add credibility to the claims to establish trust in the attributes of the holder of such credential. A passport is an example of an asserted claim about a nationality, asserted by the government to establish trust in the credential [12]. Trust in a digital identity is typically established by an Identity Provider, which acts as an intermediary for establishing the digital identity with other parties [76].

Identification is the ability to uniquely identify an individual, concerned with presenting ID information, whereas verification is the process of binding the presented information to the correct identity, to establish trust and accuracy of the identification information [12]. Authentication is concerned with the ability to provide proofs of the claimed identity. Digital authentication provide proofs of a claimed identity by establishing control of one or more valid authenticators, associated with the digital identity of the claimed subject when attempting to access a digital service [12].

The level of trust in a digital identity is establish by the Level of Assurance (LoA) in the accuracy of the identification and authentication processes. The LoA is measured by the strength of the mechanism utilised, defined through three levels of assurance (AAL) [12], respectively low, substantial and high [12].

Digital identities are context-based and used to disclosure different amounts of personal information to service providers, as displayed in Figure 3.1 [12]. The figure displays how a complete digital identify consists of context-based partial identities, and illustrates how a partial digital identity is represented in different contexts [12].

This results in scattered identities and loss of privacy, as tools relied upon to verify a digital identity are scattered across the digital landscape and multiple services providers [42].

PID is a value asset for service providers for financial and commercial purposes, they are collected and exchanged in personal data ecosystems. This increases the risk of privacy loss

and security concerns, as context-based personal data can be used to build comprehensive digital profiles [52] [4].

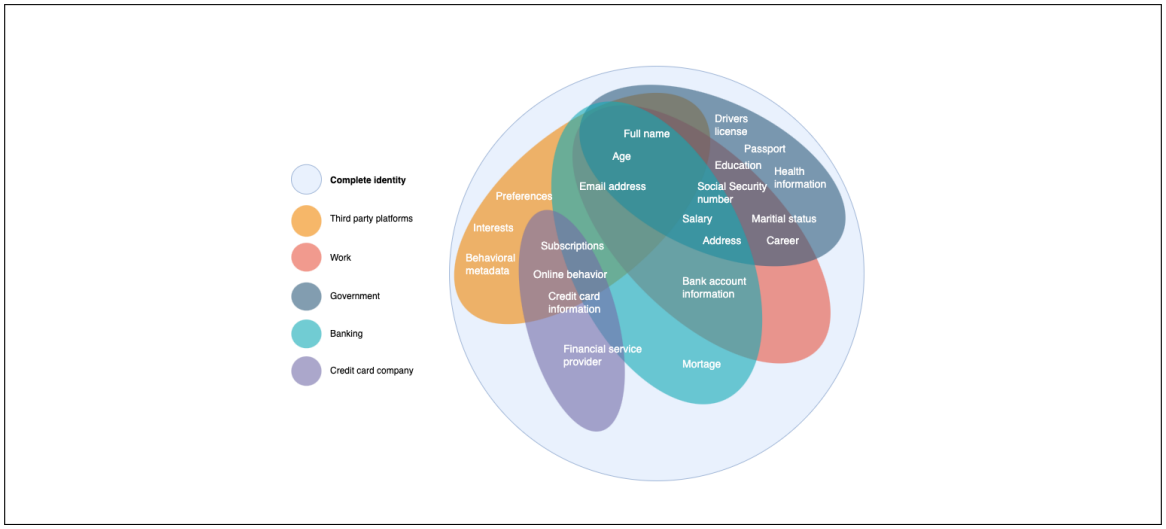

Figure 3.1: Partial digital identity [11]

3.1 Digital Identity Management Systems

Identity management systems are typically structured in such a way, that users rely on a central authority for storing and accessing the personal information used for verifying a digital identity [42]. The Identity management system utilised today in Denmark for public services and high risk scenarios, is NemID and its successor, MitID. It provides identification and authentication, and is based on a federated model for electronic ID solutions [66] [36], as described in section 3.1.1.

The purpose of identity management systems is to provide and establish trust in digital identities. These systems handle authentication and authorization of user access to protected resources, as displayed in a high level manner in Figure 3.2 [11].

Identity management systems have undergone an evolution in order to keep up with the increasing digitization [11]. Traditionally, digital identities have been issued and administered

by a single, centralized authority. This resulted in users being subject to vendor lock-in, as all aspects of the user identity is stored locally, because access to protected resources is managed on the basis of a local account [11]. The issue of the centralized access model is that is scales poorly, and it gives control and power to the centralized entities and not users [11].

Figure 3.2 displays the interactions between the actors in the centralized identity management model the user, the IdP and the Service Provider (SP) respectively [13]. The figure displays the flow of accessing a service at a service provider, when the user needs to provide assertions by a third party trusted entity, the IdP. A trust relationship between the IdP and the RP needs to be established for the user to be able to rely on asserted claims by the IdP for authentication [13]. The user initially approaches the RP, the RP specifies which IdP it has a trust relationship with. The user then interacts with a trusted IdP and requests asserted claims, which is presented to the SP, which will grant access if the asserted claims are approved [13] [11].

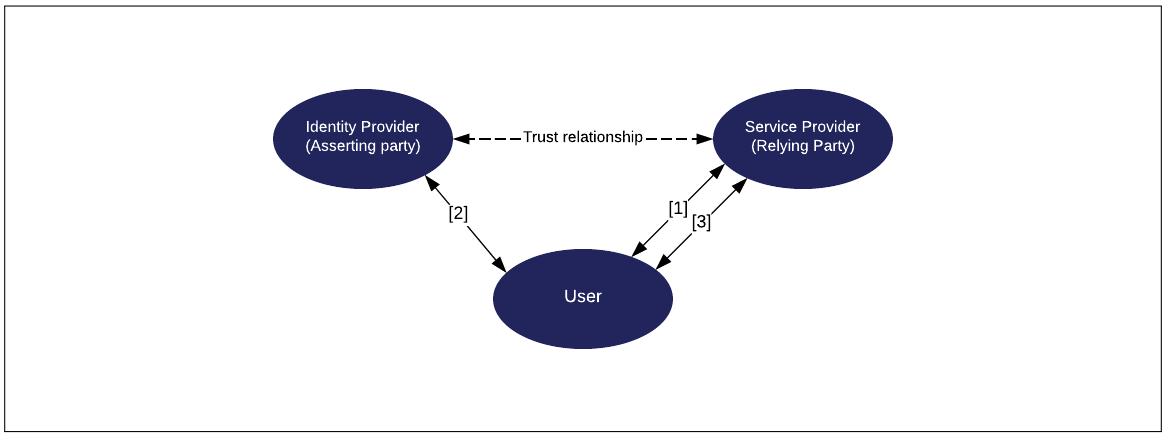

Figure 3.2: Centralized Identity Management System [13] [42]

As an improvement to the centralized model, federated models were adopted. The federated access model builds upon the principles of the centralized identity management model, but it allows users to utilize the same identity with multiple service providers [13], where service providers have multiple established trust relationships with multiple IdPs [14]. The established trust relationships enables the the SP to receive assertions from the same IdP.

In order to establish a trust relationship in the assertions of a digital identity, the intermediary that acts as an IdP must have an established trust relationship with its relying parties, as displayed in Figure 3.2, which illustrates the high level architecture of a centralized identity management model. Trust among a user and an IdP is established through the means of binding identity data with a legal person, who can be prosecuted under the law [66] [36].

Trust is represented by demonstrating control over an authenticator, such as a smartphone app combined with biometrics for verifying the authenticity of the individual. Providing such evidence, establishes trust in claimed identity and verifies that the individual is appropriately associated with the claimed real-world identity, and that the means of authentication has not been compromised [12]. This establishes high confidence and trust in the authentication method, which ensures a low risk level and enables users to engage in high risk financial transactions [12].

The federated access model of digital identities has made authentication synonymous with *logging in* through a shared secret. A shared secret in the form of a username and password combination, which force users to create, manage a comprehensive amount of shared secret combinations. This have resulted in the use of less secure, easy-to-remember passwords, and commonly re-using passwords for multiple accounts [14]. The advantage of this access model is that the service provider does not need to verify a user's credentials, as the user authenticates on the basis of a profile associated with an IdP [11]. This allows the user to access multiple services based on trust federations, dividing the power of a centralized authority among several entities [13], presuppose that there is an established trust relationship among the IdP and the SP.

Such federated access systems allow users to login through a third-party IdP such as Facebook or Google. This model sacrifices security and privacy for convenience, by allowing a third-party intermediary in the middle of all interactions online [14]. Digital identities issued by a third-party IdP are controlled by and belongs to the IdP, which reserves the right to terminate your access at any time [14].

Although this model comes with a variety of advantages compared to the initial access model, the drawback of the federated access model is that it is the IdP that determines the limits of the use of the digital identity [11].

The third phase denoted the user-centric identity, places the user in the middle of the identity process, by focusing on user consent and interoperability [13]. Adopting such a method for creating a digital identity, a user can decide to share an identity across multiple authorities without requiring a federation. This enables a user to own its digital identity [13].

A decentralized model enforces sovereignty and provides better trust and privacy compared to a centralized identity model, where an Identity Provider that evaluates and issues assertions. These tools have the ability to drive digital transformation and to build trust with stakeholder, consumers and society in general [10].

3.1.1 MitID

MitID is the new eID in Denmark and is currently in the process of replacing its predecessor, NemID. MitID offers a national digital identity that is bound to one's legal identity for Danish citizens and residents. It provides digital authentication means for managing all public self-service tasks, such as for tax reporting [66]. It is used in scenarios when a financial institution is involved, e.g. for checking bank statements and when making payment transactions online. It provides identification and authentication as it is tied to one's legal identity. MitID allows its user to sign agreements online by providing a legally valid digital signature [36] [66].

MitID is the central identity provider (IdP) for digital personal identities in Denmark, and ensures identification and authentication for enabling access to online public services and online banking, through the identity management system.

It is based on a federated model, as presented in section 3.1, where a service provider trusts the identity assertions issued by the IdP, as service providers have an established trust relationship with the IdP [66]. The identity proofing process of MitID ensures the substantial Identity Assurance Level, as identification of the individual by requiring the individual to scan the chip that newer passports of Danish citizens has been issued [36]. When the passport

has been scanned, the MitID system checks the validity of the passport through the National Police's database system. This process ensures the substantial Identity Assurance Level required for the majority of use cases to which this digital identity applies. This way, the digital identity provided by MitID is tied to a legal person which can be prosecuted [66] [36].

MitID is developed in collaboration between the Danish public sector and the Danish financial institutions. The infrastructure is build upon a broker model, where both financial and commercial brokers mediate access to MitID for the service providers, and thereby handles the technical implementation of the system. The brokers of MitID is NemLog-in3, the SAML-based SSO for business identities [32], MitID Broker, five commercial market actors and the financial institutions, BankData, Danske Bank, Nordea and SDC respectively [31] [36]. This model limits the number of entities that have access to the identities, which increases security and limits compliance requirements for service providers [36].

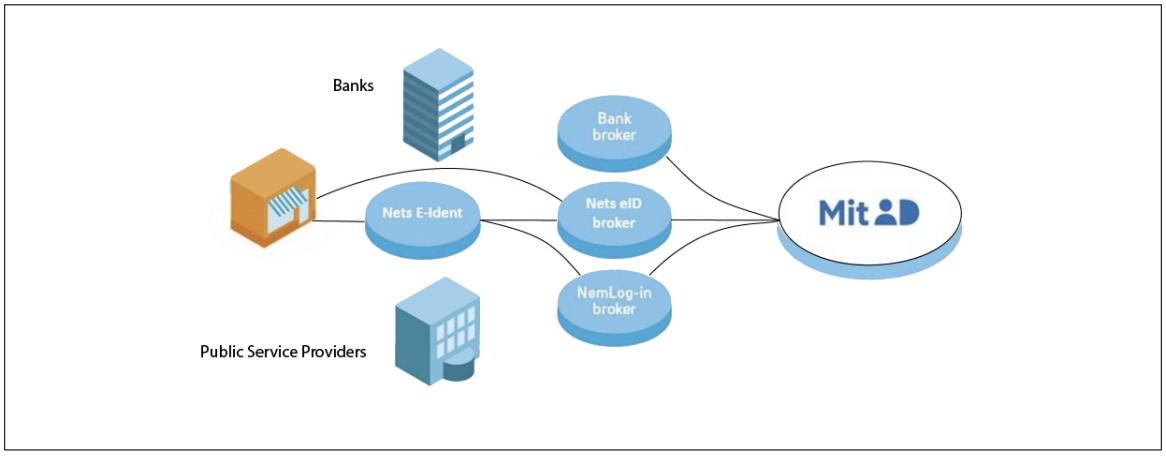

Figure 3.3: MitID brokers [48]

It is based on the OAuth 2.0 framework for authorization, and OpenID Connect for providing an identity layer on top of the OAuth 2.0 protocol [36]. The top level architecture is displayed in Figure 4.2, and consists of the MitID end user, the distributed brokers and their associated organisations. As displayed, for the user to request MitID to act as IdP, the service provider must have a trust relationship with one of the brokers of the ecosystem [66].

MitID Authentication Process

MitID presents several ways for a user to verify their identity through different means of authentication. The user logs in with a user name, which decides the possible authenticators that the user has preregistered, respectively password, MitID audio code reader, MitID code display, MitID app and MitID chip. The following authentication process is concerned with the MitID app, as this method is the most widely used and is sufficient to reach Authentication Assurance Level (AAL) substantial [29].
The end user navigates to a service provider platform that requests authentication through MitID prior to being allowed access to a protected resource. The end user requests to log on, and is redirected to the MitID Broker to begin identification. MitID Broker sends an Auth request to the user agents, to which the end user provides their credentials. User input is sent to the MitID Broker which evaluates the input credentials, and if accepted, the user agent is redirected to the relying party redirect_uri by appending the authorization code, nonce and state parameters [29].

The relying party uses the authorization code to request the ID token and the optional access token. The authorization code is validated by the MitID Broker, which returns the ID and optional access token, if the authorization code is accepted [29].

The relying party validates the ID token, and uses the access token to request claims and PSD2 token for the authentication in question. MitID Broker returns the full list of claims and tokens to the relying party. The relying party redirects the user agent to the protected site. The sequence diagram in Figure 5.3 displays the data flow occurring for the process of authenticating and authorization an end user through MitID at a relying party. The authorization flow results in an ID token and an access token, which are formatted as JSON Web Tokens (JWT) [66].

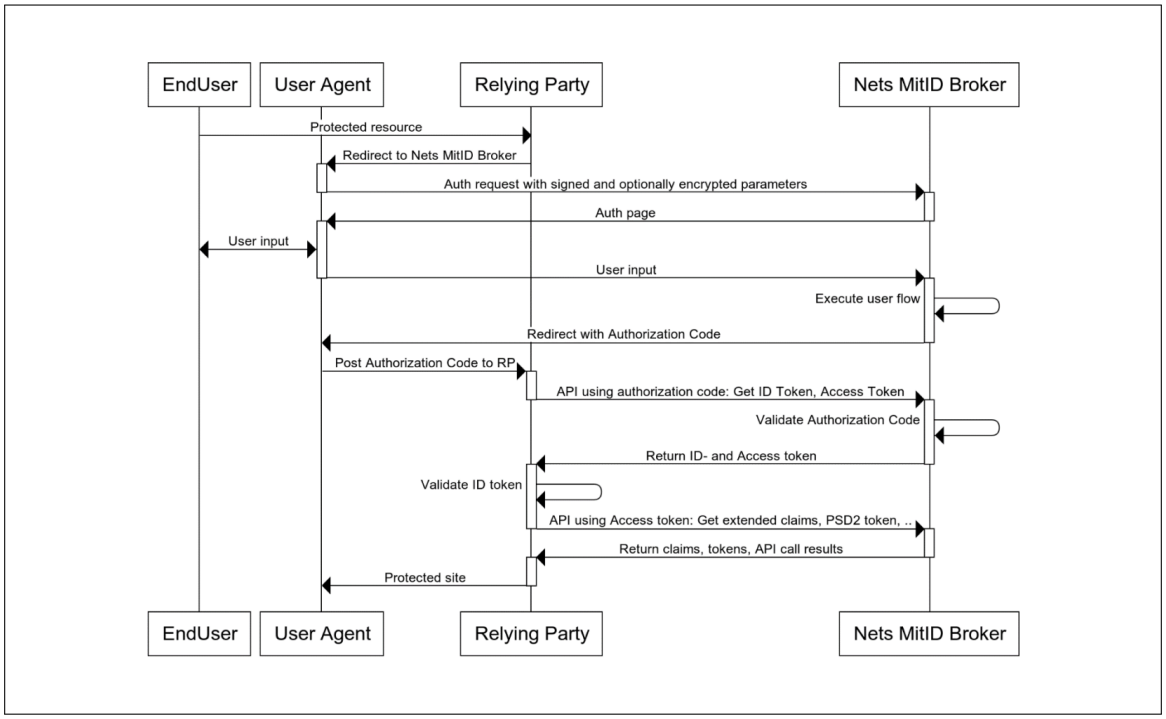

Figure 3.4: Data flow MitID authentication [66]

3.1.2 eIDAS 2.0

The electronic identification and trust services (eIDAS) regulation (EU) 910/2014 refers to a range of services concerned with verifying the identity of natural legal persons and businesses online [52]. The regulation seeks to enhance trust in the online environment, as the lack of trust makes consumers and businesses hesitate to adopt to new technology, especially technology which carry out transactions electronically [52].

The regulation aims to standardise the use of electronic identification (eID), which refers to identifying and authenticating an individual through digitally-stored identity data equivalent to traditional identity means involving physical credentials. It is a digital method for *guaranteeing the unambiguous identification of a person* [27] to tackle identification challenges experienced by digital public services across EU borders [30].

The purpose of eIDAS is to enhance trust, to ensure the proper functioning of the internal market within the European Union [**Article 1**, 52]. The regulation provides the conditions

under which Member States of EU must recognise means of electronic identification of natural and legal persons that falls under an electronic identification scheme of another Member State, rules of trust services which in particularly concerns electronic transactions [52]. In continuation of this, the regulations establishes a legal framework for electronic signatures, seals, time stamps, document, registered delivery services and certificate services for website authentication [**Article 1**, 52]. It applies to trust service providers established within the Union, and electronic identification schemes which have been notified by a Member State [**Article 2**, 52].

For electronic identification and authentication means to be applicable within EU, the electronic identification means issued in another Member State must be recognised in the first Member State for the purpose of cross-border authentication [**Article 6**, 52]. To be recognised, the electronic identification means must correspond to an assurance level equal to or higher than the assurance level which is required by the relevant public sector, if the assurance levels corresponds to substantial or high [**Article 6**, 52].

Article 8 of the regulation defines the level of assurance (LoA), that electronic identification schemes must adhere to. LoA *should characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned* [53], while taking the process of authentication and identity assurance into consideration [53].

Authentication assurance presents the strength of the methods utilized within the process of authentication, whereas the identity assurance presents the method of identity proofing at the time of registration [52]. The LoA ranges from low, substantial to high, and must meet the following criteria [**Article 8**, 52]:

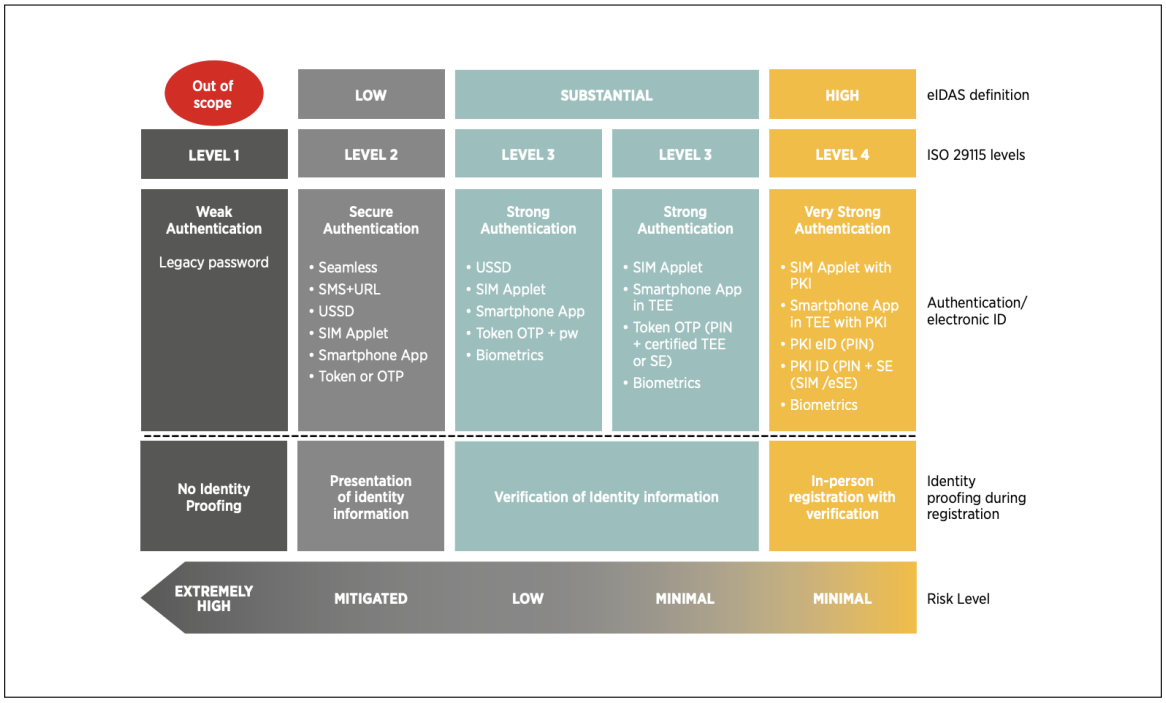

Figure 3.5: Assurance Levels [6]

3.1.3 European Union Digital Identity Wallet

Following the eIDAS 2.0 initiative, the European Commission has adopted a recommendation for developing a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework [35]. This Toolbox is developed by Member States' experts regrouped in the eIDAS expert group, and will include a technical architecture, a reference framework, a set of common standards, technical specification along with common guidelines and best practice. Data privacy and digital sovereignty are key priorities for the EU, and constitutes a central element in the development of the European Digital Identity Wallet [35].

It is a combination of several trust services which allows users to share data about themselves and electronically sign and seal documents [35]. It aims to solve the problems of the cross-border use of eIDs that does not work to a satisfying degree, and fragmented eID infrastructures, concerned with multiple eIDs for different use cases and applications areas, respectively [35]. Essentially, the EUDI Wallet is an application for citizens, which can re-

ceive and store digital credentials and interact with third parties on the basis of these in order to gain access to services [43].

The purpose is to develop the European Digital Identity Wallet ecosystem (EUDI Wallet) to promote trusted digital identities for all Europeans. This will enable all citizens to be in control of their online presence and its associated interactions [35].

The working group has approached this development by identifying the initial applications areas, such as health, education, mobility and digital drivers licenses as well as secure and trusted identification to access online service and digital finance [35].

Secure and trusted identification for accessing online services will be enabled, as secure authentication is a functionality of the EUDI Wallet [35]. The use of EUDI Wallet shall be accepted by relying parties in use cases where strong authentication for online identification is required [35]. Within the application area of Digital Finance, the EUDI Wallet could facilitate frictionless in payments and payment authentication with a high degree of security [35].

The EUDI Wallet shall be able to perform user identification and authentication with a specific set of Person Identifiable Data (PID), for identification scenarios within a legal context [35]. Currently, no binding technological choices have been made, as the development is still conceptual. For PID, W3C's Verifiable Credential data model have been considered, combined with utilizing verifiable data registries, such as a distributed ledger in the wallet ecosystem for credentials, is still an open question [35].

The Personal Identification Data providers may be the same organisations that issue identity documents today, such as the government, and would verify the identity of the EUDI Wallet user [35]. Trust is established among providers and verifiers as Qualified Electronic Attestation of Attributes (QEAA) would be provided by Qualified Trust Service Providers (QTSP) to ensure a tight link between the person and the data by issuing high assurance credentials by providers, certified by governmental entities [35].

Providers of registries of trusted sources provides registration services, and information verification for the EUDI Wallet, the PID as well as the QEAA and Attestation of Attributes (EAA). The wallet should be able to perform electronic identification, store and manage

QEAA and EAA locally or remote in a cloud-based infrastructure, for the user to share these with relying parties upon requests [35]. This recommendation shifts the trust relationships from centralized IdP for issuing assertions to a user-controlled model, where issued credentials are stored locally and controlled by the user to which it pertains.

3.2 Self-Sovereign Identities

The concept of the self-sovereign Identity (SSI) describes an identity management system for a decentralised digital identity framework, which operates independently of public and private third-party actors, by separating the digital identity from the centralised and federated models [72], presented in section 3.1. It deals with the way in which a user's identity is managed in the digital realm [11], and aims to decouple identity issuance by centralized authorities to put it into the full control of the users [72].

A digital identity is the body of information contained about an entity, such as an individual or a company, used by services to determine a user identity with the purpose of enabling access to resources [72]. SSI provides the identity holder with a higher degree of control over its digital identity, by distributing identity related information through decentralized identifiers (DIDs) that are issued for different activities, and separating the associated attributes with an identifier in verifiable credentials (VC) [72]. This distinct functionality allows the holder greater control over how its digital identity is presented to parties that rely on the identity information, and the personal information that it reveals to other parties [4].

The self-sovereign model changes this paradigm by utilizing distributed databases and decentralized networks. The difference is that the digital identity is no longer account-based, but based on a direct relationship between a user and its peer, much like a real-world identity [61]. This enable connection sharing, meaning that no one provides, controls or owns the relationship. This control shift is displayed in Figure 3.6. As displayed, the locus of control in the centralized and federated model is with the issuer and verifier in a network [61]. The SSI model, the locus of control is shifted to the individual user, who is able to interact with

everyone else as a full peer [61].

Self-sovereign identities are based on the use of decentralized identifiers (DIDs), verifiable credentials (VC) and a data wallet to support interactions where information must be shared with third parties [11]. The DID identifies that the subject owns a certain set of attestations or claims, and does not provide information about the subject itself. The VCs are signed with the private key associated with a public key, that is associated with the issuer's DID [11] to establish trust. The public key is accessible through a data registry, such a distributed ledger, which shifts the trust relationship from assertions provided by an IdP to a public key infrastructure (PKI) [11] [72].

Figure 3.6 illustrates the shifted trust relationship from the centralized and federated access models towards the SSI model. As displayed, the locus of control, the trust relationship, is among the issuer and the verifier in the centralized and federated model. The SSI model puts the user in control, and establishes verifiable trust relationships among all the entities of the ecosystem, respectively the issuer, user, verifier and data registry [61].

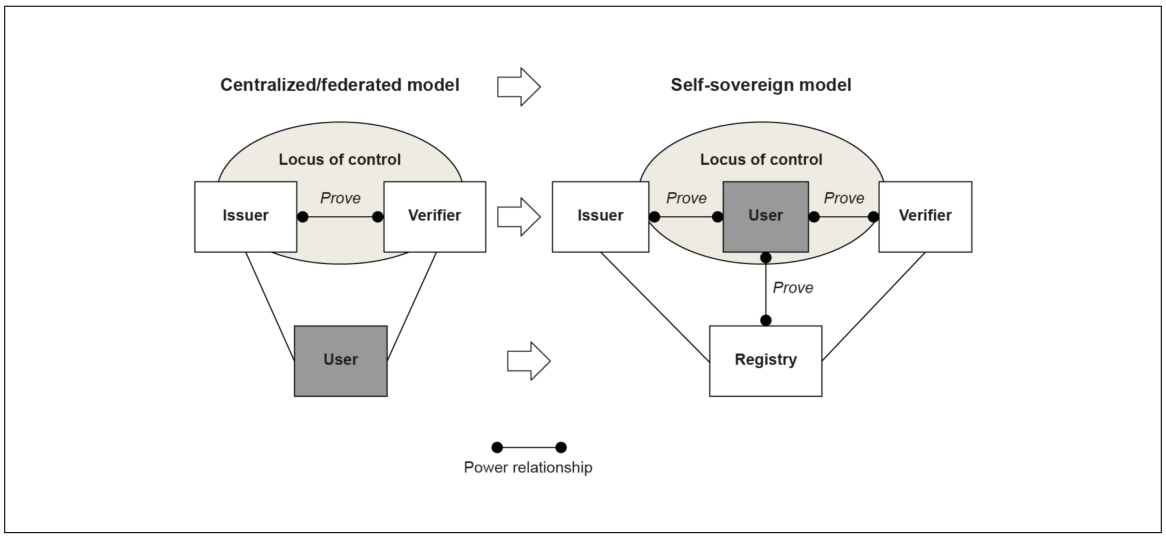

Figure 3.6: The control shift from centralized and federated access model to self-sovereign model [61]

Trusting the issuer's DID establishes trust in the issuer, so that a third party can use this proof to verify ownership and trustworthiness of a presented credential. The presentation of claims is managed by the user itself, which enable users to decide which attributes to share with third parties, allowing for selective disclosure and improving transparency [11]. This functionality holds the potential to reinforce privacy and personal data protection of digital identities [11], as the user owns its digital identity and controls the use of it.

3.2.1 Decentralized Identifier

Self-Sovereign Identity frameworks can be based on the use of decentralized identifiers (DID) and verifiable credentials (VC) [11]. A DID is a novel type of identifier, that contains a text string containing a DID URI scheme identifier, the identifier for the DID method and the DID method-specific identifier, as displayed in Figure 3.7 [71].

The example illustrates a DID which resolves to a DID document, that contains information associated with the DID. The information contained within the DID document can be ways to cryptographically authenticate a DID controller [71].

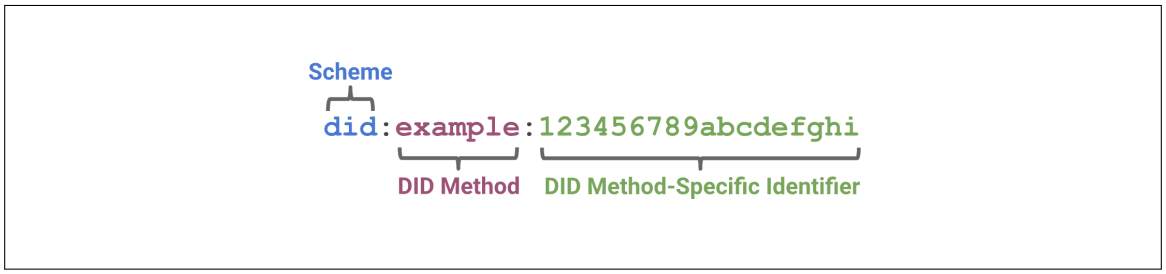

Figure 3.7: DID example [71]

A DID is a uniform resource identifier (URI) that associates a DID subject with a DID document, by providing a unique reference that resolves a DID document [71]. The DID document contains verification methods that provide a set of mechanisms that allows the DID controller to prove control over the DID to another party [4]. The DID document itself does not contain claims or credentials, but a set of data that describes the DID subject, along with mechanisms that the DID subject can use authenticate itself and prove its association

with the DID, such as cryptographic public keys and service endpoints [71].

It does not require a centralized registration authority, as control and ownership of an identifier is proved by cryptography, as every DID is bound to a public-private key (PKI) pair. This functionality removes the control point of digital identifiers from central registries to support a more transparent solution that supports decentralized use cases for enhancing transparency, trust and privacy online [71].

Figure 3.8 provides and overview of the DID architecture and the relationship of its components. The DID identifies the DID subject, which can be a natural person, group, thing or concept [71]. The DID subject might also be the DID controller. The latter is the entity which that has the capability to make changes to the DID document, as defined by the DID method specified in the DID document. The DID is resolved by a DID resolver, which is a system component that handles DID resolution into a conforming DID document, which is a serialization of a DID document that is called a representation [71].

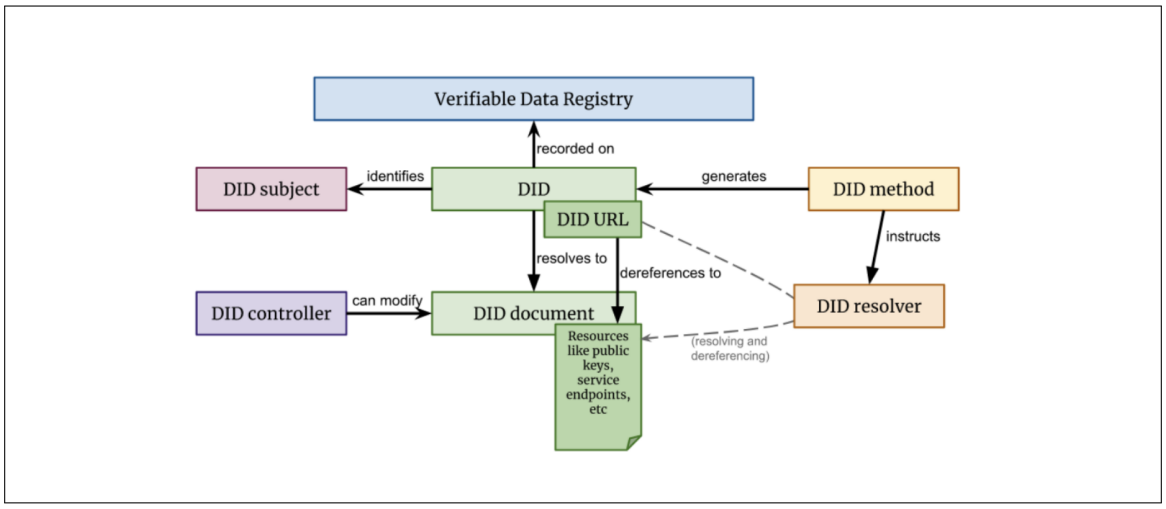

Figure 3.8: Components of the DID architecture [11]

3.2.2 Verifiable Credential

A credential is defined as *a set of one or more claims by the same entity* [8]. The components of a credential can include an identifier, and metadata that describe the properties of the credential, as displayed in Figure 3.9. Metadata include information about the issuer, expiry date, public key for verification, revocation mechanisms and representative image [8].

Verifiable credentials on the web represent the same information that a physical credential presents, and allows you to express these credentials in such a way that is cryptographically secure, privacy respecting and machine-readable [9]. A credential might consist of information that relates to identifying the subject of the credential, information related to the issuing authority, information related to the type of credential, constraints of it as well as information related to specific attributes or properties being asserted by the issuing authority about the subject, the credential represents [9]. It is a set of tamper-evident claims and metadata that cryptographically proofs who issued it [8].

The World Wide Web Consortium presents a data model which attempts to improve the ease of presenting digital credentials, in order to establish trust through digital interfaces. The holders of verifiable credentials can generate verifiable presentations, and share these with verifiers to prove possession of the credential [9].

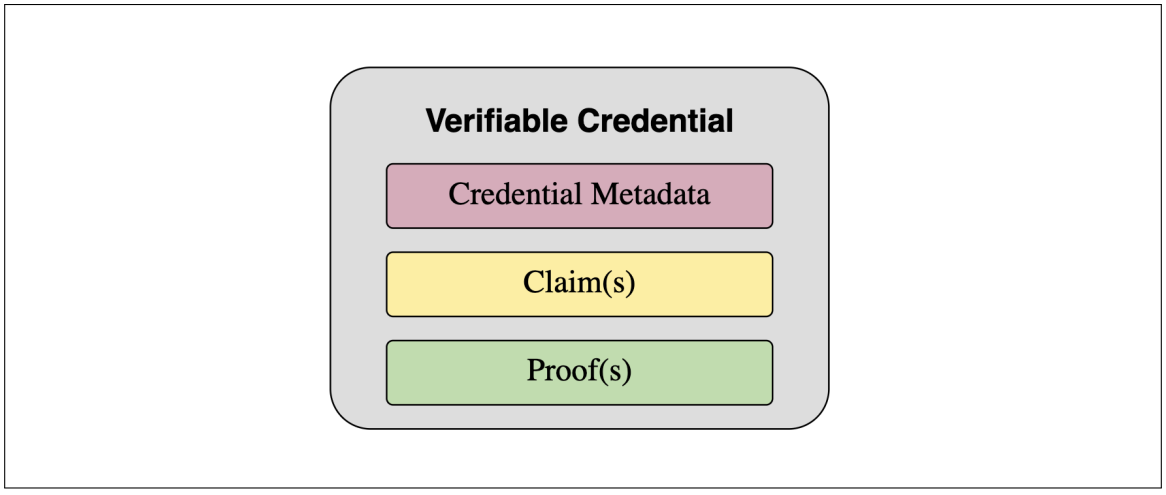

Figure 3.9: Components of a verifiable credential [8]

3.2.3 Verifiable Credential Presentation

The DIDs act as a unique identifier for VCs, and creates a secure connection for data exchange between the Issuer, Holder and Verifier of credentials. The verifiable data registry can utilise a distributed ledger for storing Public DIDs belonging to the organization that issued a credential [68]. The Verifier can then verify the validity of an attestation to a credential and its attesting party, by validating the signature of the attesting party. This way, VCs can establish trust between parties by guaranteeing authenticity of data and attestations without storing personal data on the ledger. A distributed ledger is immutable, and can never be altered or deleted [68].

Verifiable presentation is the process of presenting a compilation of verifiable credentials composed by the holder of the verifiable credentials. Such a presentation is tamper-evident, encoded in such a way that the issuance of the data is trusted after cryptographically verified [9]. Verifiable presentations can either disclose attributes of the verifiable credential, or satisfy derived predicates, such as greater than, less than equal to requested by the verifier [9]. This functionality allows a user to only express a subset of their digital identity that is appropriate in a specific situation, in order to enhance privacy [68].

A verifiable presentation is composed on minimum four information graphs, respectively the presentation graph, which contains the verifiable presentation itself along with a self contained credential graph containing claims and an associated credential proof graph which express the proof of the credentials, usually a digital signature [8]. The fourth information graph is the presentation proof graph, which express the proof of the presentation, usually a digital signature [8].

3.2.4 Ecosystem

The ecosystem of verifiable credentials consists of a number of core actors, respectively the holder, the issuer, the subject, the verifier and the verifiable data registry.

The role of the *Holder* of a verifiable credential is to acquire, store and generate verifiable presentations of the credential, that is issued by and *Issuer*. The role of the Issuer is assert

claims about a subject, create a verifiable credential and transmit this the the *Holder*. The *Holder* stores the credentials in a mobile wallet on their mobile device, so that no Personal Identifiable Information is stored in a centralized registry, such as a dedicated server or in the cloud [68]. The *Subject* is the entity about which the claims are made, and includes human beings, animals and thing. In most cases the *Holder* of a verifiable credential is the *Subject* [9]. The *Verifier* is presented with the verifiable credential, which digital signatures it checks against verifiable data registry [9]. The role of the verifiable data registry is to mediate the creation and verification of identifiers, keys, issuer public keys and verifiable credentials schemes. Such a registry include trusted databases, decentralized databases and distributed ledgers [9]. Figure 3.10 illustrates the information flow between the actors in the use of verifiable credentials.

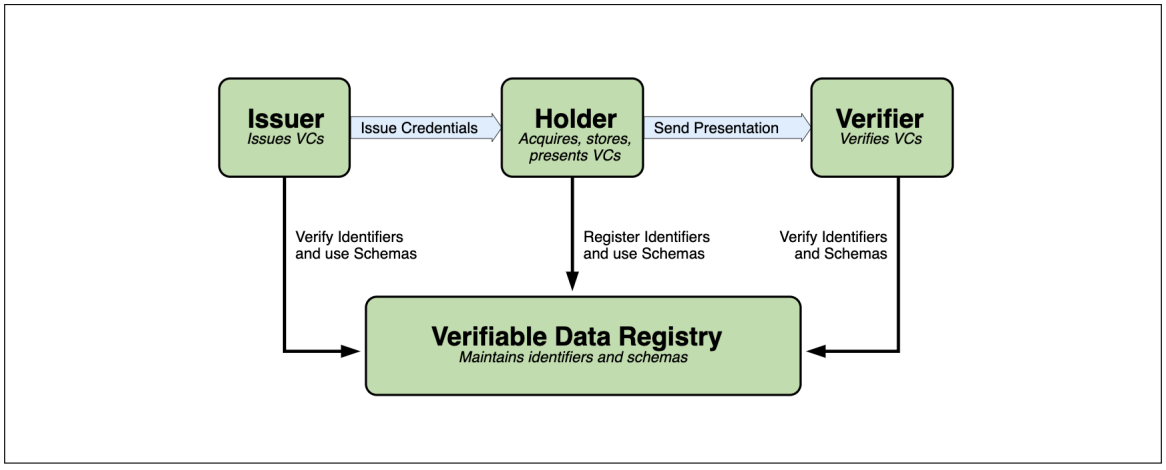

Figure 3.10: Information flow in the use of verifiable credentials [9]

3.3 Summary

The Digital Identity chapter introduces the concept of digital identities and how it relates to individuals when utilising online services. The establishment of a digital identity is presented, and how claims and assertions is used to establish trust.

The structure of Digital Identity Management Systems is presented, and how this has evolved with the increased digitisation from centralized identity management to federated models. The ecosystem of MitID and the authentication process is presented, as MitID serves the purpose of providing the digital identities for access to public services and online banking in Denmark.

The demand for digital identities and associated privacy online is addressed by the EU initiative eIDAS 2.0, which aims to enhance trust by providing the condition under which member states must recognise means of digital identification of natural and legal individuals.

Following eIDAS 2.0, the EU has presented recommendations for a European Digital Identity Framework, which constitute a central element in the development of a European Union Digital Identity Wallet. This shifts trust from the centralized systems controlled by identity providers to decentralized systems, respectively Self-Sovereign Identity management, resulting in more transparency, privacy and control for users when presenting identity information online.

The ecosystem of SSI along with the technological frameworks it consists of, respectively decentralized identifiers, verifiable credentials, verifiable data registry and data wallet is elaborated upon.

Chapter 4

Financial Sector

The following sector presents the financial sector ecosystem, and its payment processing landscape, followed by the EU initiative of the Revised Payment Service Directive, and the technological frameworks Financial-grade APIs which supports the novel trust relationships within the sector for payment initiation.

4.1 Ecosystem

The financial sector is made up of institutions and firms that provide financial services to both retail and commercial customers. Traditional banking provides one-on-one customer service, and primary functions that include essential money management, such as opening bank accounts, issue credit cards, handle payments and granting loans [47] [17].

Financial institutions provide several types of services, which covers the areas of private banking, business banking, loans and digital banking. The branch of private banking offers services for the purpose of assisting individuals in managing finances, such as bank accounts and credit cards, which enables the customers to initiate payment transactions [17]. Digital banking is concerned with enabling customers to manage finances online through digital interfaces, such as mobile applications and dedicated websites. The services digital banking provides are the ability to access a bank account and oversee the financial account move-

ments as well as making transfers directly from a bank account to another [17]. Both these service categories presuppose a direct relationship with the banking institution. Consumers can access account details through a dedicated mobile application or website made available by the individual banking institution. The banks and their customers have a direct relationship, where associated data is available through the closed ecosystem of the individual banking institution. Customers must therefore login to a mobile application or website of each individual bank to which they are customers, if they are customers are several banking institutions [17] [47].

Payment services and systems are fundamental to ensure an effective, functioning financial ecosystem. The main payment service utilizing within the European area, is card payments, which accounted for 47 pct of all non-cash retail payments in 2020. Credit transfers accounted for 23 pct, while direct debit account for 22 pct [18].

4.1.1 Payment Landscape

The payment ecosystem consists of a combination of several entities interacting with each other during payment transaction processing. The Issuing Bank, the credit card networks, the acquiring bank, the payment processor, payment gateways [24].

The Issuing Bank is the bank of the customer that holds the customer's banking account, and issues credit and debit cards to customers on behalf of the credit card networks. These banking institutions issues payments to the merchant's, the acquiring bank, on behalf of their customers, assuming the risk associated with issuing credit cards [24]. They are responsible for ensuring that a cardholder has enough funds to cover a transaction, and to ensure customer authentication in order to authorize a payment process [34].

Acquirers are banks or financial institutions that enables a merchant to accept credit card payments from customer's Issuer bank within a credit card network. They handle the processing of debit and credit card payments on behalf of a merchant, and assumes the associated risk of such processing. The acquirer passes a merchant's transaction information to the credit card network and issuer bank for completing payments [24].

Payment processors provide payment processing services to merchants, and may be associated with acquiring banks [24]. They hold responsibility for establishing merchant accounts, for accepting and processing card payments, managing card processing and implement anti-fraud measures. Front-end processors route transactions from the merchant to the cardholder's issuer bank for requesting authorization, whereas the bank-end processors accept settlements from front-end processors, and move payments to the issuer bank of the merchant [24].

The credit card networks, such as Visa and Mastercard, facilitate transactions among consumers, merchants, processors and card issuer banks [24] by providing the electronic network infrastructure for processing transactions [24]. They charge fees to the acquiring and issuer financial institution [75], and oversee payment processing activity [24].

Payment gateways are applications that enable merchants to accept card payments for in-store and online transactions. The payment gateway encrypts payment information and handles the data transfer among the merchant and the payment processor. Gateways operate either digitally or embedded within an in-store POS system as displayed in Figure 4.1 [24].

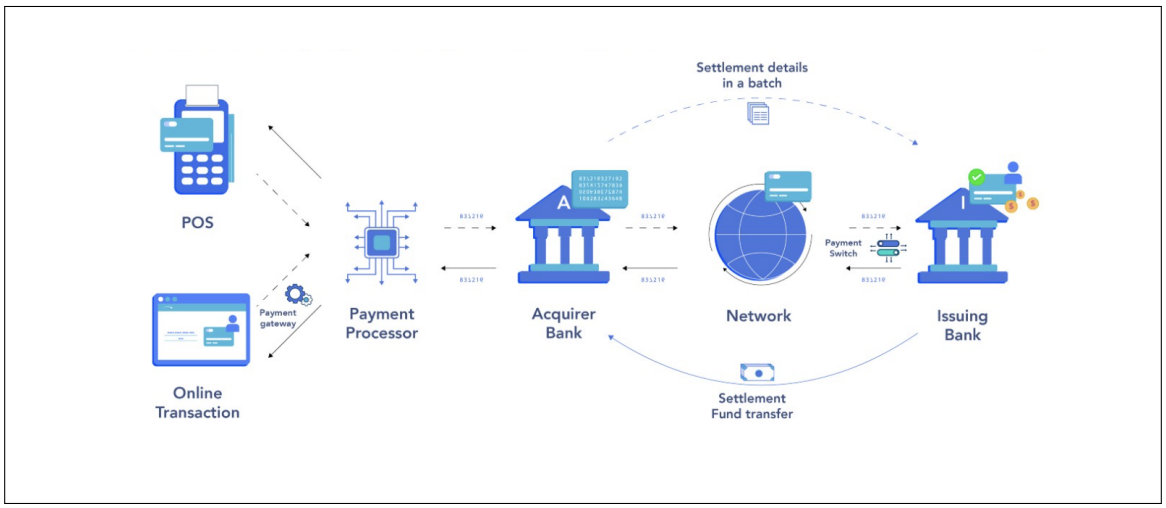

Figure 4.1: Traditional data flow for credit card processing [46]

Payment Processing Cycle

The processing cycle of credit card payments is complex, and involves the entities presented in section 4.1.1. Credit card transactions occur in a two-stage process consisting of the authorization process followed by the settlement and funding process [33].
The entities engaged in payment transactions have a trust relation, as they are all subject to compliance regulations. The business model of the processor, acquirer and the card network is dependent on interchanges fee charged for assuming the risk associated with processing credit card transactions [24].

Retail payment transactions refer to business-to-consumer (B2C) transactions, and are subject to level one credit card processing. The process of obtaining and approved transaction is displayed in Figure 5.2, and elaborated upon in the following section. The authorization request includes merchant name, date of transaction, payment amount, credit card number, expiration date, billing address and card security code (CVV) [24].

The obligation of banking institutions is to ensure identification and authentication of individuals requesting approval of a payment transactions [45]. The entities of the ecosystem has an established trust relation with the issuer banks, and it is this entity that is liable for authorizing transactions [24] [45], and by that identification and authentication. The banks therefore protects the sensitive PID that is necessary for reliable identification, described in chapter 3, because there is a trust relationship.

Credit Card Transaction Authorization

In order to initiate a payment transaction as displayed in the sequence diagram in Figure 4.2, the merchant requests personal identifiable information to reduce the risk of credit card fraud and to increase the trust in the card holder, respectively the credit card number, the name on the credit card, the card verification value (CVV), the full address and zip code of the card holder [67]. The purpose of providing this information is for the merchant to request address verification (AVS) to increase the trust in the identity of the card holder when the card is not present [24] [67].

AVS is a numeric address verification system that matches the customer information with the information associated with the card holder by the card issuer [67]. A merchant can request an AVS check on a transaction, by requesting the payment gateway to transmit the numeric address data to the customer's credit card network. The credit card network forwards this request to the issuer, which compares the received numeric address to the address numbers associated with the customer profile in the banking institution. The issuer responds with an authorization status as displayed in Figure 4.2, and the associated AVS response code to the payment gateway of the merchant [67].

The issuer bank has a trust relationship with the credit card network, as the issuer bank issues credit cards on behalf of the network to customers. The issuer bank act as an intermediary between a card holder and the card network, and is responsible for ensuring substantial LoA for authentication of card holders when a credit card is used for an online payment transaction, as displayed in Figure 4.2 [24] [67].

The issuer bank holds substantial amount of PID on their customers, as they by law are required to in order to ensure identification and authentication of customers to authorize payment transactions. The trust relationship established among the banking institution and its customer enables the bank to hold and process PID that relates to a customer banking account, such as full name, address, social security number, number of payment cards, bank accounts and card usage, employment status and financial history [47] [34] [67].

In order to authorize a payment transaction, the issuer bank request multi-factor authentication from the customer. The eID issued for Danish citizens is MitID, as presented in section 3.1.1. MitID provides identification and authentication of customers as identity information issued by the government is verified during registration of the eID [36]. MitID ensures the substantial LoA [66] as required under eIDAS 2.0 presented in section 3.1.2. The substantial LoA ensures strong authentication of individuals by combining multiple means of authentication, respectively user ID, password, proving access to the MitID smartphone app and associated biometrics. The substantial LoA provides low and minimal risk level in identification and authentication scenarios [52] [**eidasbrief**].

The sequence diagram displayed in Figure 4.2 illustrates the high level process of credit card transaction authorization through a website [24] [45]:

1. The card holder initiates a purchase from a merchant by entering their card details, including card number, expiration date and CVV/CVC code. Once card details have been entered successfully, the pull payment is triggered

2. The transaction request is passed on to the payment gateway, that forwards the payment authorization request to the merchant's payment processor.

3. The payment processor forwards the transaction request to the acquirer, which captures the transaction and validates the payment in question

4. When approved, the Acquirer passes the transaction request to the credit card network of the card holder

5. The credit card network analyses risk attributes such as type of transaction, geo-location in relation to the card holder's phone, spending history of the card holder and whether the payment transaction is taking place under unusual circumstances. The credit card network scheme calculates a risk score based on a high number of data points. Credit card use tokenization to protect communication, where the credit card number is only referenced by a token, such as the last four digits on the number

6. The credit card network routes the transaction to the issuer to have the payment transaction approved by the card holder's bank

7. The issuer bank receives the transaction request and requests 2FA authentication by the card holder

8. The card holder authenticates with the bank

9. The issuer bank place hold on funds for payment and approves the transaction, and sends it responds along with an authorization code to the credit card network

10. The credit card network send the approval to the merchant's payment processor, that forwards it to the acquirer bank.

11. The acquirer routes the approval code to the merchant, which sends a payment completed response to the card holder

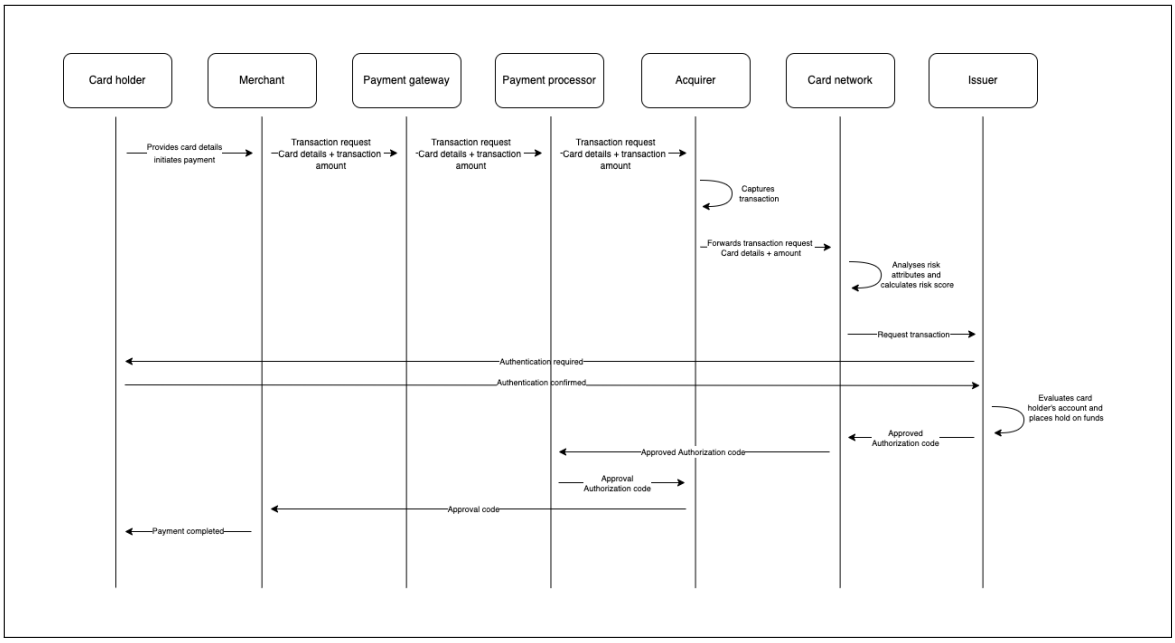

Figure 4.2: Credit card authorization processing cycle [24]

Settlement and Funding Process

The merchant receives payment from the credit cards it accepts based on the settlement and funding process. This process is initiated by the merchant that sends batches of authorized transactions to their payment processor daily [69]. The payment processor forwards the transaction details for authorized payments to the acquirer, which reconciles the batch of authorized transactions to the card network for settlement [69]. The credit card network requests each approved transaction to the appropriate issuer bank of the card holder, which charges the card holder's account and transfers the requested funds through the same channel, as displayed in Figure 4.2 and Figure 4.3 [67]. The issuer bank charges an interchange

fee, which is shared with the credit card network. The processor and the acquirer and collects a fee as well before the discounted funds are send to the merchant account with the acquirer [69]. The issuer bank then transfers the funds for the transaction to the merchant bank, and issues an interchange fee for handling this process. The merchant bank then deposits the funds into the merchant account [67] [69].

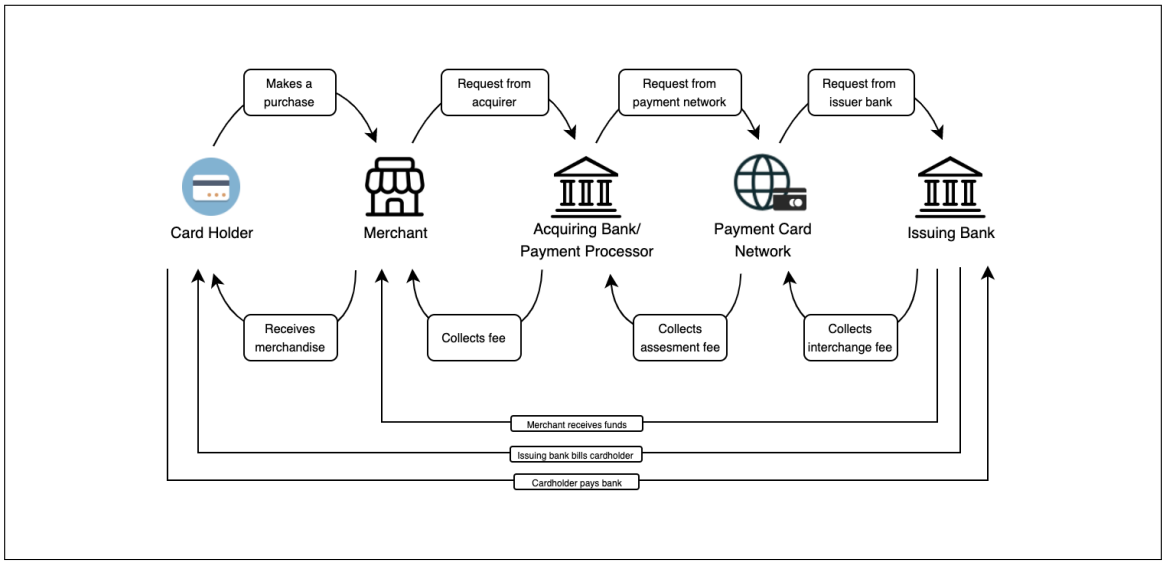

Figure 4.3: Data flow for settlement and funding process [23]

4.1.2 Payment Service Directive 2

The Payment Service (PSD2) - Directive (EU) 2015/2366 is a revised version of the directive on EU-wide payment services. It was put forward by the European Parliament and went info force on 14 September 2019 [58].

PSD2 aims to make payments safer, increase customer protection, foster innovation and competition by making it easier for novel market entrants to compete in the financial service industry [54]. The directive builds upon the current financial service system, and helps creating an interconnected ecosystem within the industry [47]. Traditional banks are encouraged to become data conscious, as the financial data of users can not solely exist in closed systems

and on proprietary networks [47] [73].

The aim of the directive is to provide a legal foundation for further development of a better internal market for electronic payments across EU borders, by establishing regulations for third party services providers, account information service providers (AISP) and payment initiation service providers (PISP) respectively [58]. It opens up the account aggregation and payment markets to new entrants to foster innovation and competition leading to greater choice for consumers, as incumbent financial institutions are legally obliged to provide third party service providers access to user data to mitigate the use of insecure methods for aggregating data, such as screen scraping [5]. The purpose of putting forward the PSD2 is to promote trust in third party service providers to foster innovation and competition [58].
The directive applies to existing and new providers of innovative payment services to ensure that incumbent institutions and innovative service providers can compete on equal terms. To do so, the directive establishes clear, and comprehensive rules, that seeks to increase consumer trust by assuring greater transparency, choice and efficiency in payment services across EU member states [58].

The key points that the regulation is concerned with, are payment institutions, including AISPs and PISPs. This new paradigm is denoted open banking [59]. The transparency of conditions and information requirements for payment services, the rights and obligations of users and providers of payment services, as well as strict security requirements for both consumers' financial data and electronic payments [58]. It opens up the EU market to companies that offers consumer- or business oriented payment services [59] [58]. The payment initiation service providers (PISP) enables a user to make payment requests through a payment service provider to a payment account held at another payment service provider [58]. Account information service providers (AISP) which allow a payment service user to access an overview of their financial situation through a third party application, and by that allows users to better manage their personal finances [58].

Along with opening up markets to new service providers, consumer rights are being enhanced by this directive. The liability for non-authorised payments are reduced from €150 to €50, unconditional refund rights for direct debits within eight weeks, and the removal

of subcharges for the usage of credit and debit cards for consumer [58]. In continuation of this directive, the European Banking Authority (EBA) is strengthened, to develop a publicly accessible central register of authorised payment institutions, assist in resolving potential disputes between national authorities as well as develop regulatory technical standards (RTS) for compliance [58]. Figure 4.4 displayed the role of the institutions outlined in PSD2 [65] [58].

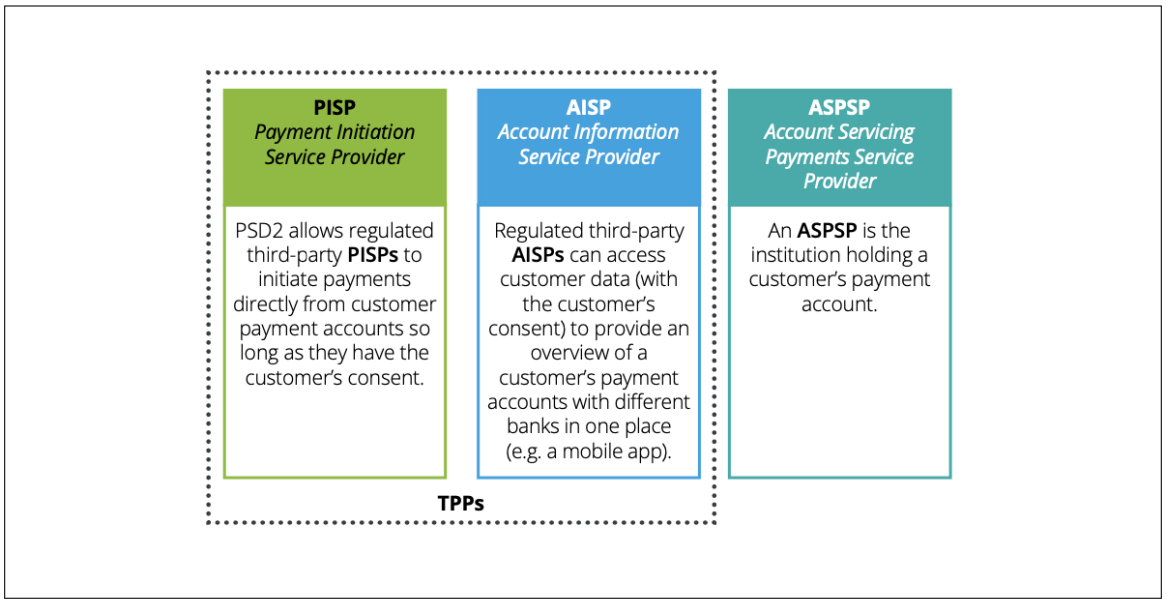

Figure 4.4: Institutions outlined in PSD2 [65]

Regulatory Technical Standards

Regulatory technical standards (RTS) are technical compliance standards, which specify particular aspects of a legalisation. The purpose of the RTS is to ensure consistency in the technical implementation within specific areas [70]. A regulatory technical standard is a delegated technical act submitted by a European Supervisory Authority [70]. The aim of such a standard is to provide a detailed specification on how to achieve the security requirements as stated in PSD2. The RTS state that A TPSP must obtain the digital certificates, Qualified Certificate for Website Authentication (QWAC), and Qualified Certificate for Electronic Seals certificate, issued by an eIDAS Qualified Trust Service Provider [57].

Furthermore, the RTS require Strong Customer Authentication (SCA), confidentiality and integrity of user credentials and open and secure communication channels. These requirements are put forward to provide a secure environment for payment processing and for preventing financial fraud [57].

To ensure SCA, the adoption of certain security elements of eIDAS is required, along with two-factor authentication (2FA), which consists of minimum a combination of two of the following elements based on the level of risk. Each element has to be independent of the other to mitigate the risk of fraud or exploitation, if one is compromised [57].

Factor	Description	Example
Knowledge	Something the user knows	PIN code, password
Possession	Something the user possesses	Card, mobile app, token
Inherence	Something the user is	Biometric identifiers; facial recognition, fingerprint

To ensure the application of SCA, it is necessary to apply adequate security features, such as length or complexity for the elements categorised as *knowledge* [70] [57].
Further more, general authentication requirements, which addresses the need for analytical capabilities within authorization sever, such as monitoring mechanisms that detect unauthorised or fraudulent payment transactions are required [58] [60]. The risk-based factors it must take into account are compromised or stole authentication elements, the amount of each transaction, known fraud scenarios and signs of malware associated with the authentication process [58] [70] [60].

Authentication code generated based on two or more elements shall be accepted by the PSP when an action is carried out through a remote channel, which may inherently imply risk [60]. SCA is exempted when the payer initiates a series of payment transactions to the same receiver, and when the amount of a payment transaction does not exceed 30€. ASPSPs shall ensure that the dedicated APIs that exposes user data uses ISO 20022 definitions for financial messaging [58]. Figure 4.5 illustrates how the adoption of PSD2 changes the customer-bank relationship [60].

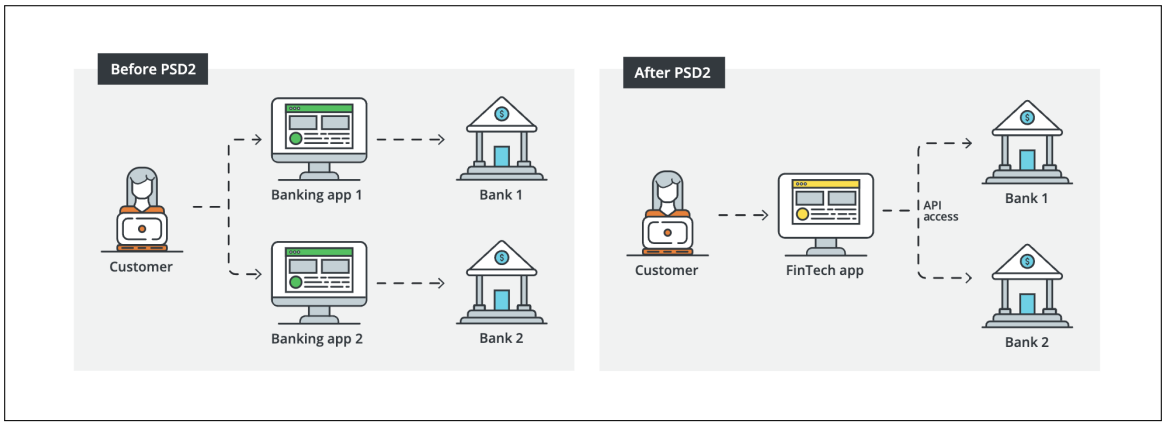

Figure 4.5: Before and After PSD2 [60]

4.2 Financial-grade APIs

Application programming interfaces (API) are sets of protocols and definitions for integrating intermediary software, that allows two applications to interact. The OpenID Financial-grade API (FAPI) is a technical specification developed by the Financial-grade API Working Group of the OpenID Foundation [41] [50]. It is built upon OAuth 2.0 for API authorization and OpenID Connect (OIDC) for user authentication. The specification defines additional technical requirements for industries, that require higher security for interacting with third party applications, such and the financial industry and the health care sector [41]. As such, FAPI is concerned with upgrading the OAuth2 infrastructure, as FAPI acts as part of the trust

architecture among the entities [41][60]. The goal of the FAPI specification is to provide JSON data schemas, security and privacy recommendations to enable applications to interact with a financial account, utilise data stored in a financial account as well as enable users to control security and privacy settings [4]. Figure 4.6 illustrates the interactions of the customer accessing a PISP or AISP for requesting a service. The customer is redirected to its banking institution for authentication. When accepted, the bank sends the PISP or AISP a token. The third party provider replies with the SSA certificate, introduced in section 4.1.2. The transaction is approved, and the service provider can proceed requested service [5].

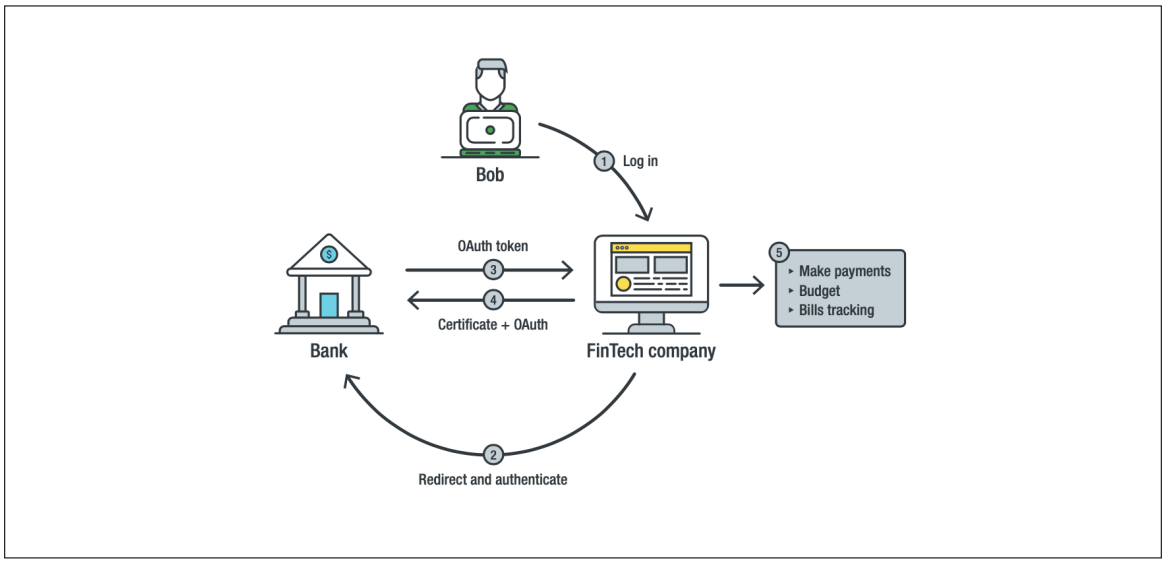

Figure 4.6: FAPI in Open Banking scenario [5]

4.2.1 OAuth 2.0

FAPI is based on the OAuth 2 authorization framework and OpenID Connect as its base. OAuth enables third-party applications to obtains limited access to an HTTP service [39], and defines four roles, the resource owner, resource server, client and authorization server. Figure 4.7. illustrates the interactions between the four roles, respectively client, resource owner, authorization server and resource server. [39].

The client initiates the interaction **(*A*)** by requesting authorization from the resource owner, either directly through the resource server or indirectly through the authorization server. The client receives an authorization grant **(*B*)** from the resource owner, which is a credential that represents the authorization of the resource owner[39].

The client requests an access token **(*C*)** at the authorization server, by authenticating with this entity and presenting the received authorization grant. The authorization server now authentications the client **(*D*)**, validates the authorization grant and issues an access token. The client presents the access token **(*E*)** for authenticating, in order to request access to a protected resource from the resource server. The resource server validates the presented access token **(*D*)**, and allows the client access if the token is valid [39].

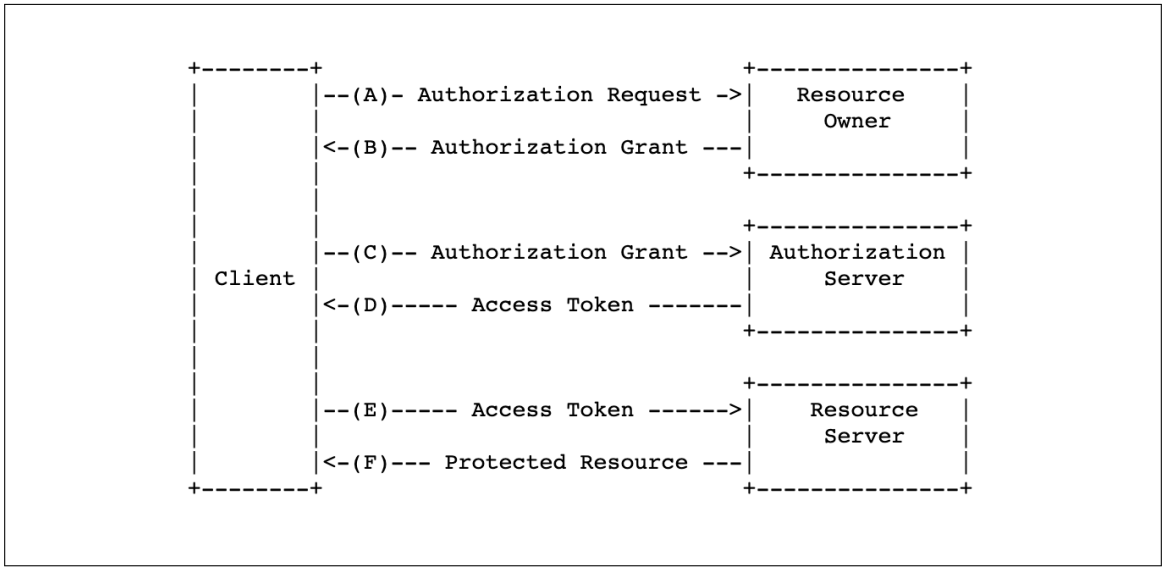

Figure 4.7: OAuth 2 abstract protocol flow [39]

4.2.2 FAPI 2.0

FAPI 2.0 defines a broad scope, and aims for complete interoperability at the interface between client and authorization server, and interoperable security mechanisms at the interface between client and resource server [41].

It is currently under development, and builds upon the OAuth 2 protocol illustrated in Figure 4.7. FAPI aims to provide a higher degree of security [3] by providing a specific implementation guideline for online financial services, by developing a data model protected by a highly secured OAuth profile [40]. The framework defines the two compliance levels aligned with different protection levels, baseline and advanced respectively, for the API access modes, read and read-write profiles [50]. The read profile is reserved for the AISP, and the read-write profile is reserved for PISP, as defined in section 4.1.2 under the PSD2 [50] [58]. In order to achieve this higher level of security, the FAPI security profiles incorporates security extensions for OAuth2 to make it secure in high risk scenarios [5] and mechanisms defined in OpenID Connect [3].

The security profiles applies to online services, and prevent client impersonation through client authentication with mutual TLS (mTLS). mTLS ensures mutual, two-way authentication for two parties authenticating each other [40]. It ensures an encrypted connection using HTTPS, as a client application is required to present a PKI client certificate in a TLS connection when accessing a token endpoint upon an authentication request. The authorization server uses the client application certificate for client authentication [40] [5]. FAPI 2.0 also supports self-signed client certificates, which must be pre-registered with the authorization server in advance [40].

It defines new values for the response mode request parameters through JWT Secured Authorization Response Mode (JARM), which enables authorization response parameters to be returned as the value of a single response parameter in a singed JWT [40].

Proof of Key Code Exchange (PKCE) was initially created for OAuth public clients with a goal of protecting against the use of intercepted authorization codes. It works by introducing a code verifier, which is a random value created by the client [3]. The client creates a code

challenge by hashing this verifier, and includes this challenge in the authorization request. The challenge is now associated with the generated authorization code, so that the client requests the authorization code at the token endpoint, the code verifier is included within the request [3]. The message cannot be intercepted, as it is sent directly to the authorization server protected by TLS. If the authorization code is exposed to a malicious party, this party cannot redeem the code to obtain the access token, as the code verifier is not know [3].

JWS Client Assertions handles the process of binding an authorization code to a certain confidential client, so that only this client can redeem the code at the authorization server. This is achieved by requiring prove possession of a key [5]. Rich Authorization Requests (RAR) tie authorization information to an access token, by enabling an access token to hold detailed information about payment such as "How much?" and "To whom" [40].

4.3 Summary

The Financial Sector chapter presents the financial sector and its associated payment landscape. The entities that constitute the ecosystem is presented along with their role associated with the credit card transaction payment process. The EU promotes opening up these established ecosystems for initiating payment transactions by adopting the Revised Payment Service Directive (PSD2), presented in section 4.1.2.

The purpose of enforcing the PSD2 is to infuse trust into third party service providers, respectively AISP and PISP, within the financial sector, in order to lower the barriers for competition for the benefit of users. In order to establish trust, the sector is subject to security requirements in providing strong customer authentication and obtaining digital certificates. The Financial-grade API specification addresses secure data exchange in the inherent high risk scenarios that includes the information exchange of PID associated with banking.

Changing traditional ecosystem creates new opportunities for utilizing technology for realising new scenarios. The technological frameworks presented are further utilized for realising these new scenarios that are made possible through legislation, while addressing the trust challenges apparent today.

Chapter 5

Analysis

The purpose of the following chapter is to gather requirements for deployment proposals, and to gain a deeper in-sight into the domain of digital trust, privacy, identity management systems and the financial sector. The chapter analyses the context of digital trust, and the combined parameters that ensures digital trust. Furthermore, it discusses the key points broad forward by the expert interviewees.

5.1 Digital Trust

The Internet as we know it today has transformed the way people, business and governments interact and operates. It has accelerated the digitalization, which has increased the amount of data that can be collected and processed [42]. Personal data related to online activities and behavior are transformed into information and realised as a new form of value, as online interactions are an integral part of people's daily lives [42].

The World Bank estimates that the global internet traffic reaches 150,000 GB per second by 2022, and personal data are expected to represent a significant share of the total volume of data transferred [19], which further increases amounts of data that are captured, and subsequently utilized by third party data collectors [42]. The knowledge of these mechanisms and lack of transparency, choice and control of how personal data is being used from the data owner, minimizes trust [49]. A shift in focus in how trust is established, has shifted from

security to privacy to sovereignty. Digital literacy, and the widespread hereof, has increased the demand for ownership and control of digital assets in order to exercise self-determination of digital identities [42].

Trust will be increased if governments and legislative bodies enforces policies and standardized protocols for data protection and privacy, which will entail improvements in the Internet. The derived effects of these interventions, will increase trust [42] [49].

Trust is defined as the confident relationship with the unknown [49]. Digital trust expands this concept to apply within the digital realm, where *the confidence users have in the ability of people, technology and processes to create a digital secure world* [63] is apparent.

The Internet was not designed to address trust issues, nor to protect data privacy, but to facilitate information sharing [10]. Utilizing technology for the purpose of misusing personal data, inappropriate surveillance and lack of transparency weakens the overall trust in how business, organisations and industries use technology responsibly [10].

Todays' digital economy requires individuals and firms to share data with third parties at an unprecedented scale, without providing ways to control how data is used by default [22]. Sharing data is necessary for engaging with digital services in order a service provider to verify attributes of a customer. This often involves sharing personal or confidential information to a large extent, and allow service providers to gain access to sensitive information [22]. This increases the risk of data breaches, which constitutes the greatest cause of distrust in digital services [49].

The demand for digital trust is creating a digital transformation, which encourages companies and legislators to place more significance on secure processes, to ensure privacy, security, reliability and ethical data handling. The success of businesses that operates digitally is impacted on trust, as users and companies are more likely to make use of trustworthy services, due to the increasing amount of personal data that are shared with different service providers online. The lack of security and transparency increases distrust in digital technology [49]. The global economy relies on digital trust due to the increasing interconnectivity across borders and sectors. There are no established requirements for creating digital trust through standardisation and protocols.

Trust is the most central aspects of the relationship between a financial service providers and their customers [55]. The majority of financial institutions have spent decades building trust with its customers. Open banking entails data sharing of sensitive consumer data, which mandates a need for stronger authentication mechanisms for building trust in assuring the identity of individuals [55].

Banks need to take strong measures in order to increase digital trust through trust mechanisms, which ensures strong security and data protection for sharing financial data. Banking service offerings become more digitized, the demand for digital trust affects the financial sector, as data security dominates digital finance concerns from consumers [55]. 82 pct of global consumers have concerns about using digital financial services, which indicates that the financial sector need to build further trust and reassurance in digital products provided [55]. The top concerns related to third party financial services providers relate to data safety and security. 43 pct of global consumers are concerned about an increased risk from hackers. The same proportion, 43 pct, are concerned about identity theft [55].

The Edelman 2021 Trust Barometer survey shows that 68 pct of its respondents globally, trusts that technology businesses will do the right thing. This number declines to 52 pct, when financial services are considered [62].

Building digital trust is crucial for businesses pursuing digital transformation efforts for integrating technology into every aspect of their operations, with the intent of increasing consumer interaction, growth and revenue. Asking customers to trust businesses in new ways with personal information as well as behavior information, create new demands for using digital technology to build trust [10]. Novel technology framework ensuring privacy-by-design can be utilized for building trust by enhancing transparency, reinforce ethical and responsible practices, boost data privacy and strengthen security activities [10] [49].

Transparency and accessibility comprises the first aspect of building trust. It considers transparency in business practises, such as how personal data is collected, stored and processed, how the business model operates, and the disclosure of information, such as privacy policies and terms of service [10].

The second aspect considers ethics and responsibility, and comprises the responsibility

of organisations to work towards the welfare of customers when developing technologies, as technological innovations that gives organisations more power raises ethical questions [10]. Technological innovations that promotes welfare will generate higher credibility and trust, as technology is only as ethical as it is designed to be [10].

Privacy and control constitutes the third aspect, which encourages companies to deploy technologies for safe and secure sharing of personal data [10]. For long, personal data has been traded for access, convenience, and a personalized experience when engaging with digital service [10]. The most apparent policy issue within the digital realm today, considers social networks, which are accused of misusing people's personal data for corporate gain, advertisers and larger technology firms that displays ads are accused of tracking their users without their knowledge, and a variety of firms are accused of using collected data for unrelated purposes without consent [22]. The data that firms have collected legitimately might often be stored and processed without sufficient strong controls, which might lead to data loss, exposure and potentially malicious abuse [22].

The problem with data sharing, is the perception of loss control and privacy, due to lack of transparency in data processing and how far-reaching consent is. Allowing users to control their personal data, and minimizing the disclosure of data when engaging with third party service providers [10].

Security and reliability denotes the fourth aspect, which can be build by verifying the identity of people claiming to be customers or service providers, in order to mitigate impersonation and fraud [10]. Digital biometrics and multifactor authentication helps identifying customers based on behavior to ensure a frictionless experience [10]. Collecting data about behavior and digital gestures for the purpose of building trust, raises further questions about user data privacy [10]. According to Okta's Trust Index, security is an important aspect of digital trust, and secure log-in options such as multi-factor authentication infuses trust with consumers [49].

Transparency, security and privacy are key aspects for rebuilding digital trust. Users need to trust stakeholders within ecosystems, which requires an individual to control what information that can be communicated to others. Combining these aspects will satisfy the

necessary conditions which needs to be present for trust to emerge in today's digital realm [65] [49].

More trust makes thing possible, as stakeholders can be trusted and verified by all parties. In order to build trust in a digital realm, all parties must be verified, and users must be able to verify themselves in such a way that does not sacrifice either privacy or usability and convenience [42]. Trust frameworks are mechanisms for building trust online, by defining policies, technical specifications and requirements that needs to be met in order to ensure privacy, security and identity management and interoperability. Utilizing better trust frameworks is a driver for innovation and new business possibilities [42].

Digital trust is established through such trust frameworks, which are responsible for ensuring identification and authentication of the entity in question. Digital identities is a core component of trust frameworks as presented in chapter 3, and necessary for putting access control policies in place, identify where data is stored and for establishing trust between parties [42].

The digital identity market is powered by the financial service industry, and this tendency is amplified by the increasing digitization of transactions and account access. The financial sector is highly reliant on consumer trust, which drives the incentives for investments in the development in digital identity management systems [37]. According to a Eurobarometer survey, 72 pct of users want to know how their data is handled and processed when using social media accounts, and 63 pct want a single digital ID for all online services [26].

In today's digital world, centralized identifiers are rented by IdPs, and can therefore solely be used based on the terms defined by the IdP, as presented in section 3.1. The user of an identity system is provided with a proof of authenticity of their digital identity, through a token linked to their identity record at the IdP. This token can then be used to login to a service provider, or relying party, which trusts the identification and authentication provided by the IdP, as displayed in Figure 3.2 [37] [26].

5.2 Interviews

In order to investigate digital trust in institutions and the role of data privacy, three expert interviews have been conducted with respondents from different actors of the ecosystem. The professional background of the interviewees define their approach towards the area of digital trust and data privacy. To investigate the area from different perspectives, and to gain a deeper insight into the domain, a respondent from the organisation D-Mærket, the Danish Digitization Agency as well as a respondent with a background in financial services, have been interviewed. The interviews have been semi-structured, and the questions asked are based on the interview guide found in Appendix A.

5.2.1 Lead Auditor, D-mærket

The first interview was conducted with Emil who is Lead Auditor at the Danish organisation D-mærket, which operates under the Danish Industry business organization and certifies companies in it-security and responsible data handling. D-Mærket is a part of the private sector, and serves as a trusted verifier of companies in order to establish digital trust with consumers [21]. Companies use this certification to ensure partners and customers that they exhibit digital accountability, in order for them to be trusted. The purpose of D-Mærket is to provide business value to the company in terms of digital trust, for both business partners and customers, which helps in creating a stronger digital Denmark [21].

The purpose of this interview was to gain an insight into the role of trust and data privacy of consumers, and therefore a commercial parameter for companies today.

The company is experiencing great interest from various SMEs in Denmark for this certification. This interest stems in a lack of trust, from the perspectives of consumers as well as stakeholders and business partners. Legislation is not enough, the companies need to establish digital trust in other ways to gain a competitive advantage, and to keep up with the currents of time in society today.

The GDPR followed by the Cookie Directive adopted by the EU have helped, and put

movements in motion in right direction, as awareness and accountability have increased for both consumers and companies. This statement emphasizes the role governmental entities and legislative bodies in creating an insight and knowledge base at the consumers, which will foster a demand transparent and responsible data handling.

According to the interviewee, there is still room for improvements within the realm of privacy, transparency and increased accountability. *In most cases, it is still cumbersome to oversee and discern the amounts of data collected, and the purpose for the collection and processing of it.* It is difficult for consumers to evaluate how far reaching consent is, when it has been provided.

From his point of view, a number of companies and firms are still putting own interests ahead of consumers, where they should place greater emphasis on consumer privacy.

The expectation is that novel legislation which aims to strengthen data privacy and thereby lead to better data protection, will increase the knowledge and the demand from, first and foremost, the consumers. They identify an increased demand from consumers in relation to privacy and responsible data handling, which companies have to act accordingly upon. This puts further incentives and pressure on working responsibly with data handling, and being able to communicate this to their consumers in a transparent way.

5.2.2 Lead Architect MitID, The Danish Digitization Agency

The second interview was conducted with Mogens Rom Andersen, who is Lead Architect on MitID on behalf of the Danish Digitization Agency. MitID is the digital identification solution in Denmark. Mogens is taking part in the EU Digital Identity Wallet working group, which is introduced in section 3.1.3.

The purpose of conducting this interview was to gain an in-depth insight into the effects of PSD2 and eIDAs in the EU, introduced in section 4.1.2 and 3.1.2 respectively.

The PSD2 addresses the competitive situation within the financial sector in the EU, by enabling new business opportunities for third party service providers. In order to provide services, third parties must access sensitive customer data through banks APIs. *The problem*

lies in the implementation of the APIs that must provide access to data - someone needs to implement something on top of the APIs, which can provide security.

What Mogens implies in terms of security to comply with PSD2, is the implementation of 2FA through digital identities, as users need to be authenticated due to know-your-customer (KYC) requirements, made to minimize the risk of money laundering and financial crimes of the like. The aim of eIDAs is to provide users with the opportunity for deciding what data banks must have access to, what attributes that needs to be passed on, as the privacy aspects of the user is at the center. Mogens states that *It is about pressuring the banks commercially for accepting customer that want more privacy.* Financial institutions need to decide whether they want these customers, and if not, these customers might go somewhere else.

In Denmark, the digital identity verification and authentication system for governmental entities and online payment services, is centrally governed, as elaborated upon in section 3.1. Trust is inherently established among the IdPs and service providers, so that data is shared among authorities which enables users to access their data. The EU digital wallet presented in section 3.1.3 provides users with access to their data through a wallet, for the purpose of enabling control to a larger extent. *The problem is that there is an assumption that users are capable of making an informed decision.* Herein he refers to the concept of informed consent, and adds that some users might not be able to make such an informed decision.

According to Mogens, a lot of scams involve tricking users into sharing sensitive information about themselves. His concern is that the protection of the centralized systems enforced in Denmark today, might disappear with a data wallet. The centralized systems protect users from such mistakes, opposed to a decentralized model, where users are in control of their data, the user will have provided consent for sharing sensitive information. This is an interesting take on this issue, as being tricked into sharing sensitive information, the user has provided explicit consent, but based on insufficient, or even inaccurate information.

This will place greater demands on the companies that collect and process user data for providing users with sufficient information for them to be able to make an *informed decision.*

He continues elaborating upon the potential future scenarios of utilizing a decentralized digital data wallet compared to the centralized system provided to day - *In relation to the*

banks, here are users very protected. This might change by utilizing a data wallet - Now you, as a user, have more responsibility and this might entail an increase in the price for insurance excess.

The banks are required to oversee processes related to KYC to avoid fraud. This means that as a company are they interested in knowing as much as possible about their customers. *The consequence of open ecosystems is more fraud, when banks have less control of user data, which the users will pay for the price for.*

When asked about his opinion about the biggest threat of data privacy in society today, he replies social media (SoMe). Today, larger parts of the population are incapable of evaluating the threat of data privacy. *The question is how mature people are to know, what they are doing. They make data accessible to the world and by that risks that the world might use that to your disadvantage.*

5.2.3 Product Manager, Financial Services

This interview was conducted with Jakob Andkjær, who has a background working with financial services, among others the Danish FinTech company MobilePay.

The purpose of conducting this interview was to explore the approach and opinions towards open ecosystems and an increased focus on data privacy and security within the financial sector. Open ecosystems and a greater focus on user-centric data privacy, challenges the established trust relationships among financial institutions and the ecosystem they are part of. The sector consists of large institutions that handle and ensures large systems and processes. *It is about stability and meeting the expectations placed on them.* According to the respondent, these systems meet the expectations to a large extent.

The PSD2 creates the opportunity for technology to innovate to a greater extent within the financial sector, increasing competition for the benefit of the consumer *...but much of it is still the ASPSP that bears the traditional liability on the transactions performed today.* It is therefore in the interest of the banking institutions to ensure the trust relationship with third party service providers as well as ensure the level of trust in identification and authentication

of their customers. This becomes especially important, when it comes to the data that has traditionally existed exclusively within closed data silos. *These providers a subject to regulation, e.g. they must register as either a PISP or an AISP.* This registration is handled nationally within the Member states, and registered in a central registry launched by the European Banking Authority, that provides transparent means for displaying the identity of the authorised payment and account aggregation service providers.

Globally, the payment market is growing and continuously increasing, around 6 pct a year. More payment transactions take place online, and an increased number of micro transactions create potential for growth.

Incumbent financial institutions are aware of the competitors and low barriers of entering the market, as a large part of bank's earnings come from payment transactions. The increase in the payments market is highly depended on the increased global digitization, which entails a growing market for payment transactions which ensures that there are room for many providers. *The increasing globalization means that one might expect there to become a greater amount of cross-platform services among digital services*, such as building banking services and payment options into existing solutions that contains a large user base, e.g. the Facebook platform.

Banks are interested in minimizing the amount of data collected, which constitutes the necessary data that they are required to by law. This is the data that relates to identifying and authenticating legal persons to that level of assurance that is required in the context of mitigating the risks of money laundering, terrorism financing and tax fraud. The respondent's person position is positive towards regulation that considers the individual's personal data. *Other parties can now access this data which means that it needs to be subject to proper regulation. And as a private individual has the explicit opportunity to choose with whom this data is shared with.* It is a trade-off between the privacy and control of the individual, and a matter of security from the perspective of the banks.

In terms of trust, the respondent believes that trust is nationally and culturally conditioned and targeted the individual service provider. In Scandinavia, financial institutions have a high degree of trust, which is expressed through the reduced use of cash payments

compared to other European countries, such as Finland and Germany. *They have a completely different relationship with money, banks and institutions in general. Cash payments are much more pronounced.* This can be an expression of a lack of trust in institutions, as online and credit card payments are traceable.

5.3 Comparison

5.3.1 Traditional ecosystem

The PSD2 impacts the ecosystem for payment initiation and account aggregation. According to a Deloitte survey conducted among 90 European banking institutions, the expected impact on the market following the PSD2, in the product category, the area of payments is expected to have the largest impact by 90% followed by the day-to-day banking by 65% and customer loans by 47% [51]. The acceptance and adoption of digital solutions for offering banking services are rapidly increasing. According to a YouGov report investigating the future of financial services in 18 global markets, making payments using a digital wallet is the strongest challenger to traditional finance activities. 42 pct of consumers reporting using a digital wallet to make online payments, followed by 26 pct reporting using contactless mobile payments in store [55].

Figure 5.1 displays the ecosystem for credit card transaction processing when a user engages in a credit card payment transaction from a website within the established ecosystem. The diagram displays the high level trust relationships among the entities taking part in credit card payment online.

As displayed, the user initiates a credit card payment transaction through a website using a credit card. The information for the payment transaction is sent from the payment gateway to the payment processor, captured by the acquirer bank and forwarded to the appropriate credit card network. The latter forwards the request to the correct issuer bank, which requires SCA, as presented in section 4.1.1.

The identification and authentication is handled by the MitID system, as elaborated upon in section 3.1.1. The user and the IdP has an established trust relationship, and the

IdP and relying party has an established trust relationship. This ecosystem does not ensure transparency, control or privacy as there is not transparency in data processing among the intermediaries. The MitID IdP controls and tracks the usage of the digital identity, and the associated PID that pertains to a user is bundled in authentication processes.

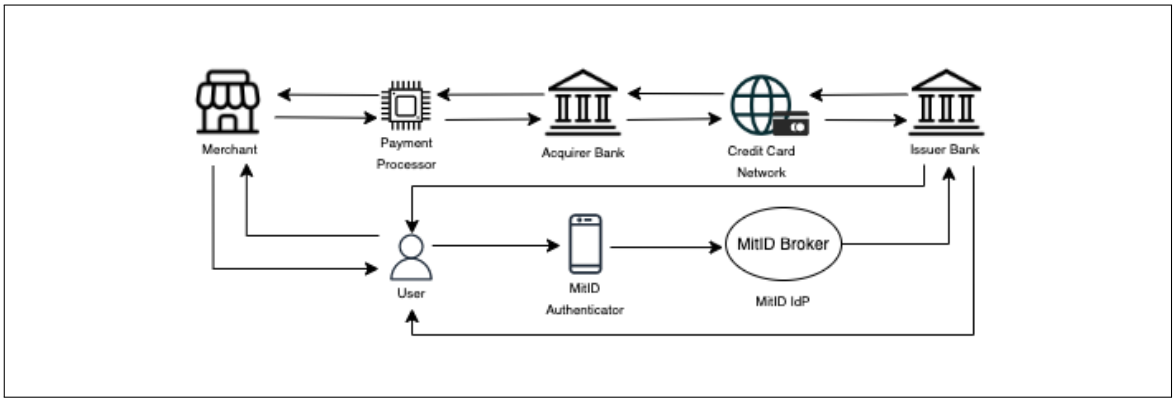

Figure 5.1: Established credit card transaction ecosystem

5.3.2 Interchanged ecosystem

The implementation of PSD2 and the paradigm of open banking that it entails, changes the trust relationship among financial institutions and the environment they operate in. Third party service providers are subject to regulation for ensuring strong customer authentication, and must obtain either a PISP and AISP certificate from the national authorities, which is accessible in a central registry provided by the European Banking Authority, as elaborated upon in section 4.1.2.

The incumbent financial institutions is now in a new, direct trust relationship with third party services providers, represented by QWAC certificates, are issued by Qualified Trust Service Providers, as stated under eIDAS 2.0 in section 3.1.1.

Figure 5.1 illustrates how the traditional 1-1 banking relationship is changed by ecosystem enabled relationships. Transitioning from a closed model to an open, platform-based ecosystem introduces transparency and openness in the market, which will eliminate the

asymmetries in information, previously referred to as the data silos in section 4.1.1.

The financial institutions will still have to ensure the quality of external services [51], as they will continue to be responsible for ensuring secure access to data, as well as for the ownership and security of customer data [54] to maintain trust with customers and trust with stakeholders of the ecosystem [51]. Unreliable services will damage trust [51] [54] as *much of it is still the ASPSP that bears the traditional liability on the transactions performed today*, as stated by respondent number three in section 5.2.3. The image displayed in Figure 5.2 provides a high level of how the ecosystem enabled relationship changes the traditional bank centric model.

Open ecosystems poses security challenges for financial institutions, as banks and third party service providers must adopt the same security standard in order to mitigate the risk of industry-wide inconsistencies, and the challenges that a lack of proper API standardization might entail, such as screen scraping [54]. The PSD2 RTS does not provide explicit technical details of development in terms of protocol requirements for APIs within its RTS [51], presented in section 3.3.1.

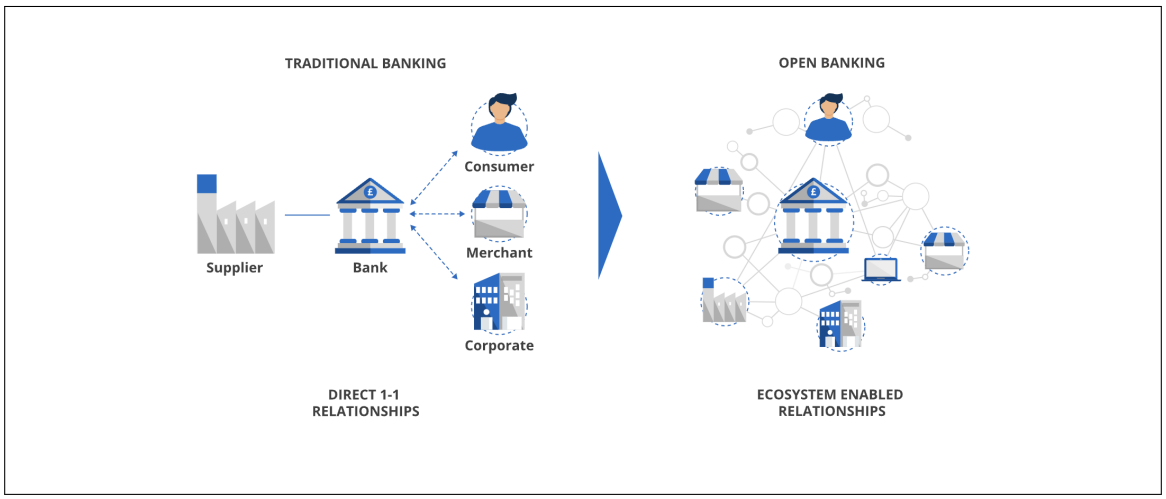

Figure 5.2: Traditional banking and open banking ecosystem [47]

Enabling open ecosystems supports the necessity of a digital identity that is not dependent on a third party entity for controlling and issuing identity assertions, as elaborated upon in section 3.1. SSI allows users to proof their identity without involving a third party [72], as in the case with centralized identity management systems and MitID presented in section 3.1.1.

The third expert interviewee respondent in section 5.2.3 states that *the increasing globalization means that one might expect there to become a greater amount of cross-platform services among digital services.* In order to achieve the ambition of PSD2 and mitigate vendor lock-in to ensure greater choice, consumers should not be locked-in to identity providers.

The eIDAS 2.0 initiative brace the decentralized identity management model, enables financial institutions to have a direct trust relationship with their customers, as no third party IdP is necessary for ensuring strong customer authentication in order to accommodate the substantial LoA required for high risk transactions [52], as denoted in section 3.1.2.

Self-Sovereign Identity, elaborated upon in section 3.2, presents a new user-centric trust triangle [38], as displayed in Figure 5.3, which eliminates the need of an intermediary IdP, that service providers must have an established trust relationship with, as introduced in section 3.1. and displayed in Figure 3.2.

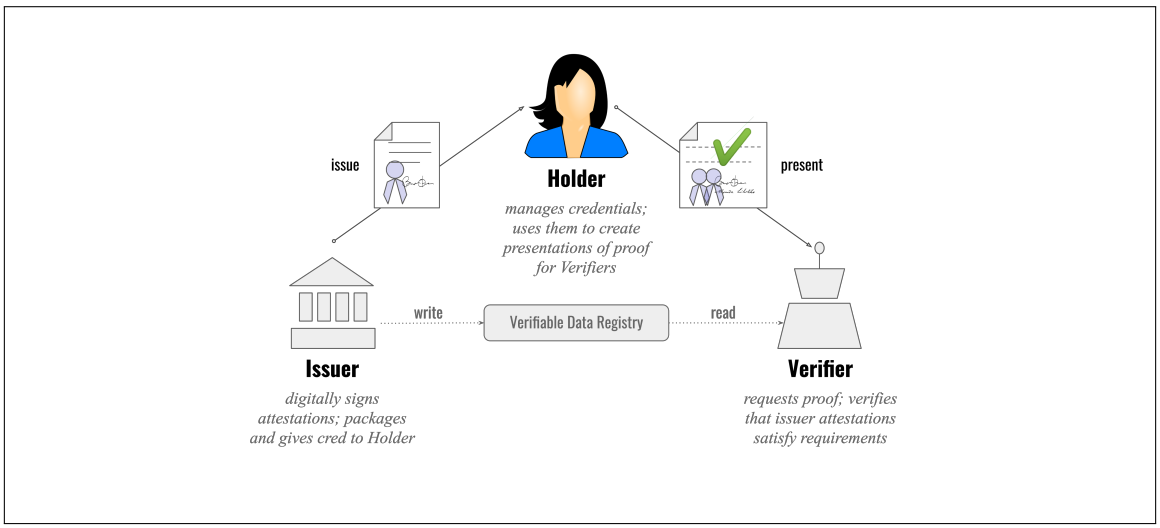

Figure 5.3: Self-Sovereign Identity trust triangle [38]

The PKI data registry establishes bilateral trust among the parties, and guarantees the authenticity of data and attestations without storing any personal data in the data registry. As displayed, this novel trust triangle eliminates the need of a third party IdP, which preserves privacy as the issuer does not have a direct relationship with all verifiers [38].

Holders manages their verifiable credentials through a digital wallet stored on their smartphone device, which supports biometric authentication such as fingerprint and facial recognition. The data wallet in which the verifiable credentials are stored, is protected by such biometric authentication means to increase the binding to holder. This enables holders to selectively disclosure the data necessary for a given authentication context and control their digital identity and associated identifiers [72].

SSI enables digital trust by combining the aspects of trust presented in section 5.1. Transparency is provided through storing personal data on the smartphone that the holder controls, as the holder manages their credentials and presents proof to verifiers. Verifiers request the attributes necessary for specific authentication scenarios, rather than requesting an entire data bundle, as it is the case with centralized identity solutions [13], such as MitID presented in section 3.1.1.

This presents transparency in what PID is shared, and addresses this issue presented by respondent number one in section 5.2.1, who stated that *In most cases, it is still cumbersome to oversee and discern the amounts of data collected, and the purpose for the collection and processing of it.*

Furthermore, privacy and control is enhanced, as verifiable credentials can support minimization of data disclosure, which enables user to indirectly proof a claim without revealing its attributes. The verifiable credentials are encrypted with the private key of the holder to ensure security and reliability in the identity data, at it would require access to the private key for at attacker to decrypt it. This mitigates the risk of impersonation and fraud [2], as identified in section 5.1.

In continuation of the eIDAS 2.0, the EU Commission has proposed the EUDI Wallet presented in section 3.2.3, for the development of the associated identity credentials. According to the proposition, each EUDI wallet should have a unique identifier. This would enable

digital tracking, correlation and profiling and act like a global super-cookie, presumably for the purpose of allowing a wallet provider to dismantle the wallet for protection purposes, in case a credential is lost or stolen [20]. This appears to entail several usability challenges, as a digital wallet would likely contain credentials that are not issued and certified by Qualified Trust Service Providers (QTSPs) solely, in order to avoid imposing private sector restrictions [20]. The wallet issuers are Member States and organizations mandated by Member States.

In order for users to benefit from these services, they need to trust the entities of the ecosystem. The financial institutions, the third party service providers, merchant and issuers of credentials must be trusted [65]. As the open banking paradigm enables user data to be shared among organisations, banks need to ensure data protection, and user control of PID is handled and shared to ensure transparency and privacy. As PSD2 does not mandate the creation of common API standards means each banking institution must make their data available through different technical standards, adding an addition layer of complexity around data aggregation and sharing [65].

5.4 Summary

The Analysis chapter presents digital trust, and why digital trust is bad today. The chapter presents the key parameters necessary for establishing digital trust, respectively transparency, accessibility, privacy, control, security, reliability, ethics and responsibility.

Section 5.2 discusses the key points presented by the three expert interviewees elaborating upon the topics of trust, potential issues of open ecosystems and decentralized identities as well as the current state of the payment landscape within the financial sector.

Furthermore, section 5.3 presents a high level comparison of the traditional ecosystem within the financial sector, and the interchanged ecosystem that the SSI enabled trust triangle and PSD2 entails.

Chapter 6

Deployment Proposals

The following chapter presents the novel scenarios that PSD2 and eIDAS 2.0 initiatives entails. It provides a qualified suggestion to how the SSI framework and FAPI specification supports the novel trust relationships by presenting potential deployment proposals.

The European initiatives presented in section 3.1.2 and 4.1.2 opens up for new scenarios, which holds the potential to change existing ecosystems within the financial sector. The scenarios identified are based on the interchanged trust relationships presented in 5.3.2. The diagram presented in Figure 6.1 displays how the interchanged ecosystem could look like, compared to the traditional ecosystem presented in Figure 5.1.

In order to accommodate the potential of the EU initiatives, the technological frameworks must support the scenarios that becomes apparent while enhancing privacy and transparency within a novel ecosystem. The high level deployment proposals elaborated upon in this chapter, explains how such a system could behave, and how SSI and FAPIs supports the required functionality in order to establish trust. The scenarios and selected deployment proposals demonstrates how the technology potentially could support the eIDAS 2.0 and PSD2 initiatives and by that ensure freedom, less dependency and lock-in in financial services, as well as privacy, transparency and mitigate single dependency on a digital identity provider.

6.1 Scenarios

The scenarios listed below are derived from chapter 3, chapter 4 and the analysis of digital trust and the interviews presented in chapter 5. The scenarios present potential application areas for SSI and FAPIs.

PISP initialization For PISPs to initiate payment transactions from a banking institution, the PISP must have published a DID to a public ledger and obtained an SSA from a QTSP directory.

Payment Initiation PISPs can initiate instant bank payment transaction directly from a banking account, eliminating the need of credit cards networks and payment processors.

Recurring Payment Initiation Subscription-based payment models can benefit from the lack of friction and cost advantage as one-time payments, as the subscription to a recurring payment relationship does not depend on the validity of a credit card.

Personal Finance Management AISPs can aggregate financial data from several accounts through a read-only security profile, enabling service providers to display information from multiple accounts in one place. This scenario eliminates the need for users to login in to multiple platforms, and mitigates customer lock-in which increases competition.

Know-Your-Customer SSI enables frictionless ID verification means, by extending the current single-use ID verification, presented in section 3.1.2, to a user-centric reusable KYC, which requires verification once. This enables user to instantly share KYC credentials with a merchant.

Digital ID Applicable Across Industries SSI enables user to present identification information across industry ecosystems, which improves privacy, security and improves onboarding processes for new customers and users.

The role of the entities and its description presented in the deployment proposals elaborated upon in the following sections is presented in Table 6.1.

Role	Description
Issuer	The party that creates and issues Verifiable Credentials to Holders
Holder	The party to whom the Verifiable Credential has been issued to
Verifier	The party that requests and verifies Verifiable Credentials to provide a service
Relying Party	The party who relies of Verifiable Credentials for identification and authentication in order to provide a service
ASPSP AS	Issuer Bank authorization server
ASPSP RS	Issuer Bank resource server
PSU	Payment Service User who initiating a payment process through a PISP
QTSP	Qualified Trust Service Provider which issues QWAC and QCSEAL certificates

Table 6.1: Role Description [54] [72] [39]

6.2 Impact of PSD2 and eIDAS 2.0

The PSD2 presented in section 4.1.2 changes the ecosystem for account aggregation and payment initiations. Figure 6.1 displays the potential interchanged ecosystem and its entities, respectively the PISP, the Issuer bank, the Holder, the Merchant and the PKI data registry. The high level overview of the ecosystem illustrates how the trust relationship is shifted, as the PISP has a direct relationship with the customer denoted the holder, the issuer bank and the merchant.

The diagram displays the new role of the PISP and how SSI could support strong customer authentication scenarios. As displayed, the PISP has a direct relationship with the bank, which changes the payment landscape presented in section 4.1.1 by excluding the payment processor, acquirer bank and credit card network intermediaries from this process. This

enables the open ecosystems stated under PSD2 in section 4.1.2, as data can be exchanged through APIs instead of proprietary networks. Eliminating the number of intermediaries changes the trust relationships, which is privacy enhancing, and provides transparency in which entities taking part in the process and handling the associated PID, as discussed in section 5.1.

The ecosystem presented in Figure 6.2 assumes that the PISP and the merchant has an established relation, and that the holder has been issued a verifiable credential by its issuer bank and a verifiable credential by a government institution. The bank credential is used for authentication at the PISP, which checks the authenticity of the credential at the PKI data registry, and requests the payment initiation through the FAPIs at the Issuer bank. The verifiable credential issued a government institution, denoted identity credential, is used for authenticating at the merchant. Utilizing the verifiable credentials eliminates the centralized intermediary, that MitID constitutes as displayed in Figure 5.1, and shifts the trust relationships among the entities. The issuer to holder trust is shifted in SSI compared to the centralized identity management systems, presented in section 3.1, as the intermediary IdP is eliminated. This entails privacy, control and transparency in how PID is shared. The issuer to verifier trust is also shifted in SSI, as issuers do not have to establish a direct trust with verifiers, as the digital identity does not rely on assertions issued by an intermediary IdP. The high level process is elaborated upon in the following, whic illustrates hos the payment landscape could presented in section 4.1.1 and the traditional ecosystem displayed in Figure 5.1 could be interchanged.

1. The holder requests a merchant to show a license in order to validate the authenticity of the merchant

2. The merchant shows a license issued by the government which the holder verifies by checking the DID of the issuer. The holder trusts the government that issued the license, which the holder can check without contacting the issuer, as it checks the DID published in the data registry

3. The holder initiates a purchase from a merchant, which requests the holder to generate a verifiable presentation of PID, respectively full name and address. The verifiable presentation is displayed in Appendix B.5 and derived from the verifiable credential in Appendix B.4.

4. The merchant verifies the verifiable presentation and requests the holder to select the PISP which should process the payment

5. The holder selects a PISP from a list of PISP that the merchant has a trust relationship with

6. The payment initiation request is forward to the selected PISP by the merchant

7. The PISP requests the holder to present PID and banking attributes by its banking institution

8. The holder generates a verifiable presentation as requested by the PISP

9. The PISP checks the DID of the verifiable credential issuer presented by the holder

10. The PISP requests the payment initiation at the issuer bank by providing the name of the holder, the account number of the holder, the name of the merchant and its associated account number at its acquirer bank

11. The bank receives the payment requests and requests the holder to present its verifiable credential issued by the bank

12. The holder generates a verifiable presentation to the bank and consents to the payment

13. The payment is approved and consumed from the banking account

14. The PISP forwards the payment to the merchant

15. The holder receives a confirmation that the payment was processed correctly

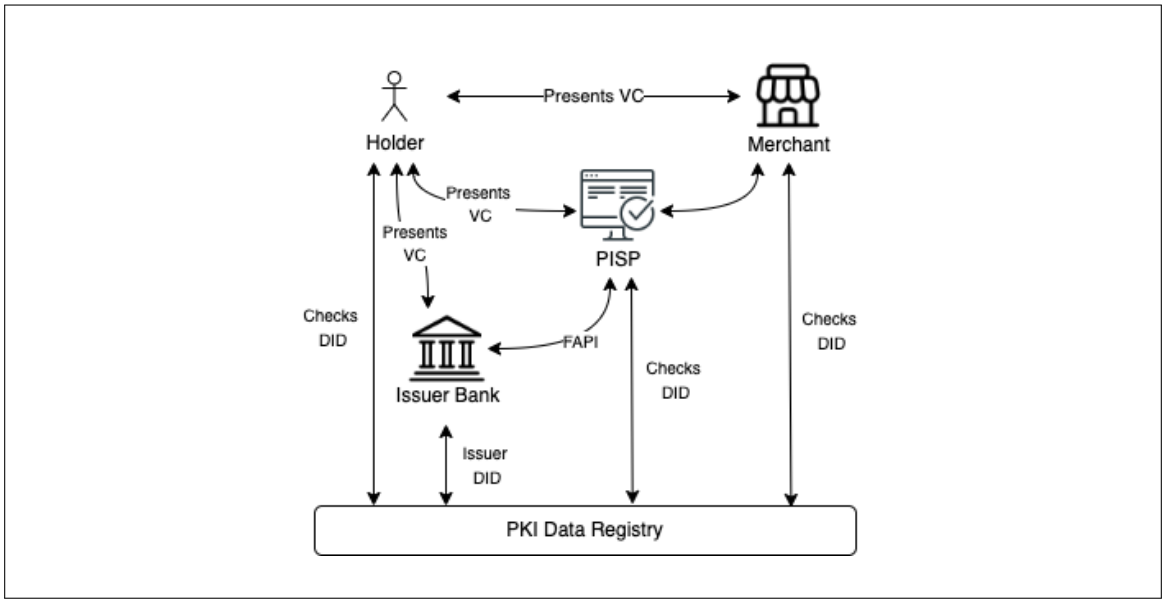

Figure 6.1: PISP and SSI Payment Process Ecosystem

6.3 Initialization

In order to take part in this ecosystem all entities must be verifiable. To build trust, it is crucial to ensure that it is the correct entity that is being communicated with, as they can be cryptographically verified. This is done by generating a public/private key pair. The private key encrypts a credential or a license, and the public key decrypts it and verifies the issuer of the credential or license as well as the holder.

The entities, respectively the issuer bank, the PISP, the merchant and the holder publish a DID document and its associated public key to a public ledger, which enables verifiers to verify the authenticity and validity of an issued credential or license, as described in section 3.2.1. This allows the issuer bank to issue a verifiable credential to the holder, which the PISP and the bank itself can verify. It allows the PISP to verify itself to the bank, the holder and the merchant, and it allows the merchant to verify that it was issued a license from a government institution to the holder and the PISP, which would enable the merchant it verify itself.

The ecosystem presented in section 6.2 and displayed in Figure 6.1 assumes that the

banking institutions has issued a verifiable credential to the holder, which the holder uses to authenticate at the bank and the the PISP. In order to issue a VC, the bank must publish its DID document with its public key to the data registry for verifiers to verify the authenticity of issued credentials.

The sequence diagram in Figure 6.2 presents the flow of registering a DID document to a data registry, which uses PKI in a decentralized manner. The data registry is an immutable public ledger as it has the ability to remain unchanged. This functionality ensures that it cannot be altered hence data is not easily changed, and by that ensures the integrity and security of the DIDs published on the ledger.

Figure 6.2 displayed the process of publishing a DID document to a data registry. As displayed, the issuer uses a standardized schema which outlines the meta data of issued credentials and registers a DID on the data registry which signs all issued credentials [68].

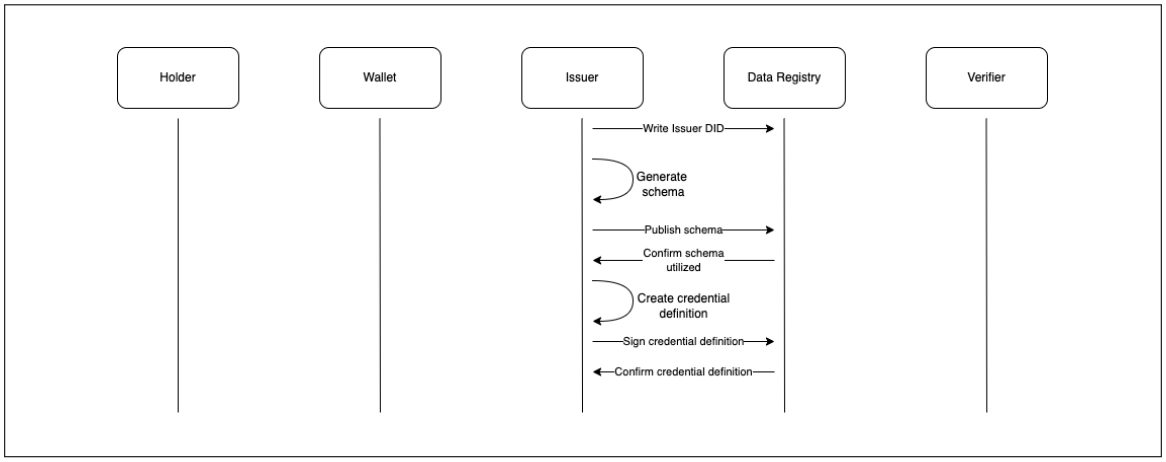

Figure 6.2: Issuer create DID document [68]

Issuing Verifiable Credential

In order to obtain a verifiable credential, holder must download a wallet to their phone, which must possess SSI capabilities for holding credentials and verifying them. As displayed in Figure 6.3, the holder downloads a wallet and uses it to register a user DID and its public key to the data registry. This enables the holder to sign the verifiable credential it holds with its private key to proof ownership of issued credentials, as the private key is not shared.
The banking institution can choose to present an optional offer to a holder. The sequence in Figure 6.3 displays how a holder requests a verifiable credential at the issuer, which is its banking institution. The issuer requests attributes of PID to conduct identity proofing that accommodates the IAL2 as defined under eIDAS 2.0 presented in section 3.1.2, which can be completed remotely as presented in section 3.1.1. The KYC credential issued by the bank displayed in Appendix B.2, accommodates the IAL2, by supporting the existence of the claimed identity and verifying that the user is appropriately associated with the real-world identity [12].

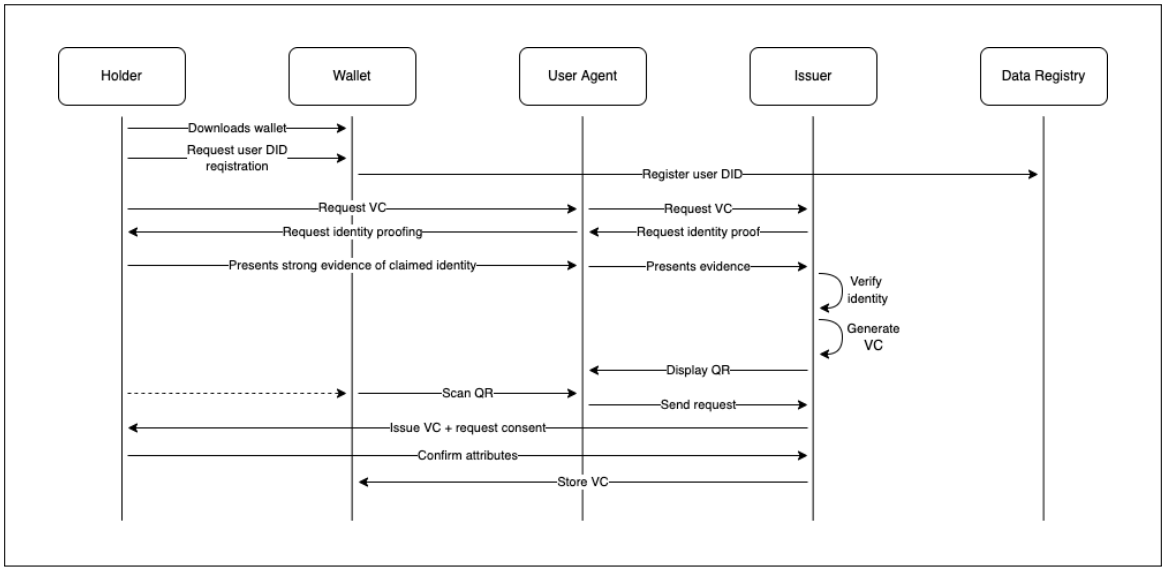

Figure 6.3: Process of obtaining a Verifiable Credential [68]

The verification process is concerned with binding the claimed identity to the presented identity through biometrics comparison. [12]. This ensure the substantial degree of confidence in the classification level of the verifiable credential, as presented in Figure 3.3, providing high confidence that the user controls multiple authenticators [12]. AAL2 requires proof of possession and control of two distinct authentication factors, respectively a cryptographic authentication device with an integrated biometric sensor [12].

When the Issuer has verified the identity through the identity proofing, the holder receives a QR code from the Issuer, which is scanned with the data wallet of the holder. The verifiable credential is displayed to the Holder to verify its attributes, and accept the credential by authenticating using biometric facial recognition. The verifiable credential is now issued and stored in the holder's wallet.

Obtaining SSA

For a PISP to be able to handle the known and established scenarios of initiating a payment transaction as elaborated upon in section 4.1.1, the PISP must establish a trust relationship within the financial sector. The PISP must obtain QWAC and QCSEAL certificates as stated under the PSD2 RTS in section 4.1.2, issued by a Qualified Trust Service Provider (QTSP). Appendix B.1 presents the requirements for obtaining the certificates.

Figure 6.2 displays the process of establishing the trust relationship with the bank. As displayed, the PISP requests the Software Statement Assertion (SSA) at a QTSP. The QTSP evaluates and issues the signed SSA to the PISP, which is a JSON Web Token containing client meta data about the PISP. Banking institutions use this SSA to establish trust with the PISP. The PISP can now request access to a banking API gateway by presenting its issued SSA. The bank checks with the QTSP directory, which acts as a trusted third party. The SSA is valdated, and the PISP receives a client ID and secret from the banking institution in question.

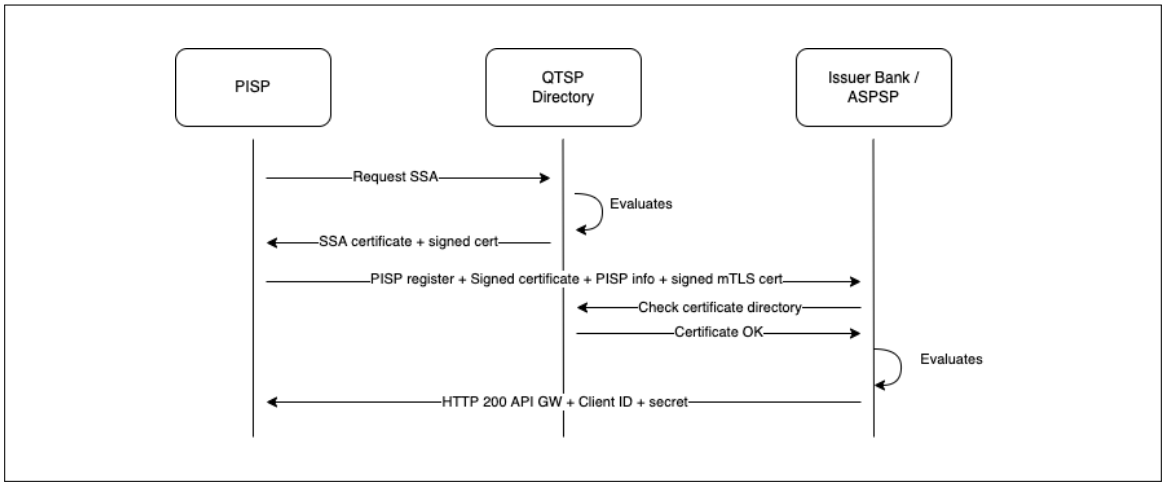

Figure 6.4: Establish trust relationship with bank [15]

6.4 Ad Hoc Payment Transaction between PISP and Bank

In order to complete a payment transaction between a PISP and a bank, the initialization process presented in section 6.2 is prerequisite. It considers a user initiating a payment transaction with a PISP, which must have an established trust relationship with a QTSP directory. Ad hoc interactions with a PISP can ensure an open ecosystem of payment initiations as well as greater choice and a better user experience. The ad hoc payment does not assume that the PISP has an established relationship with a banking institution.

It assumes that the holder has a trust relationship with a banking institution, and a verifiable credential which confirms this. The deployment proposal presented is realized by utilizing the SSI framework presented in section 3.2 and the Financial-grade APIs presented in section 4.2. Table 6.1 presents the roles associated with the deployment proposals and their individual responsibility.

The following deployment proposal considers an ad hoc payment transaction between a PISP and a bank. Figure 6.7 illustrates the flow of the Financial-grade API presented in section 4.2. This flow assumes that there is a relationship between the holder and the issuer and the holder and the verifier, which is the established direct trust relationship between the bank and the PSU.

The diagram is based on the high level interaction displayed in Figure 6.1, which presents the payment initiation and how the established ecosystem payment processing presented in section 5.3.1 is changed. The diagram presents an qualified suggestion to how the flow in the novel trust relationships, the SSI framework and FAPIs supports, could look like. As displayed, the PSU in the diagram, requests to initiate a payment transaction through a PISP. The initiation request considers generating the verifiable presentation displayed in Figure 6.6.

As displayed, the user requests a payment initiation at the PISP by generating a verifiable presentation which expresses a subset of the data contained in the verifiable credential issued by its banking institution, the ASPSP. The verifiable presentation is displayed in Figure 6.6, and derived from the verifiable credential found in Appendix B.2.

The attributes contained within the verifiable credential presented is used to request the payment initiation at the ASPSP. The verifiable credential which the verifiable presentation is based on is stored in a data wallet on a device the user controls. As displayed, the verifiable presentation contains identifiers, meta data and a set of claims pertaining to the credential holder. The meta data describes the properties of the credential, respectively the type, the issuer and date of issuance. It contains an identifier of the subject of the presentation, which is a DID denoted "credentialSubject", as well as a DID of the Bank which issued the credential. The PISP evaluates the authenticity of the verifiable presentation by checking the data registry which is an immutable distributed ledger. The "customerOf" claim in the verifiable presentation is expressed using subject-property-value relationships, as displayed in Figure 6.5 [9]. The claim contains the DID of the issuer of the credential in question.

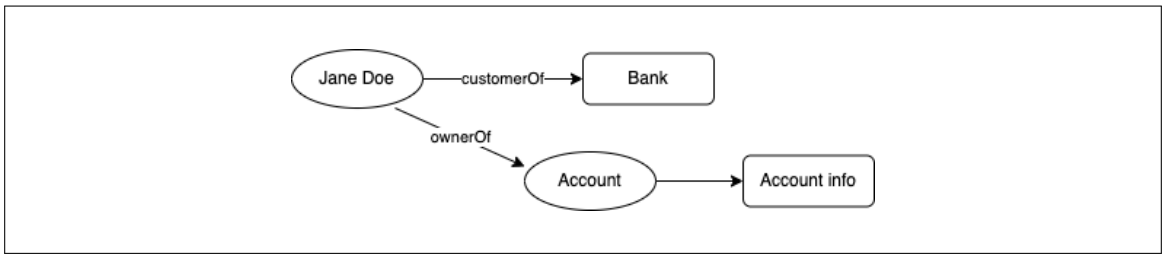

Figure 6.5: Subject-property-value relationship in the verifiable credential [9]

The DID contained in the presentation resolves to a DID document, as presented in section 3.2.1, which contains the public key of the issuer that verifies that the credential in question was issued by the claimed bank. The PISP trusts this issuer which verifies the attributes of the credential. The verifiable presentation contains the DID associated with the holder, which signs the verifiable presentation with its private key bound to biometric identifiers associated with its device that stores the data wallet. The PISP checks the DID document that contains the associated public key, which verifies the credential was issued to the holder generating the presentation. This ensures that the data can be trusted as it has been cryptographically verified.

The verifiable presentation expresses the information the PISP needs in order to request a payment initiation at an ASPSP. As displayed in Figure 6.6, the presentation presents the necessary information required by the PISP, respectively the name and the account number with the bank [16]. The presentation is signed with the digital signature of the holder who uses a biometric identifier to consent, which ensures binding of the presented credential to the holder.

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "type": "VerifiablePresentation",
  "verifiableCredential": [{
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.w3.org/2018/credentials/examples/v1"
    ],
    "id": "http://example.edu/credentials/1872",
    "type": ["VerifiableCredential", "KYCCredential"],
    "issuer": "https://example.edu/issuers/565049",
    "issuanceDate": "2022-05-08T19:23:24Z",
    "credentialSubject": {
      "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
      "customerOf": {
        "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
        "account": [{
          "firstName": "Jane",
          "lastName": "Doe",
          "accountNo": XXXX XXXX XXXX 4501"
        },]
      }
    },
    "proof": {
      "type": "RSASignature2018",
      "created": "2017-06-18T21:19:10Z",
      "proofPurpose": "assertionMethod",
      "verificationMethod": "https://example.edu/issuers/565049#key-1",
      "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X
        sITJX1CxPCT8yAV-TVkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUc
        X16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G_zS245-kronKb78cPN25DGlcTwLtj
        PAYuNzVBAh4vGHSrQyHUdBBPM"
    }
  }],
  "proof": {
    "type": "RSASignature2018",
    "created": "2018-09-14T21:19:10Z",
    "proofPurpose": "authentication",
    "verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec21#keys-1",

    "challenge": "1f44d55f-f161-4938-a659-f8026467f126",
    "domain": "4jt78h47fh47",
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..kTCYt5
      XsITJX1CxPCT8yAV-TVIw5WEuts01mq-pQy7UJiN5mgREEMGlv50aqzpqh4Qq_PbChOMqs
      LfRoPsnsgxD-WUcX16dUOqV0G_zS245-kronKb78cPktb3rk-BuQy72IFLN25DYuNzVBAh
      4vGHSrQyHUGlcTwLtjPAnKb78"
  }
}
```


Figure 6.6: Verifiable presentation requested by PISP [68] [9]

The PISP forwards the request to the ASPSP through FAPIs. The PISP establishes mTLS between the authorization server (AS) and the resource server (RS) prior to each request. The process of obtaining an access token in order to access protected resources is illustrated in Figure 4.7 and elaborated upon in section 4.2.1.

The expert interview discussed in section 5.2.2 presents the issue of how the sensitive financial data is shared within the ecosystem. The interviewee states that *the problem lies in the implementation of the APIs that must provide access to data - someone needs to implement something on top of the APIs, which can provide security.*

The Financial-grade APIs presented in section 4.2, provides a security framework for sharing sensitive data. FAPI requires mutual TLS for exchanging data, and ensures a binding among the end user, the client and the API endpoints using JWT [1]. The PISP request the payment initiation on behalf of the user.

The bank requests strong customer authentication as mandated under PSD2 in section 4.1.2 to authorize the payment transaction. The user generates a verifiable presentation based on the verifiable credential issued by the bank, as displayed in Appendix B.2, and consents to the transaction. The bank evaluates the authenticity of the verifiable presentation by resolving the issuer DID to its associated DID document in order to confirm that it was the issuer of the credential. The bank also check the user DID document in the data registry in order to determine whether it is the correct holder who is generating the verifiable presentation. As the presentation is bound to biometric identifiers of the holder, the substantial level of assurance which mandates strong 2FA authentication is reached, as presented in Figure 3.5.

The bank authorizes the payment transaction and PISP forwards the payment to the merchant as displayed in Figure 6.1.

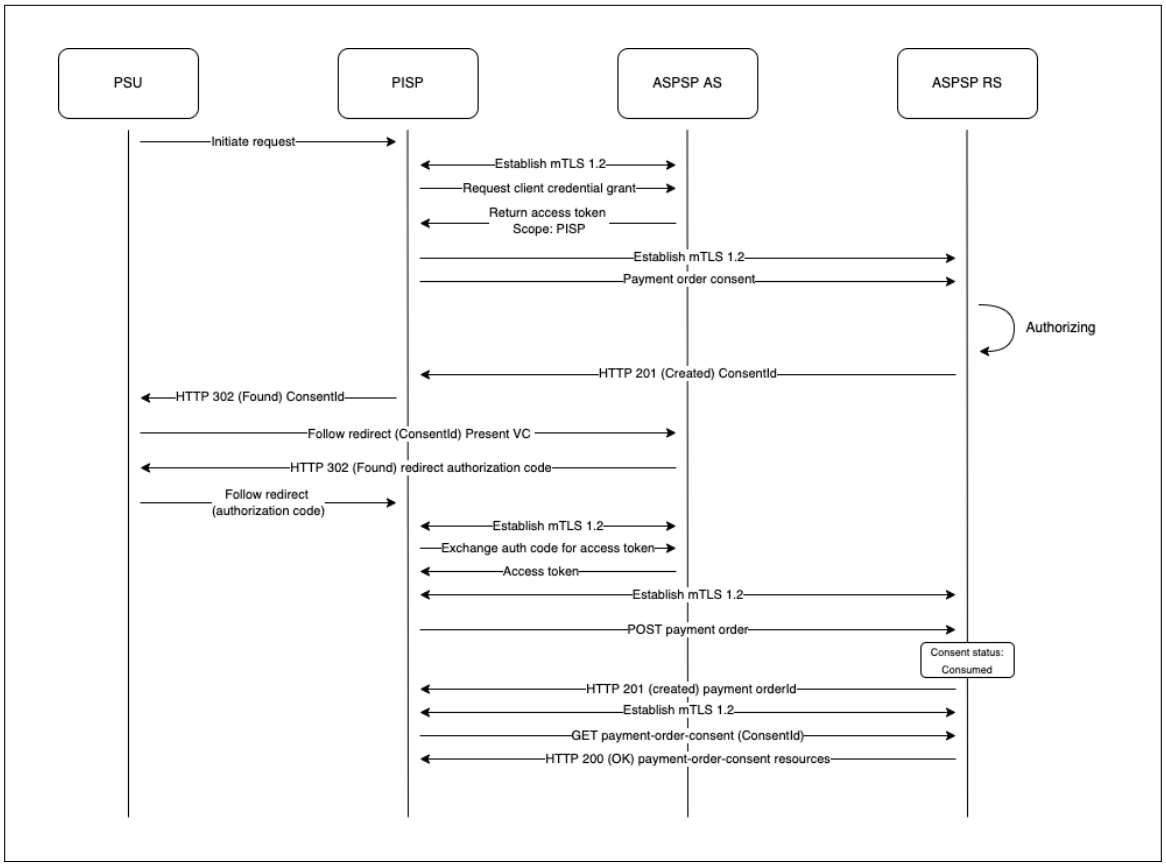

Figure 6.7: FAPI payment initiation flow sequence [41]

6.5 Resulting trust

The established ecosystems of payment transactions do not enhance privacy, transparency or control, as they depend on a single data controller for providing authentication. The traditional ecosystem of centralized identification and authentication presented in section 5.3.1 which utilizes MitID presented in section 3.1.1, is substituted with the Self-Sovereign Identity framework. Figure 5.3 displays the new trust triangle, which does not rely on one single IdP and hereby enables trust without integration. This ensures that interactions are tracked by one single IdP, as credentials are held by the individual to who they pertains. Ecosystems interact in a peer-to-peer manner using verifiable credentials, where organisations define their risk tolerance. This can enable the selective disclosure of data, where people only need to share information that is necessary within the specific authentication context.

The number of intermediaries within the payment processes is minimized, as discussed in section 5.3.1, which supports privacy and transparency in the entities that take part in processes. Control is established as users control their credentials and where they are shared. SSI and FAPI constitute a paradigm shift in the trust relationships, as the user is put in the centre of exchanging PID to verifiers. This allows the user to control their relationships with verifiers independent from third party identity providers, enabling control in how credentials are issued and how credentials are disclosed [7].

This shifts the trust relationships from an indirect relationship where trust is established based in assertions issued by a third party entity. A verifier therefore needs to directly trust the issuer. Figure 6.8 presents the potential interchanged trust relationships in the ecosystem that EU initiatives eIDAS 2.0 and PSD2 braces. The trust relationship among the entities within the identity ecosystem is shifted, as the user is centered in the identity process [7].

SSI and FAPI can work together to establish digital trust in the third party service providers to achieve a broad adoption as proposed by the PSD2. The SSI eliminates the need of username and password and improves authentication and authorization processes, which helps in building trust in transactions online [7].

SSI establishes direct trust, and relies on trust being build by exchanging verifiable cre-

dentials. To build trust, it is necessary to known who you are communicating with to ensure that it is the correct entity that you are communicating with. The entity controlling a DID needs to be verified in order to established this trust.

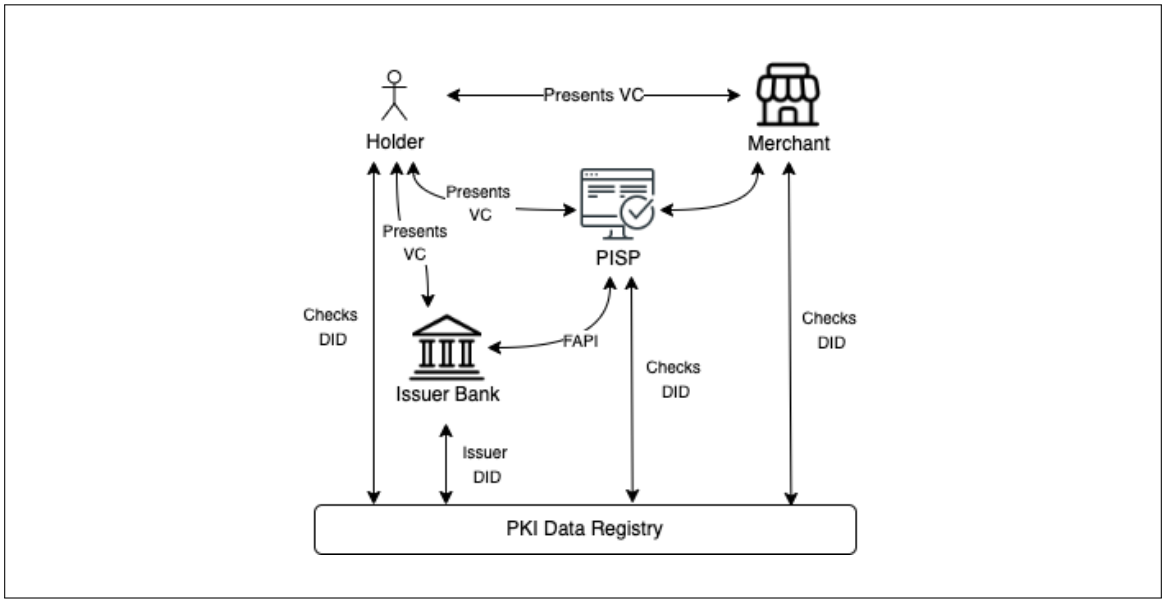

Figure 6.8: PISP and SSI Payment Process Ecosystem

Chapter 7

Discussion and future perspectives

Opening up established ecosystems presents new technological challenges in how user data is shared and protected in order to ensure digital trust, as trust is foundation for adopting new digital services.

Today, trust is not good due to the lack in transparency, control and choice of how personal data is shared. Financial-grade APIs and SSI holds the potential to utilize novel scenarios online payment transactions, which supports user empowerment and data privacy. Improving customer choice and enabling a broader environment for information sharing and payment initiation through open ecosystems, ensures transparency, freedom and less dependency, and thereby trust. In order for people to adapt novel digital services, trust must be present.

The European Union is pushing forward to change incumbent ecosystems through legislation. The purpose of the PSD2 is to infuse trust in to third party service providers, by subjecting them to security requirements, to mitigate obsolete data sharing techniques such as screen scraping and storing user passwords. This have resulted in a lack of trust, which prevents the adoption of new digital services from consumers as presented in section 5.1.

Chapter 6 presents the potential novel trust relationship, which minimizes the intermediaries in payment transactions. Figure 6.8 displays the ecosystem with a PISP, introducing a privacy and transparency enhancing ecosystem, compared to the ecosystem of credit card payment processing, presented in illustrated in Figure 4.2 and the traditional ecosystem displayed in Figure 5.1. However, the lack of standardization in how banking institutions

provide secure information exchange creates a complex environment for AISPs and PISPs, which could inhibit the ambition of the initiative. Furthermore, it is indecisive whether the business incentive for the AISPs is aligned with the privacy incentives, since such business models could be based on collecting data for the purpose of building data profiles of users. As these frameworks continue to evolve and no standardization have been adapted, these design proposals presents a realistic suggestion to how the ecosystem could potentially look like.

The regulation mandate strong customer authentication, further increasing the complex digital relationships that customers find themselves in. eIDAS addresses this issue by promoting the right for all individuals to have a digital identity, which enables citizens to share identification information in multiple contexts [52], and by that manage their provider trust relationships [44]. This opens up the opportunity to leverage the benefits of self-sovereign identity, which ensures bilateral trust between parties as identification and authentication does not depend on direct interaction between issuers and verifiers, and the digital identity is owned and managed by the individual to whom the identity claims concern.

The expert interviewee in section 5.2.2 states that *users are very protected today with the banks and centralized systems. That might change when having more responsibility, which might entail an increase in the price for insurance excess*, as users could fall victims to social engineering scams and share sensitive information. This trust is shifted as all entities are verifiable, which could enable users to identify untrusted sources in a transparent manner.

The design proposals treats payment scenarios because these are high risk scenarios in banking services. The expert interview discussed in section 5.2.3 states that *globally, the payment market is growing and continuously increasing, around 6 pct a year. More payment transactions take place online, and an increased number of micro transactions create potential for growth.*

The proposals present the direct authentication with a banking institution using a verifiable credential issued by the bank, which is used to generate a verifiable presentation requested by the PISP. This enables the PISP to focus on the digital services that they provide, as they would not be required to store a lot of sensitive PID and thereby save money on due diligence and performing id checks.

The incentive for financial institutions for supporting SSI is being able to rely on know-your-customer checks performed by another banking institutions. This mitigates the need for spending a lot of resources performing id checks, and for users to provide a lot of information every new place they go. Streamlining process for login without passwords, and being able to rely on identification previously performed could be beneficial in on-boarding new customers in banking as well as other commercial actors.

The sensitive information stored with verifiers, which is banking institutions, third party services providers or merchants, is becoming a liability. Being able to rely on good proofs which are cryptographically verifiable, will limit the amount of sensitive data stored, which could potentially ensure that a data breach would not be beneficial for a hacker, as the data alone becomes useless when the holder of a credential needs to proof that the credential in question was issued to them every time it is requested. This makes it significantly harder to impersonate a holder of a credential, as their private key must be compromised. In order to do so, the phone that they hold the data wallet on must be compromised. In this context, using biometric identifiers to bind credentials to holders adds an extra layer of security.

Furthermore, the challenge for implementing SSI stems in adopting a common standard for deploying verifiable credentials and methods for proving ownership of the issued credentials. The method presented in the design proposals are decentralized identifiers, but other potential cryptographically verifiable methods are being investigated as well.

Verifiers must trust the wallet that holds the verifiable credentials without compromising the privacy of its users. The reference architecture for the European Union Digital Wallet discussed in section 3.1.3 proposes to have a unique identifier for each data wallet. This could potentially work as a super cookie and thereby not support privacy. This creates a roadblock for the prevalence of SSI in terms of the root of trust, as the verifiers potentially needs to directly trust an unknown number of issuers with whom it has no established trust relationship with. How to establish trust within the data registry is challenge for future work.

Chapter 8

Conclusion

This thesis sets out to investigate *How can Self-Sovereign Identity support the implications of the liberalization of banking services that the PSD2 entails?*

In order to answer the problem formulation, comprehensive desktop research and semi-structured expert interviews have been conducted.

My research shows that in order for consumers to adopt novel digital services, digital trust is an important driving force. When trust is present, things are possible. Digital trust is established by combining the aspects of privacy, control, transparency, ethics and security. Utilizing SSI for digital identity management systems will change existing scenarios, and shift the trust relationships, as issuers cannot track where credentials are used. The Self-Sovereign Identity framework holds the potential to solve the issue of lack in transparency, control and privacy on how personal identifiable data is shared.

Financial-grade APIs support the open banking ecosystem that the PSD2 entails, which changes established ecosystems within the financial sector, respectively payment transaction scenarios and account information aggregation scenarios. Enabling PISPs changes the ecosystem within payment transaction initiation, and could lead to the exclusion of credit card networks and payment processor intermediaries.

My contributions to the academic field with this thesis is to propose how these technological frameworks can support EU legislation and shift trust in existing ecosystems. Enabling open ecosystems will ensure less dependency, vendor lock-in and more freedom and privacy

for users. To ensure a consistent user experience and secure data handling, a standard for FAPI must be adopted. A decentralised approach towards digital identity management systems is important in this context, as the identity is not tied to a single data controller, which mitigates the risk of single-point-of-failure while accommodating the required level of assurance through cryptographically verifiable data which is bound to biometric identifiers of the holder to which the PID pertains.

The areas of Self-Sovereign Identity and Financial-grade APIs frameworks are on-going and rapidly improving. The proposed design proposals in chapter 6 is a qualified suggestion to how trust is shifted with the PSD2 and eIDAS 2.0 initiatives, and how SSI and FAPI supports these novel trust relationships.

Bibliography

[1] Akana. *What is FAPI - Financial-grade API?* Dec. 2020. URL: https://www.akana.com/blog/what-is-fapi (visited on 05/10/2022).

[2] Andreas Abraham et al. "SSI Strong Authentication using a Mobile based Identity Wallet Reaching High Level of Assurance". In: *Proceedings of the 18th International Conference on Security and Cryptography* 1 (July 2021), pp. 137–148. DOI: 10.5220/0010542801370148.

[3] Daniel Fett et al. "An Extensive Formal Security Analysis of the OpenID Financial-grade API". In: *CoRR* abs (1901.11520) (Jan. 2019). DOI: https://doi.org/10.48550/arXiv.1901.11520. arXiv: 1901.11520. (Visited on 03/25/2022).

[4] Evgenia Nikolouzou et al. *Digital Identity: Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust.* Tech. rep. Jan. 2022.

[5] Feike Hacquebord et al. *Ready or Not: The Risks of Open Banking.* Tech. rep. Sept. 2019. URL: https://documents.trendmicro.com/assets/white_papers/wp-PSD2-The-Risks-of-Open-Banking.pdf (visited on 03/30/2022).

[6] Julia Clarke Mariana Dahan Vyjayantu Desai et al. *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation.* Tech. rep. July 2016.

[7] Kristina Yasuda et al. *OpenID for Verifiable Credentials.* Tech. rep. URL: https://openid.net/2022/05/12/openid-for-verifiable-credentials-whitepaper/ (visited on 05/24/2022).

[8] Manu Sporny et al. *Verifiale Credentials Data Model v1.1*. URL: https://www.w3.org/TR/vc-data-model/#core-data-model (visited on 03/29/2022).

[9] Manu Sporny et al. *Verifiale Credentials Data Model v1.1*. URL: https://www.w3.org/TR/vc-data-model/#what-is-a-verifiable-credential (visited on 03/29/2022).

[10] Nancy Albinson et al. *Building digital trust: Technology can lead the way*. Tech. rep. 2019. URL: https://www2.deloitte.com/content/dam/insights/us/articles/6320_Building-digital-trust/DI_Building-digital-trust.pdfhttps://openid.net/wg/fapi/faq/ (visited on 03/31/2022).

[11] Niels van Dijk et al. *Technical exploration Ledger-based Self-sovereign Identity*. Tech. rep. May 2021.

[12] Paul A. Grassi et al. *NIST Special Publication 800-63-3 - Digital Identity Guidelines*. Tech. rep. DOI: https://doi.org/10.6028/NIST.SP.800-63-3. (Visited on 05/02/2022).

[13] Christopher Allen. *The Path to Self-Sovereign Identity*. URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (visited on 03/15/2022).

[14] Alex Andrade-Walz. *The Future of Authentication is Self-Sovereign*. URL: https://www.evernym.com/blog/the-future-of-authentication-is-self-sovereign/ (visited on 03/24/2022).

[15] Danske Bank A/S. *Open Banking Documentation*. URL: https://developers.danskebank.com/documentation (visited on 05/10/2022).

[16] European Banking Authority. *Account data required by ASPSP to execute a payment order via a PISP*. URL: https://www.eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4854 (visited on 05/12/2022).

[17] Danske Bank. *Danske Bank - Online Banking*. URL: https://danskebank.dk/en/personal/tools/e-banking/online-bankinghttps://danskebank.dk/en/personal/tools/e-banking/online-banking (visited on 05/12/2022).

[18] European Central Bank. *Payment Statistics: 2020*. Tech. rep. URL: https://www.ecb.europa.eu/press/pr/stats/paysec/html/ecb.pis2020~5d0ea9dfa5.en.html (visited on 05/03/2022).

[19] The World Bank. *World Development Report 2021*. Tech. rep. URL: https://wdr2021.worldbank.org/stories/crossing-borders/ (visited on 04/04/2022).

[20] Evernym Blog. *eIDAS 2.0: How Europe Can Define the Digital Identity Blueprint for the World*. URL: https://www.evernym.com/blog/eidas/ (visited on 04/15/2022).

[21] Richard Gendal Brown. *Hvad er D-mærket?* URL: https://d-maerket.dk/om/#:~:text=D\%2Dm\%C3\%A6rket\%20er\%20Danmarks\%20nye,skaber\%20et\%20st\%C3\%A6rkere\%20digitalt\%20Danmark. (visited on 04/02/2022).

[22] Richard Gendal Brown. *Why We Need the Next Generation of Digital Trust Technology*. URL: https://venturebeat.com/2022/03/04/why-we-need-the-next-generation-of-digital-trust-technology/ (visited on 03/31/2022).

[23] Chase for Business. *CA crash course on taking the mystery out of payments*. URL: https://business.chase.com/resources/start/a-crash-course-on-taking-the-mystery-out-of-payments (visited on 04/05/2022).

[24] CardKnox. *The Payments Industry Landscape: What Does it Look Like Today?* Tech. rep. URL: https://2f0gzq466hza2r8os02tcwno-wpengine.netdna-ssl.com/wp-content/uploads/Payment-Landscape-White-Paper-Cardknox-1.pdf (visited on 05/03/2022).

[25] Pranam Codur. *Beyond PSD2*. Tech. rep. URL: https://www.ibm.com/blogs/security-identity-access/wp-content/uploads/2019/01/Beyond-PSD2_Paper.pdf (visited on 04/17/2022).

[26] European Commission. *Digital Identity for all Europeans*. URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en (visited on 04/17/2022).

[27] European Commission. *Electronic Identification*. URL: https://digital-strategy.ec.europa.eu/en/policies/electronic-identification (visited on 04/10/2022).

[28] European Commission. *What is personal data?* URL: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en (visited on 05/02/2022).

[29] Signicat Developer. *Level of assurance and authenticators*. Tech. rep. URL: https://developer.signicat.com/enterprise/identity-methods/mitid/loa.html#possible-authenticator-combinations (visited on 04/11/2022).

[30] CEF Digital. *Improving the user experience of cross-border eID*. URL: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2019/07/02/Improving+the+user+experience+of+cross-border+eID (visited on 04/10/2022).

[31] Digitaliseringsstyrelsen. *11 brokere i MitID*. URL: https://digst.dk/it-loesninger/mitid/nyheder-om-mitid/nyheder-fra-2021/11-brokere-i-mitid/ (visited on 04/11/2022).

[32] Digitaliserinsstyrelsen. *Fremtidens infrastruktur for digitale identiteter i Danmark*. Tech. rep. Oct. 2019. DOI: https://digst.dk/media/20382/infrastrukturbeskrivelse-v31_oktober-2019.pdf.

[33] Ben Dwyer. *Credit Card Processing: How it Works*. Apr. 2020. URL: https://www.cardfellow.com/blog/how-credit-card-processing-works/ (visited on 05/03/2022).

[34] Ebanx. *Acquiring vs. Issuing Banks: What Are the Differences?* URL: https://business.ebanx.com/en/resources/payments-explained/acquiring-bank (visited on 04/05/2022).

[35] eIDAS Expert Group. *European Digital Identity Reference and Architecture Framework*. Tech. rep. Feb. 2022.

[36] Digitaliserinsstyrelsen og Fianans Danmark. *Om MitID*. Tech. rep. Oct. 2021. DOI: https://www.mitid.dk/media/4fxnnj0e/om-mitid-whitepaper.pdf.

[37] GSMA. *Digital Identity: What to expect in 2018*. URL: https://www.gsma.com/identity/digital-identity-expect-2018 (visited on 04/11/2022).

[38] Daniel Hardman. *What are Verifiable Credentials?* URL: https://www.evernym.com/blog/gentle-introduction-verifiable-credentials/ (visited on 05/27/2022).

[39] Ed D. Hardt. *The OAuth 2.0 Authorization Framework*. URL: https://datatracker.ietf.org/doc/html/rfc6749 (visited on 03/25/2022).

[40] Authelete Inc. *A Comprehensive Commentary on Financial-grade API*. Tech. rep. (Visited on 05/02/2022).

[41] Takahiko Kawasaki. *Introduction to FAPI*. URL: https://fapi.openid.net/2020/02/26/guest-blog-financial-grade-api-fapi-explained-by-an-implementer/ (visited on 03/18/2022).

[42] Kheng-Leong Tan Chi-Hung Chi Kwok-Yan Lam. "Analysis of Digital Sovereignty and Identity: From Digitization to Digitalization". In: arXiv, Feb. 2022. DOI: https://doi.org/10.48550/arXiv.2202.10069.

[43] Lissi. *eIDAS and the European Digital Identity Wallet: Context, status quo and why it will change the world*. URL: https://medium.com/@lissi-id/eidas-and-the-european-digital-identity-wallet-context-status-quo-and-why-it-will-change-the-2a7527f863b3 (visited on 03/30/2022).

[44] Mattr. *Financial Services Whitepaper - The Critican Need for Digitial Identity and Verifiable Credentials*. Tech. rep. URL: https://cdn.460degrees.com/wp-content/uploads/2020/05/12210518/MATTR_FinancialServices.pdf (visited on 05/11/2022).

[45] Tim Maxwell. *How major credit card networks protect customers against fraud*. June 2021. URL: https://www.bankrate.com/finance/credit-cards/major-credit-card-networks-protect-against-fraud/ (visited on 05/03/2022).

[46] Medium. *Credit Card Processing - A Definitive Guide*. URL: https://medium.com/m2p-yap-fintech/credit-card-processing-a-definitive-guide-3aae35c12aef (visited on 04/05/2022).

[47] Safa Mohamed. *Traditional Banking vs. Open Banking: What Is the Verdict?* URL: https://tarabutgateway.com/traditional-banking-vs-open-banking-what-is-the-verdict/#:~:text=Traditionally\%2C\%20within\%20financial\%20services\%2C\%20banks,access\%20at\%20any\%20given\%20time. (visited on 03/20/2022).

[48] Nets. *Two ways of integrating to MitID at Nets*. Tech. rep. URL: https://www.nets.eu/solutions/digitisation-services/identification/Pages/MitID.aspx (visited on 04/11/2022).

[49] Okta. *The Okta Digital Trust Index: Exploring the human edge of trust in a fast-changing world*. Tech. rep. URL: https://www.okta.com/uk/resources/whitepaper-the-digital-trust-index/ (visited on 04/29/2022).

[50] OpenID. *Financial-grade API (FAPI) WG*. URL: https://openid.net/wg/fapi/ (visited on 04/08/2022).

[51] Pinar Ozcan. "The API Economy and Digital Transformation in Financial Services: The case of Open Banking". In: *SSRN Electronic Journal* (Jan. 2016). DOI: DOI:10.2139/ssrn.2975199.

[52] The European Parliament. *eIDAS Regulation*. URL: https://www.eid.as/ (visited on 03/08/2022).

[53] The European Parliament and the Council of the European Union. *Regulation (EU) No 910/2014 of the European Parliament and of the Council*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910 (visited on 04/10/2022).

[54] Marijana Petrovic. "PSD2 Influence of Digital Banking Transformation: Banks' Perspective". In: *Journal of Process Management New Technologies* (Jan. 2020). DOI: DOI:10.5937/jouproman8-28153.

[55] YouGov PLC. *The future of financial services: A global exploration of evolving trends in the financial services industry*. Tech. rep. Mar. 2022. URL: https://commercial.

yougov.com/rs/464-VHH-988/images/YouGov-Global-Future-of-Financial-Services-Report-2022.pdf (visited on 04/17/2022).

[56] Manasi Gyanchandani Priyank Jain and Nilay Khare. "Big data privacy: A technological perspective and review". In: *Journal of Big Data* 3 (25) (Nov. 2016). DOI: 10.1186/s40537-016-0059-y.

[57] European Union Publications Office. *Commission Delegated Regulation (EU) 2018/389 on supplementing Directive (EU) 2015/2366*. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex\%3A32018R0389 (visited on 03/04/2022).

[58] European Union Publications Office. *Revised rules for payment services in the EU*. URL: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366 (visited on 03/04/2022).

[59] Raisin.co.uk. *Open Banking Explained*. URL: https://www.raisin.co.uk/banking/open-banking/ (visited on 03/16/2022).

[60] Threat Ravens. *When PSD2 Opens More Doors: The Risk of Open Banking*. Tech. rep. URL: https://threatravens.com/ayttgcjwbsk/ (visited on 03/17/2022).

[61] A. Preukschat D. Reed. *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*. 2021st ed. Manning Publications Co., 2021, p. 387.

[62] Tonia E. Ries. *Edelman Trust Barometer 2021: Global Report*. Tech. rep. URL: https://www.edelman.com/trust/2021-trust-barometer (visited on 04/29/2022).

[63] Jeffrey Ritter. *Digital Trust*. URL: https://www.techtarget.com/whatis/definition/digital-trust (visited on 05/12/2022).

[64] Abilio Rodrigues. *What is an AISP and why are they so important for open banking?* URL: https://nordigen.com/en/blog/what-aisp-important-open-banking/ (visited on 05/13/2022).

[65] Viktoria Rudenko. *Standardising PSD2 API: a key for unlocking the PSD2 Trilemma?* URL: https://www2.deloitte.com/nl/nl/pages/financial-services/articles/

standardising-psd2-api-a-key-for-unlocking-the-psd2-trilemma.html (visited on 03/09/2022).

[66] Signaturgruppen. *Net MitID Broker - Technical reference for service providers*. Tech. rep. Oct. 2020. URL: https://broker.signaturgruppen.dk/application/files/6715/8505/5685/Nets_MitID_Broker_Technical_reference_v._0.9.2.pdf.

[67] Worldpay Editorial Team. *Address verification service improves online payment security*. July 2019. URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en (visited on 05/03/2022).

[68] Tykn. *Verifiable Credentials*. URL: https://tykn.tech/verifiable-credentials/ (visited on 04/26/2022).

[69] Condy Unger. *Beyond the Swipe: The Inner Workings of Credit Card Processing*. May 2021. URL: https://www.wyomingsbdc.org/biz-tips/beyond-the-swipe-the-inner-workings-of-credit-card-processing/ (visited on 05/05/2022).

[70] European Union. *Types of legislation*. URL: https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en (visited on 04/23/2022).

[71] W3C. *Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations*. URL: https://www.w3.org/TR/did-core/ (visited on 04/26/2022).

[72] A. Giannopoulou F. Wang. "Self-Sovereign Identity". In: *Glossary of Decentralized Technosocial Systems* 10.2 (Apr. 2021), pp. 166–171. DOI: doi.org/10.14763/2021.2.1550.

[73] Olag Watkuska. *What is Open Banking?* URL: https://www.pragmaticcoders.com/blog/what-is-open-banking (visited on 03/20/2022).

[74] European Commission Website. *A Europe fit for the digital age*. URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en (visited on 04/10/2022).

[75] Alexandria White. *Here's the difference between a credit card network and a card issuer.* URL: https://www.cnbc.com/select/credit-card-network-vs-card-issuer-difference/ (visited on 04/05/2022).

[76] Ldap Wiki. *Identity Proofing.* URL: https://ldapwiki.com/wiki/Identity\%20Proofing (visited on 05/02/2022).

[77] Robin Wilton. *Identity and Privacy in the Digital Age.* Tech. rep., pp. 1–18. URL: http://futureidentity.eu/documents/Identity_and_Privacy.pdf.

List of Figures

Appendix A

A.1 Interview guide

A.1.1 Formalities

- Introduction to research topic and goals of the interview
- Ask for permission to record interview and use the data for my research
- My current position as a student and my research background
- My relation to data privacy

A.1.2 Questions

- What role does data privacy play in your organisation?
- What implications does the PSD2 regulation have on your organization?
- What are the most important opportunities and threats?
- In relation to PSD2; which, if any, organizational changes did you. have to make?
- To what extent are users in control of their own data?

- When a user provides their payment information, does this contain data that refers to another user without this user's consent? In this case, who owns the data?
- How important is transparency in the use of personal data in your organization?
- What information is shared with third parties? (in relation to PSD2?)
- How do you work with authorization? (RBAC, ABAC, PBAC)
- What kind of third parties does your customers engage with?
- What kind of scenarios and use cases do you see in your organization?
- What specific scenarios could be changed/disrupted as a consequence of privacy related regulations?
- In your opinion, what is the most important privacy related consequence of PSD2?
- In your opinion, what is the most crucial threats on data privacy?
- In your opinion, is there anything missing in privacy regulations today?

A.2 Interview with Emil, Lead Auditor D-mærket

Notes from the interview

Hvor er vi lige nu ift data privacy, og hvor er vi på vej hen?

Situationen som den er nu, er en hvor der stadig er plads til forbedring inden for privacy, gennemsigtighed og øget ansvarlighed. Det er stadig i mange tilfælde besværligt at overskue og gennemskue hvad der bliver indsamlet af data om en og til hvilke formål.

GPDR i 2018 og Cookie-direktivet har hjulpet noget, og sat bevægelser i gang i den rigtige retning, hvor bevidstheden og ansvarligheden er steget hos både forbrugere og virksomheder. Det var for mange en hård start, men også en effektiv kickstart af opmærksomheden på området. Der er dog stadig et stykke vej endnu for virksomhederne, der stadig (måske forståeligt nok) ser egne interesser før forbrugernes, og stadig i højere grad burde vægte forbrugernes privatliv.

Hvordan påvirker lovgivning efterspørgselen for data privacy hos forbrugerene?

Ny lovgivning der vil styrke privacy generelt er på vej, så pilen peger i retning af mere indsigt og større krav på området. Der en EU-forordning på vej omkring ansvarlig AI, og der en it-sikkerhedslovgivning (NIS2) på trapperne, som også indirekte vil løfte niveauet for privacy, da det (forhåbentlig) vil føre til bedre databeskyttelse. Så vi er slet ikke i tvivl i D-mærket om, at interessen og indsigten fortsat vil stige hos både virksomheder og forbrugere.

Vi ser da også en stigende efterspørgsel fra forbrugere på privacy og ansvarlig dataanvendelse, og det kan ligeledes mærkes hos virksomhederne. Tal fra DI, der formentlig bliver offentliggjorte i løbet af foråret, viser at mere end halvdelen af SMV'erne oplever efterspørgsel eller gevinst i at arbejde etisk med data.

Hvordan arbejder I med data privacy hos D-mærket?

D-mærket hjælper virksomheder med at få indsigt i deres ansvarlighed inden for dataanvendelse, deres it-sikkerhed og dataetiske forhold i deres virksomhed - og privacy er indlejret flere steder i de tre områder. Vi arbejder ud fra 8 kriterier som du kan læse om her (https://d-

maerket.dk/kriterier/) hvor kriterierne 5-7 arbejder direkte med at implementere privacy (bl.a. minimering og brugerkontrol), og 1-4+8 stiller krav der styrker privacy indirekte. Ved at klikke på et kriterie kan du anmode om vores adgang til vores selvevalueringsværktøj, hvis du vil gå i dybden med kriterierne.

Oplever I stor interesse hos virksomhederne for at blive certificeret med D-mærket?

Vi oplever en stor interesse for D-mærket, og vores kendskab blandt SMV'er (der er vores målgruppe) er på 20% siden vores lancering i slut-september, og vi har været/er i direkte kontakt med mere end 300 virksomheder. Det er tal vi er tilfredse med, men kendskabet og antallet af D-mærkede virksomheder skal selvfølgelig stige markant herfra for for alvor at forbedre privacy og ansvarlig dataanvendelse.

Hvordan evaluerer I dataminimering, brugerkontrol og dataetik?

Vi tjekker konkret på dataminimering, brugerkontrol og dataetik når en virksomhed anmoder om tilsyn, hvilket er påkrævet for at kunne bryste sig af D-mærket. Inden da er der tale om en selvevaluering i virksomheden, som indgrupperes efter dens størrelse og scope. Dataminimering tjekkes kun i tilfælde af at virksomheden udvikler software, hvorimod dataetik og brugerkontrol tjekkes hos næsten alle virksomheder. Dataetik er indlejret mange af vores kriterier - bl.a. i kriterie 5 om brugerkontrol - men fremstår også selvstændigt i kriterie 8 som et refleksionspunkt.

A.3 Interview with Mogens Rom Andersen, Lead Architect MitID

Notes from the interview

Ift til PSD2, hvilke muligheder og trusler ser du i Europa ved at åbne økosystemer op for tredje part?

Der er ikke meget konkurrence i den finanasielle sektor, hvis vi kigge på Danmark, eftersom vi ikke har så mange banker i Danmark. Lovgivningen er målrettet EU som helhed, så den addresserer den manglende konkurrencemulighed i EU. Problemet ligger i implementeringen af de her API'er, som skal give adgang til data. Nogen skal implementere noget ovenpå API'er, som skal give den her sikkerhed.

Interviewee: For at vi lige for scopet området; i hvilken kontekst kigger du på data privacy i den finansielle sektor?

Det skal forstås i den kontekst, at jeg kigger på forskellige frameworks der eksiterer ift digital data wallet of self-sovereign identities. ift at minimiere data disclosure og informeret consent til en bruger. Det, jeg forstår med de her API'er er, at de ikke nogen mulighed for, at man som bruger, kan meget klart differentiere mellem hvad det er for noget data, man giver videre til en tredjepart.

Det er det, som eIDAs forsøger at gøre. At give brugeren mulighed for at selv at bestemme hvilken data, bankerne skal have. Brugere skal authentificere sig gennem PSD2, det skal væer et krav til bankerne. PSD2 er ikke være end eIDAs. Det er den her lovgivning, som ligger et lag oven på en API som privat virksomhed. Det er nødt til at være national eller EU lovgivning.

Ser du nogle områder i eIDAs lovgning, som kunne være bedre eller skarpere formuleret, eller skarpere skåret?

EU Wallet eIDAs er en forordning, dvs den har lovgivningsmæssigt kraft i alle EU lande. Den har en meget skarp privacy formulering. Det er brugerens privacy rettigheder, som er i

centrum. Bankerne vil derfor være forpligtiget tli at tage imod betalinger fra brugere, som gør brug af EU wallet. Ellers skal der laves noget national lovgivning, som jeg ikke tror er realistisk. PSD2 er fremsat ift hvidvaskning og know your customer (KYC), hvorimod EU Wallet handler om at brugeren selv bestemmer hvilke attributter, der skal videregives til bankerne. De kan også gøre brug af pseudonymer, hvor bankerne er nødt til at tage stilling til om de vil have de her kunder. Ellers går de nok bare et andet sted hen. Det handler om at presse bankerne kommercielt.

Hvad tænker du om hvordan lovgivningen er udformet? Skal det være rammebetingelser eller meget konkrete krav til hvordan det her skal implementeres i virksomheder? Virksomheder er jo forskellige, og specielt i en digital kontekst med tredjepartsudbydere.

I eIDAs er selective disclsoure meget stramt beskrevet. I Danmark idag har vi et centralt styret system, hvor man har portaler, og data flyder mellem myndigheder og tjenesteudbydere, som giver brugere adgang til deres data. Det man ønsker at gøre, er at give brugerene deres data i en wallet, så de selv er istand til at styre med hvem og i hvor høj grad de bliver delt. Problemet er, at man antager, at brugere er i stand til at tage en informeret beslutning. Meget svindel går ud på, at brugere narres til at frigive oplysninger om dem selv. Der er også nogle brugere, som frigiver oplysninger mod betaling. Der er nogle brugere, som ikke er i stand til at træffe en informeret beslutning, da de ikke har informationerne til at gøre det. De centrale systemer, vi har i Danmark beskytter brugeren i den kontekst mod at lave fejl. Den beskyttelse kunne forsvinde med en data wallet, eftersom man som bruger selv gav samtykke. Som bruger kan man vælge ikke at bruge data wallet, men i stedet bruge det centrale system. Ift til bankerne er brugerme meget beskyttet, men et kan måske komme til at ændre sig med brugen af en data wallet. Nu har du jo selv mere ansvar, så skal du måske selv betale mere ift selvrisiko.

I forlængelse af eIDAs og informed consent, hvor man kan minimere hvilket data, der bliver givet videre til banken - er det bredt formuleret? Er der nogle meget

klare rammer for, hvordan det skal kommunikeres til brugeren? Hvordan ved man som helt almindelig bruger, hvad det er for noget data jeg giver videre, og hvad kan konsekvensen ved at videregive data være?

Jeg tror, og det her er et udtrykt for min egen personlige holdning, at den helt brede del af befolkningen vil være i stand til at tage vare på deres data og ikke uhensigstmæssigt videregive den. Der er måske en større gruppe i samfundet, som ikke vil være i stand til det.

Ift til bankerne, så er know-your-customer processmæssigt lagt ud til bankerne, hvor de sætte gærdet lavest. Know-your-customer er processmæssigt lagt ud til bankerne, hvor de som virksomhed har en interessee i at vide så meget som muligt om deres kunder og hvordan de skal håndteres ift svindel og hvidvaskning. Så det er et trade-off.

Hvad ser du som de største trusler mod data privacy ift hvor, vi er idag?

Den største trusel, som jeg ser det, er sociale medier. Spørgsmålet er, hvor modne folk er til at vide, hvad de gør. De gør data tilgængeligt for verden, og risikerer derfor, at verden bruger det mod én.

Hvad er den vigtigste privacy relaterede konsekvens af PSD2?

Konsekvensen af at åbne økosystemer er mere svindel. Bankerne har et godt og tæt samarbede på kryds og tværs for at minimere svindel. Der vil komme mere svindel, når de har mindre kontrol over bruger data, hvilket kunderne kommer til at betale prisen for. Det kan ikke være anderledes.

A.4 Interview with Jakob Andkjær, Product Owner Financial Services

Transcribed interview

Interviewer will be denoted "I" and respondent will de denoted "R" in the following.

Interviewer: På baggrund af din erfaring, vil du sætte nogle ord på, hvad der sker i den finansielle sektor i EU?

Respondent: Der sker en masse ting, og på sin vise synes jeg ikke der sker så meget. Der er nogle store spillere, nogle store systemer og processer, der er på plads og som gør rigtig mange ting. Det handler meget om stabilitet og at leve op til de forventninger, der er. Det gør de her systemer i høj grad. Så kan man sige, om de er rigtige for det samfund vi måske forestiller os, vi gerne vil leve i. Det er måske ligeså meget en politisk diskussion, det er jo også der den her regulering (PSD2) kommer fra. Selv synes jeg, det er særligt velkomment. Jeg synes, at den her regulering i nogen grad åbner op for øget konkurrence til gav for forbrugeren, til gave for samfundet. For at skabe bedre... skabe arbejdspladser, skabe, jeg vil ikke sige teknologiforspring, men i hvert fald muligheden for at tek i højere grad kan innovere i den finaniselle sektor.
Interviewer: Fordi der bliver skabt en... formålet med PSD2 var også der skulle innoveres, at forbugere skulle have tillid til de har tredje parts udbydere, fordi de skulle være underlagt noget regulering, fremfor at have mulighed for at have en usikker adgang til data.

Responsdent: Ja, men selvfølgelig er der noget regulering der, du skal jo fx registrere dig som en PISP eller AISP, men meget af det er jo stadigvæk AISPSP'en som bærer traditionelle liability på transaktionerne, eksempelvis på transaktionerne, som du jo også gør i dag.
I: Det tænker jeg også, de fremadrettet vil gøre. Tror du, at de traditionelle bank institutioner føler sig, øh, deres forretningsmodel bliver truet, eller at deres ejerandel i markedet bliver truet?

R: Jeg tror, de er opmærksom på det. Kagen, der hedder betalinger er rigtig, rigtig stor. Den vokser, øh, globalt set måske mere i Asien og der er nogle forskellige grene af det. Men generelt set så vokser betalingerne. En kæmpe del af bankernes indtjening idag, en ret stor del, den vokser selvfølgelig også meget det lave rente niveau. Det gør også at der er et ben, dér er forvundet dér på lån, eller i hvert fald blevet væsentlig mindre, men antallet af betaling stiger, ehm, og der er gode indtjeningsmuligheder ehh for mange i hvert fald. Så jeg tror nok de er opmærksomme på, at der kommer nye spillere og at barrieren for at komme i gang er

lavere end den har været før. Men der er også plads til mange.

I: Så indtrykket er, at kagen bliver større?

R: Ja, i en eller anden grad. Jeg tror, den vokser 6 pct om året eller sådan noget. Tror jeg nok, de sidste på år. Det er jo heller ikke fordi, det er voldsomme tal, men der bliver handlet mere og mere, og der bliver købt mere og mere på nettet. Ehm flere og flere micro transaktioner, der er mange ting som holder noget potentiale. Øh, med en øget globalisering som man måske også forventer, at der er mere og mere på tværs af digital tjenester. Og bygge betalinger i andre digitale tjenester, om det så er Facebook eller ehm hvad det er, som også gør at der formegentlig er en vækst i betalinger generelt set.

I: Har du nogle konkrete scenarier eller use cases, som du ser bliver ændret af en strammere lovgivning på privacy området, som man jo også kan sige den her PSD2 har gjort, eller forsøger at gøre i hvert fald?

R: Ja, jeg ved ikke, er den så meget stramme end det, der var i forvejen?

I: Den har jo... Det den slår sig på, er det her med tillid, men også at der skal være, hvad hedder det, Stronger Customer Authentication, på flere transaktioner.

R: Ja, så SKA, som man kalder det på dansk, er jo ikke sådan en privacy ting men mere en sikkerhedsting.øhm, PSD2 og Danmarks Lov og betaling (?) indeholder også data paragraffer. Jeg ikke jeg kan huske det, jeg tror, det er 124-125, der omhandler betalinger. Der omhandler eh person data ifb med betalinger. Ehm, men jeg ved ikke om det er noget PSD2 har introduceret, eller ej?

I: Det med 2-faktor?

R: Ja, det er. Men det er mere en sikkerhedsting.

I: Det andet tænker jeg, man er underligt GDPR lovgivningen ift data håndtering

R: Det er du også, men jeg tror at lov om betalinger i andre tilfælde, nu kan jeg ikke huske det juraområde, men hvad skal man sige, er over dér. Og du udveksler også persondata bagscenen mellem penge institutter, når der bliver lavet nogle overførsler. I hvert fald i nogle lande i Europa. Jeg ved, Finland er et eksempel hvor at der bliver sendt data til pengeinstituttet når du overfører til en eller anden virksomhed som udlejer en svedhytte i Finland, så får pengeinstituttet også noget data på, hvem du er som afsender. Det er ikke noget modtageren, virksomheden kan se, men det pengeinstitut får det af compliance (KYC) hensyn. Ehm, så man kan sige overordnet at PSD2 og den regulering tager i nogle tilfælde stokken over GDPR

I: Det er jo meget interessant. Hvem ejer den data i den kontekst?

R: Hvad tænker du i?

I: Når du sender nogle penge, til en modtager og der så er noget data på dig som afsender til en modtager

R: Ja, det ville, det kan jeg måske ikke helt svare på. Det vil være både afsendende pengeinstitut og modtager tror jeg.

I: Modtager

R: Begge dele. De har begge to de samme data.

I: Det er en meget interessant diskussion især med det her privacy og finanisiel sektor. Ehm, hvad er, hvad tlnker du er vores generelle forventninger til de her finansielle systemer? Er

der en udpræget tillid? Altså sådan digitalt? Digital tillid?

R: Det tror jeg til mange. Ehm, til mange spillere i Danmark. I Europa. Det er også meget lande specifikt, det er der også i Tyskland. Som jo egentlig også er et veludviklet samfund, industrielt land, på mange måder. De har et helt andet forhold til penge, til banker, til institutioner. Kontanter er meget mere udpræget, end det er i Danmark. Også selv i Finland som man tænker er et meget, et nordisk land, som man tænker Nokia og den slags, men kontanter er også indtil for ganske nylig haft noget helt, har været meget mere udpræget, end det har været i Danmark, Norge og Sverige. Virkelig forskel. Så jeg tror det handler meget om operering. Hvis vi taler om PSD2 som er i Europa, eller EØS er det jo i virkeligheden, for nogle transaktioner. Der er stor forskel på hvordan de gennemsnits person i Spanien opfatter en bank, eller penge institut eller betalingstjeneste ift hvordan måske gør i Danmark som land, som måske er modsætninger.

I: Så det er meget nationalt funderet. Den tillid er på det enkelte pengeinstitut?

R: En blanding sikkert. Jeg tror båder er noget kulturelt, også er der også noget den enkelte udbyder/tjeneste.

I: Hvad tænker af sådan potentielle konsekvenser for data privacy ved det her open banking paradigme? Kan man kalde det. De har åbne økosystemer i finansielle institutioner?

R: På nogle måder er det jo ikke helt åbent. Det er jo stadig forbeholdt en relativ lille skare af TPP'er, ehm. Jeg synes, det er godt, at der er regulering, min egen personlige holdning. Som både handler om datahensyn, individets datahensyn, men også mere generelt. Der er jo andre der jo andre der kan få adgang til den her data og det skal vi selvfølgelig også være reguleret på nogle ordentlige forhold. Og at man som privatperson har mulighed for at vælge hvem har lyst til at det her med. Der er så både lov om betalinger, det er selve betalingen. Den data du lægger ud via ESP (?) funktionalitet. Men derfra er det jo i virkeligheden

GDPR lovgivningen. Så vi kunne godt have et TPP som hiver noget kontodata ud. Der er det PSD2 og de nationale lovgivninger baseret på PSD2, der regulerer den del. Ligeså snart daten er ude. Så vil det typisk være GDPR der regulerer den del. Så hvis det er et regnskabssystem, så er det formegentlig GDPR der regulerer det.

I: Hvad er det egentlig bankerne tænker? Der er man vel interesseret i at minimere hvor meget data man egentlig har - eller generelt?

R: Ja, den rigtige data. Den, der nødvendige data man har et lovmæssigt grundlag for at indsamle og kan bruge til noget fornuftigt. Ikke bare opbevare data bare fordi man kan. Også omvendt også helt sikkert ligger der en eller anden McKinsey rapport i en skuffe, der siger, at data er det nye guld. Og derfor skal man bare indhente den. Jeg tror, at i DK vil jeg gætte på, at man er ret opmærksom på, hvad man indsamler og hvad man bruger den til. Jeg tror generelt ikke at der bliver indhentet data bare fordi så finder vi ud af hvad vi kan bruge den til på et eller andet tidspunkt. Det tvivler jeg på.

I: Fra finansielle institutioner i hvert fald? I hvilket omfang skal man som privat bruger have kontrol over sin egen data i interaktionen med finansielle institutioner? Med banker?

R: Ja... Man kan anskue det på flere forskellige måder. Du har til dels et lad mig kalde det, anti-hvidvask/terror-finansiering/anti-al muligt omgåen af diverse lovgivninger. Skattesvindel. Der giver det mening, synes jeg, at man kan ved hvem man kan med at gøre. I nogen grad tror jeg at the ultimate beneficiary på den her betaling af penge. Det er der selvfølgelig også folk, der kan snyde med. Stråmænd osv. Også er der et andet perspektiv er, at det rager ikke nogen at jeg købte en flæskesteg i fredags fx. Det jeg da have lov til at bruge mine penge på, hvis jeg har lyst til det. Uden at jeg skal føle, at jeg efterlader et eller andet spor for altid af at; du købte flæskesteg den der fredag. Så jeg synes, man kan se lidt af begge dele. Jeg tror, de fleste er enige i at når det er ude i omfattende terror-finansiering, så synes alle nok, at det er en rigtig, eitgi god ide. Men lad os sige, at det er ulovlig overvågning, som

er af nogen som ikke har gjort noget ulovligt eller at der ikke er nogen mistanke om, hvad skal man sige, så er det nok lidt en anden holdning også fra de fleste også mig. Jeg kan se lidt at begge perspektiver. Jeg synes, man skal have lov til at bruge sine penge som man har lyst til. Omvendt så er man også nødt til at have et net der gør, så man ikke finansierer terror eller modtager penge fra diktaturer eller hvad ved jeg. Så det er en lidt svær ting. For det er jo noget rigtig vigtigt

I: Det er jo en afvejning af at du som enkelt individ føler du er i kontrol men også i at bankinstitutioner skal være i kontrol fordi de er kritisk infrastruktur i vores samfund.

R: At de både har et ansvar og en pligt

Appendix B

B.1 TPP Application Documentation

No.	Requirement
1	Business plan
2	Financial Model for 3 year
3	Operational programme
4	IT risk management policy
5	AML/CTF policy
6	Financial crime prevention policy
7	Data protection policy
8	Statistical data collection policy
9	Incident reporting policy
10	Counterparty risk management policy
11	Complaints handling policy
12	Internal audit policy
13	Risk matrix
14	Terms and conditions

Table B.1: TPP Application Documentation requirements [64]

B.2 KYC Verifiable Credential


```
{
"@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
],
  "id": "http://bank.org/credentials/1872",
  "type": ["VerifiableCredential","KYCCredential"],
  "issuer": "https://bank.org/issuers/565049",
  "issuanceDate": "2022-05-08T19:23:24Z",
  "credentialSubject":
 {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "customerOf": {
      "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
      "account": {
      "DOB": "1989-02-01",
      "socialSecurityNumber": "01021989-2332",
      "firstName": "Jane",
      "lastName": "Doe",
      "type": "Checking",
      "accountNo": "XXXX XXXX XXXX 4501",
      }
    }
},

"proof": {
    "type": "RsaSignature2018",
    "created": "2017-06-18T21:19:10Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "https://bank.org/issuers/565049#key-1",
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X
      sITJX1CxPCT8yAV-TVkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUc
      X16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G_zS245-kronKb78cPN25DGlcTwLtj
      PAYuNzVBAh4vGHSrQyHUdBBPM"
   }
}
```


Figure B.1: Verifiable Credential [68] [9]

B.3 KYC Verifiable Presentation


```
{
 "@context": [
   "https://www.w3.org/2018/credentials/v1",
   "https://www.w3.org/2018/credentials/examples/v1"
 ],
 "type": "VerifiablePresentation",
 "verifiableCredential": [{
   "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
   ],
  "id": "http://bank.org/credentials/1872",
  "type": ["VerifiableCredential","KYCCredential"],
  "issuer": "https://bank.org/issuers/565049",
  "issuanceDate": "2022-05-08T19:23:24Z",
  "credentialSubject": {
   "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
   "customerOf": {
     "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
     "account": {
     "firstName": "Jane",
     "lastName": "Doe",
     "type": "Checking",
     "accountNo": "XXXX XXXX XXXX 4501",
     },]
   }
 },
 "proof": {
   "type": "RsaSignature2018",
   "created": "2017-06-18T21:19:10Z",
   "proofPurpose": "assertionMethod",
   "verificationMethod": "https://bank.org/issuers/565049#key-1",
   "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X
     sITJX1CxPCT8yAV-TVkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUc
     X16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G_zS245-kronKb78cPN25DGlcTwLtj
     PAYuNzVBAh4vGHSrQyHUdBBPM"
 }
}],
"type": "RsaSignature2018",
   "created": "2018-09-14T21:19:10Z",
   "proofPurpose": "authentication",
   "verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec21#key-1",

   "challenge": "1f44d55f-f161-4938-a659-f8026467f126",
   "domain": "4jt78h47fh47",
   "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..kTCY
   t5SjkdsghSGDJHGh AV-TVIw5EWutusi01-pQy7UJiN5mgEEkjhsdHJKHSDUIHIv6JHSDb
   JPÆQq_PbChMqsLfRoskdjfhjD-WkdfhuX16dlskjdf-kronb7Pjt3brk-BuQ-sdjslkdfj
   kjf342lkjsdkj4vGHsrHUGTwLPjAnkb78"
   }
 }
```


Figure B.2: Verifiable Presentation [68] [9]

B.4 Identity Verifiable Credential


```
{
"@context": [
 "https://www.w3.org/2018/credentials/v1",
 "https://www.w3.org/2018/credentials/examples/v1"
] ,
   "id": "http://gov.org/credentials/1272",
   "type": ["VerifiableCredential","IdentityCredential"],
   "issuer": "https://gov.org/issuers/465049",
  "issuanceDate": "2021-05-08T19:23:24Z",
  "credentialSubject":
{
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "eID": {
      "id": "did:example:b286e12ec21ebfeb1f712ebc6f1",
      "healthInsuranceCertificate": {
      "socialSecurityNo": "01021989-2332",
      "firstName": "Jane",
      "lastName": "Doe",
         "address": {
           "street": "Frederikskaj",
           "houseNo": "10",
           "zipCode": "2450",
           "city": "Copenhagen",
         }
      }
   }
},
"proof": {
 "type": "RsaSignature2018",
 "created": "2016-06-18T21:19:10Z",
 "proofPurpose": "assertionMethod",
 "verificationMethod": "https://gov.org/issuers/465049#key-1",,
 "jws": "heyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X
   sITJX1CxPCT8yAV-TVkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUc
   X16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G_zS245-kronKb78cPN25DGlcTwLtj
   PAYuNzVBAh4vGHSrQyHUdBPPM"
   }
}
```


Figure B.3: Verifiable Credential issued by a government institution [68] [9]

B.5 Identity Verifiable Presentation


```
{
 "@context": [
   "https://www.w3.org/2018/credentials/v1",
   "https://www.w3.org/2018/credentials/examples/v1"
 ],
 "type": "VerifiablePresentation",
 "verifiableCredential": [{
   "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
   ],
  "id": "http://gov.org/credentials/1272",
  "type": ["VerifiableCredential","IdentityCredential"],
  "issuer": "https://gov.org/issuers/465049",
  "issuanceDate": "2021-05-08T19:23:24Z",
  "credentialSubject": {
   "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
   "eID": {
     "id": "did:example:b286e12ec21ebfeb1f712ebc6f1",
     "healthInsuranceCertificate": {
     "firstName": "Jane",
     "lastName": "Doe",
           "address": {
             "street": "Frederikskaj",
             "houseNo": "10",
                    "zipCode": "2450",
       "city": "Copenhagen",
     }
     },]
   }
 },
 "proof": {
   "type": "RsaSignature2018",
   "created": "2016-06-18T21:19:10Z",
   "proofPurpose": "assertionMethod",
   "verificationMethod": "https://gov.org/issuers/465049#key-1",
   "jws": "heyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X
     sITJX1CxPCT8yAV-TVkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUc
     X16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G_zS245-kronKb78cPN25DGlcTwLtj
     PAYuNzVBAh4vGHSrQyHUdBPPM"
   }
 }],
 "type": "RsaSignature2018",
   "created": "2018-09-14T21:19:10Z",
   "proofPurpose": "authentication",
   "verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec21#key-1",

   "challenge": "1f44d55f-f161-4938-a659-f8026467f126",
   "domain": "4jt78h47fh47",
   "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..kTCYt
   5SjkdsghSGDJHGhAV-TVIw5EWutusi01-pQy7UJiN5mgEEkjhsdHJKHSDUIHIv6JHSDbJPÆ
   Qq_PbChMqsLfRoskdjfhjD-WkdfhuX16dlskjdf-kronb7Pjt3brk-BuQ-sdjslkdfjkjf3
   42lkjsdkj4vGHsrHUGTwLPjAnkb78"
 }
```


Figure B.4: Verifiable Presentation for merchant [68] [9]