Towards cross-border interoperable digital identity in electronic banking

Artem Poryadin
(artem.poryadin@hig.no)

Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2011

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Towards cross-border interoperable digital identity in electronic banking

Artem Poryadin

1st July 2011

Abstract

For years, banks have been required to secure their online banking services and manage number of customers' identities, addressing security and privacy issues. Identity management systems facilitate cost-effective and secure way of managing these identities. However, the heterogeneous identity landscape, when every bank employs its own "siloed" identity infrastructure, causes many obstacles for development and popularization of online-banking services along with increasing costs of managing identities. The emergence of identity management solution accepted by multiple parties and operating cross-border and cross-organization can lead to enormous benefits for both banks and their customers.

The research is comprised of two multifaceted multiple-case studies of current identity management solutions in Europe, Norwegian BankID, and current cross-border interbank systems such as VISA, SWIFT, and IdenTrust. During the research, we identified the fundamental factors influencing identity management system acceptance and adoption rates. Furthermore, the analysis of socio-economics, success factors, explicit and implicit requirements of previously mentioned solutions was the base for designing cross-border and multi-party accepted identity management system for e-banking with the goal of saving costs and simplifying market. It was found that cultural background and public trust in identity provider predefine security requirements and, along with ease of implementation, usability, interoperability and exploitation in "a must" applications, facilitate adoption to a great extent. The economical consideration and business aspects showed, among other findings, that in general identity management system should be considered as a two-sided platform leveraging interests of relying parties (service providers) on one side and identity-holders on the other. Finally the results were leveraged by designing prototypes of business model and architecture, adhering to the identified success principles of identity management systems.

The project establishes a solid ground and a roadmap for future research in cross-border identity management; it contributes to better understanding of digital identity in terms of driving factors, economic and cultural implications.

Keywords

Electronic Banking, Digital Identity, Identity Management, Cross-border systems, Interoperability, BankID, Economics, Business Model, Trust, Success Factors, Case Study Research

Preface

> *"The purpose of life is not to be happy.*
> *It is to be useful, to be honorable, to be*
> *compassionate, to have it make some*
> *difference that you have lived and lived well."*
>
> — Ralph Waldo Emerson

Our society and everyday life are getting more digitalized by the hour. Back in days, it was hard to imagine that people could communicate and share their life moments not seeing each other, it's possible now with social networks. There is no need to go to a shop because you can buy almost everything online in few clicks. Even banks and governments are now offering their services electronically. Indeed, we are lucky to witness the unique era when more and more services and traditionally offline relationships are moving to online environment. So do people, being represented online by means of digital identities. Secure and trusted digital identities have become and will continue to get important for protecting privacy, securing critical infrastructures and the cyberspace.

The story of this project began in August 2010 when me and my classmates were asked to choose a topic for the master thesis. The field of identity management has always been interesting for me and I quickly decided to go in this direction. Driving by thought to elaborate on something especially valuable and useful for the society, I started preliminary research to identify the topic. I was looking for something interesting and able to make a difference, something beyond simple researches comprised of an ordinary experiment or a simple survey. Few months later after number of discussions with Prof. Dr. Bernhard M. Hämmerli we identified such topic with a great potential impact, but also representing a significant challenge. In the beginning of year 2011 we started this research project, which eventually resulted in one of my most challenging and interesting projects. The qualitative researches and in particular multiple-case studies are usually chosen if there's a lot of time to make this kind of research. At the same time, the qualitative research seemed to the most suitable to address the research problem in the most effective way. Ultimately, I decided to gave up time and work more over the changing the research method and potentially trade-off the quality. As a consequence, this project generated results for three different papers, one of which is already written and two others are being written now for publication.

Writing a master thesis and elaborating on something new and challenging, you often feel overwhelmed by the amount of work needed to be done in a relatively short period of time. Behind the name on the front page, there are people who helped and supported me in the course of my work and made possible to successfully get to the finish line.

Most of all, I want to thank my supervisor Prof. Dr. Bernhard M. Hämmerli for hours of useful discussions, a number of contacts, encouragement, guidance, and support from the first to the final step. During the entire period, he has shown the great interest in my work, always been available for discussions and motivational talks, and taught me how to become a good researcher kindly correcting and advising me. I want also to thank my

co-supervisor Dr. Patrick Bours, who showed interest and agreed to support me in this project.

I want to express my gratitude to all my colleagues and friends at Gjøvik University College for being interested in my work, and providing me with valuable feedback and comments. I appreciate the contributive feedbacks from all commentators and, especially, from Rolf Prantl. Special thanks go to my friends Jose Mario Perez Velasquez who was enthusiastic about my project and promoted my work by writing an article about it, and Pavel Storozhuk-Bozhenov who was motivating and supporting me during the course of my work, and also helping me with proof-reading.

Finally, I would like to give my heartiest thanks to my family and friends for all the motivation I have got, and for helping and backing me up during this work.

Artem Poryadin, 1st July 2011

List of Figures

List of Tables

List of Abbreviations

EBICS	Electronic Banking Internet Communication Standard
EBIMS	Herein, the EBIMS stands for Electronic Banking Identity Management System and is used for simplicity, replacing the phrase cross-border interoperable digital identity management system for electronic banking services
ENISA	European Network and Information Security Agency
ID/IdM/IdMS	Identity / Identity Management / Identity Management System
IdP	Identity Provider
KYC	Know Your Customer policy
NBN	Norwegian Birth Number (fødselnummer in Norwegian)
NSTIC	U.S. National Strategy on Trusted Identities in Cyberspace
OIX	Open Identity Exchange
PET	Privacy Enhancing Technology
PKI	Public Key Infrastructure
RP	Relying Party
SOA	Service Oriented Architecture
SSN	Social Security Number
SWIFT	Society for Worldwide Interbank Financial Telecommunication

Contents

1 Introduction

This chapter introduces the topic covered in this thesis, describes existing problems needed to be addressed as well as research questions. Following justification, motivation and benefits highlight the importance of solving the problems. In addition, claimed contribution of the thesis and methodology used to achieve these results are covered. The thesis structure is outlined in the end of current chapter.

1.1 Topic covered by the project

The more financial services are offered online, the more society depends on strong security of these services. Electronic banking is one of such services offered by almost every bank. It's hard to find a person who doesn't use electronic banking services today. The convenience of electronic banking along with its efficiency in saving time and money are highly appreciated by both financial institutions and their customers. However, as any other critical service, electronic banking requires a high level of security. In particular, a financial institution has to assure that its services are accessed by the right customer, in other words customer should be identified and authorized properly to use the services such as electronic banking, for example. In real-life "offline" world a customer can identify itself visiting its bank institution, but in online environment entity is represented through the medium called digital identity.

For years, banks have been required to secure their online services by various regulations, standards and best practices. Today, a regular bank offering electronic banking services has to manage a lot of customers' identities and address related issues in the way of securing their electronic business processes. Identity management systems are intended to facilitate cost-effective and secure way of managing these identities for banks, but not always for customers. Heterogeneous identity "ecosystem" in EU, when every bank employs its own "siloed" identity infrastructure, causes many obstacles in a way of development and popularization of online-banking services along with increasing costs of managing such identities for both banks and their customers.

1.2 Problem description

Today, a regular banking customer usually has accounts in more than one bank, has to remember all the passwords and take care of all one time password tokens (s)he has in order to get access to online banking facilities. The approach is unusable, challenging, often expensive (as for multinational organizations) and can potentially undermine security by a lack of password managing. This creates a significant threat referred to as ID theft. A solution need to be found in order to mitigate the risk of ID theft and increase overall usability level as well.

Identity management procedures and routines, such as in-time provisioning and deprovisioning of identities or entitlements, are costly operations. All the more, switching banks by a customer creates additional problems for the bank because it increases the cost of identity management along with the amount of "paper work". An interoperable, sound identity would allow additional cost-savings for banks.

Lack of interoperable and multi-party accepted digital identity is one of biggest obstacles in a way to developing of e-trade in a global context. Today, the most common way used to perform payments in e-trade sector is either credit card or a kind of e-cash (e.g. PayPal). Often, it's not secure enough and sometimes not the most convenient way to perform payments. In fact, an interoperable identity could be used to perform such payments directly instead of using a credit card or e-cash.

Yet another issue is usage of identity. Today, identities are mainly used to control access to electronic banking services. However, a number of potential applications go far beyond the one use case. For example, the Norwegian BankID showed that such an interoperable identity may successfully provide digital signature service, be used to get access to other financial and governmental services, or serve as a payment option. Nevertheless, it requires to reconsider related security & privacy issues which may be addressed through application of privacy enhancing and user-centric technologies.

Although various tries to develop a universal identity infrastructure had place only few of them (e.g. credit cards) became interoperable and multi-party accepted in a cross-border and even global context. Why do some IdM systems succeed while others don't? A research of implicit and explicit requirements is, obviously, needed to attain better understanding of the nature of a digital identity and the "ecosystem" required to enable it operates in a cross-border situation and spreads out fast.

Indeed, banks and customers could benefit a lot from multi-party accepted interoperable identity, but often different regulations and standards existing in different countries and regions, traditionally strong competition between banks, various cost of operation of IdM systems, as well as differences in deployed systems and policies call not only for suitable IdM model, but also for an effective business model to address the problems and enable such cross-border identity in e-banking.

1.3 Justification, motivation and benefits

At present time, identity management is multidisciplinary and well-recognized area covering many dimensions such as technical, legal, political, social, cultural, security, economic, and psychological. A lot of companies are involved in various researches in the field and give it the highest priority.

The need for cross-border interoperability of IdM systems is acknowledged on EU level and addressed by number of various research projects. The PARSIFAL project[1] identified the lack of interoperable cross-border identity as one of eight important issues for future research in financial sector. [4, 5, 6] To study the interoperability of identity in Europe different project were started: the large scale SPOCS pilot [7] aims to develop interoperability framework to link various existing eGovernment solutions of EU Member States; the STORK project [8] aims to develop and test common specifications for electronic identity interoperability. Besides, the user-centric approach and necessity in cross-border identity were highlighted in FIDIS[2] project as ones of important open research challenges and further work: "*The duality of IdM between User Centricity and Organisation Centricity is of major importance. Further research in conjunction with practical application in the field (e.g. mergers and acquisitions of companies or enhancing IdMS of (European) states for mutual recognition of eIDs across national borders) is necessary.*" [9]

[1] Protection and Trust in Financial Infrastructures (PARSIFAL) http://www.parsifal-project.eu/

[2] The Future of Identity in the Information Society http://www.fidis.net/

A lack of business model for the cross-border IdM system is recognized by both the financial industry and researchers. In particular, during an industry roundtable discussion organized by Dialogue magazine, five industry experts were asked the following question: "Within the protection framework required for customer-bank-customer information flows (both individual and corporate), are the key remaining challenges to identity management technical, business or legal?" Three respondents believe that all three are equally important, while two others gave the business model higher priority. "*From the perspective that a framework does not exist – not that it should not; just that it does not – the key challenge is business.*" - Wes Wilhelm, senior analyst at Aité Group; "*While I'm sure there are some technical hurdles or challenges, I think business and legal issues are the bigger challenge.*" - Gary Greenwald, CIO of Citi's global transaction services. [10]

The importance of development and research of business models is emphasized in "The State of the Electronic Identity Market: Technologies, Infrastructure, Services and Policies" by European Commission Joint Research Centre. The report considers the lack of business model as one of barriers in the way of development efficient identity ecosystem. The report states that "*the market for eID products and services is fragmented, far from efficient and lacks viable business models. Effective regulation of the personal identity space and its economic externalities requires a clear understanding of how the market for identity functions. But very little is known about emerging identity markets and the business models that support the use of personal identity data in transactions.*" [11] Despite the importance of IdM business models studies, there are very few researches addressing this problem.

A research of implicit and explicit requirements can contribute to general understanding of the nature of digital identity in a cross-border environment, its economics and success factors, as well as "ecosystem" required to enable an identity operates in a cross-border situation.

The emergence of an IdM solution accepted by multiple parties and operating cross-border and cross-organization will lead to enormous benefits for stakeholders such as organizations, consumers, and banks. Cost of management of the identities will be decreased significantly as well as amount of related "paper work". The ability to use single identity to access multiple banks creates great convenience for the customers through easier application processes and increased security. In turn, increased convenience will ultimately lead to better adoption and acceptance, paving the way for new revenue and cost-saving models.

A cross-border interoperable IdM system will give banks opportunities to introduce new value-added services. For example, being multi-party accepted, such IdM system might be used in payment services. The introduction of a new payment option would provide users with more payment options increasing usability and giving opportunities to banks for easier expansion to the market of electronic payments.

Overall the single secure identity landscape would facilitate the opening of markets and removing of barriers. If a regular customer (a person or a company) can access any bank with a single secure ID issued once by his bank or to start new relationships without a need to go to the branch office, it's not just customers who benefits from the system, but also banks. Because banks may offer their product to larger market. For example, a local bank can typically offer e-banking services to customers within the region or the country it operates in, or simply with the customers provided by the bank with an identity to access these services. The interoperable cross-border IdM system would allow to offer services to any customer within the breadth of spread of the solution. For example, assuming that every EU citizen of working age has a bank account and so the ID to access the account, such interoperable IdM system would allow even a local bank to offer its e-banking services to as many as around 300 million people[3]. In turn, every European citizen holding such ID could access almost 7 000 banks in the EU-27[4]

1.4 Research questions

The research questions are as follows:

- Why do some IdM systems succeed while others don't; what are the implicit and explicit requirements enabling cross-border identities?
- How can we use a single identity to access multiple banks and manage multiple bank accounts?
- What can be learnt and adopted from the experience of Norwegian BankID initiative to a larger scale situation such as EU?
- What is the potentially successful business model and architecture that can enable such cross-border interoperable IdM system[5] ?

1.5 Methodology

1.5.1 The research framework

The master's thesis embodies a qualitative socio-economical research conducted in three main stages:

1. Multiple-case study of Norwegian IdM experience put in international context. In particular, the BankID system (the key case) along with the national ID number and its history are studied in comparison to other large-scale IdM models adopted in four selected EU countries: Germany, Austria, Sweden, and Denmark;
2. Multiple-case study of existing cross-border inter-bank systems (Credit Cards and VISA, SWIFT and 3SKey, IdenTrust);
3. Design of prototypes of potentially successful business model and the architecut.

The research framework is depicted in figure 1.

[3] The number of people aged 15-64 years (working age population) is provided according to EU Population Statistics of 2006. This is the rough assumption though, because not all of the people in working age may have a bank account. Additionally, the IdM system needs to be supported by majority of EU banks in order to provide such coverage, which also defines the size of potential market to a great extent.

[4] As of 2009, The overall bank population in the EU-27 was almost 7 000, including 5 000 commercial banks-members of European Banking Federation. [12]

[5] Throughout the thesis the term "successful" is being used as a main pre-requisite for proposed design of the system and the business model. Hence, it's needed to make clear what is meant here by a "success" in application to IdM system. Herein, an IdM system is considered successful if it's accepted by multiple parties, widely-adopted within an application context (e.g. in e-banking), and able to operate efficiently and effectively across borders and organizations.

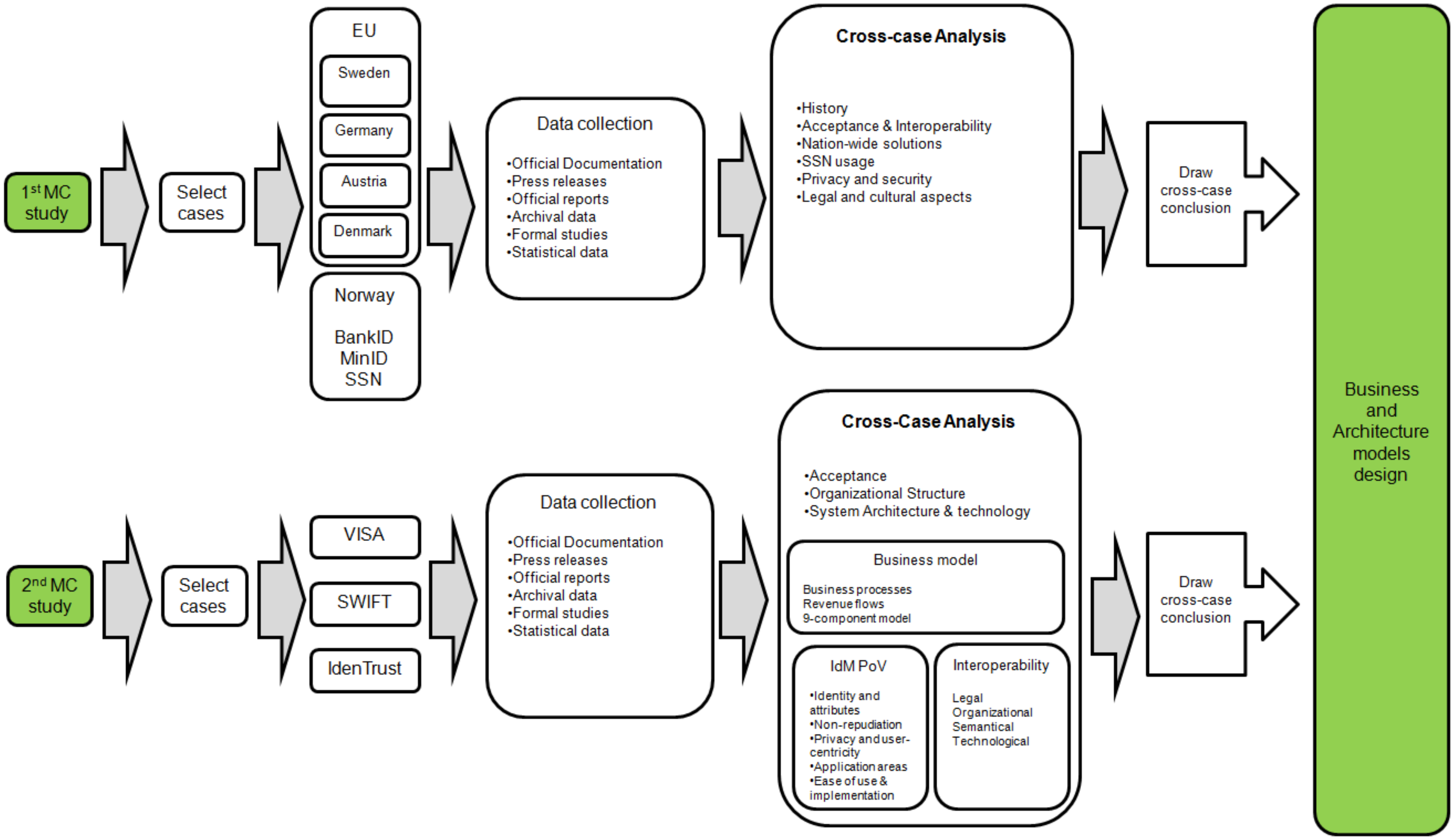


Figure 1: Methodology: The Research Framework

The multiple case study method has been chosen as the one which fits best to the type of research questions and the type and goals of the research itself. In particular, it allows to explore and explain phenomenon and casual links which are too complex for survey or experimental strategies, to describe context in which a phenomena occur and other benefits. The choice of method and design of these studies were done following recommendation given by Robert K. Yin in "Case Study Research: Design and Method (3rd edition)"[13] and Paul D. Leedy in "Practical Research: Planning and Design (9th edition)"[14]. Two multiple-case studies result in a set of requirements and recommendations for identity ecosystem, business model and architecture, which are used in a design stage as input data.

1.5.2 Business Model Analysis and Design

The research implies business model analysis in every case of second multiple case study. Therefore it's worth to describe the methodology for these analyses in more details. The analyses and design follow the same methodology which is suggested by Alexander Osterwalder in "The Business Model Ontology: A Proposition in a Design Science Approach", and since then it has been recognized as an efficient tool for business model analysis & design by number of organizations [15, 16]. Osterwalder defines a business model as "*the rationale of how an organization creates, delivers, and captures value*"[15].

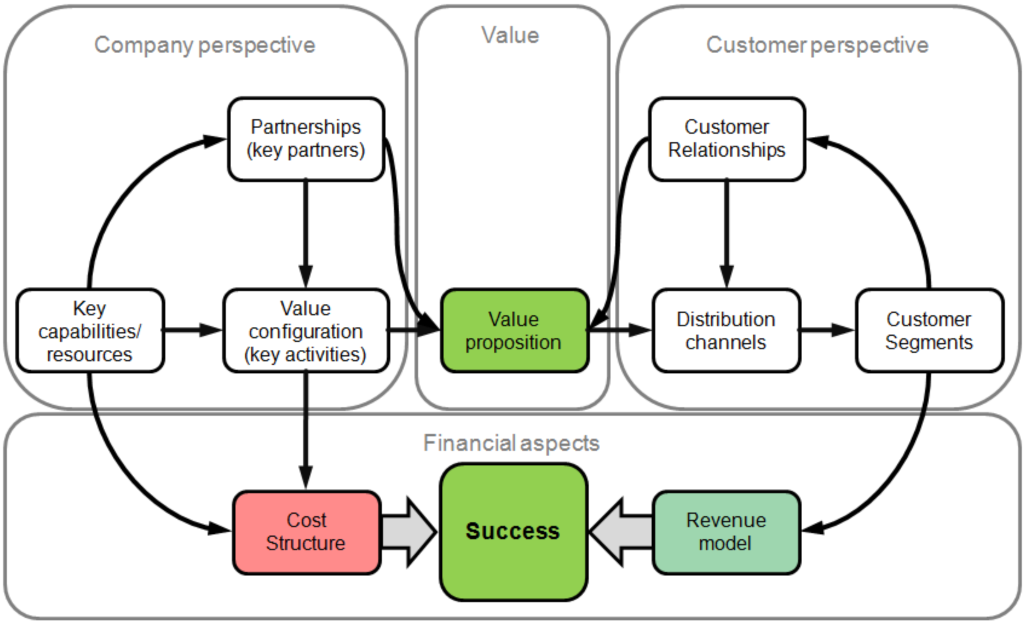


Figure 2: Methodology: The Framework for Business Model Analysis and Design

Typical business model consists of 9 key-components (Fig.2):

- **Customer segments** served by an organization. Key questions: Who is a customer? Whom is a company creating value for?
- **Value Proposition** intended to solve customer problems and satisfy needs. Key questions: What does a company offer and what problems does it solve? What is the value delivered to the customer?

- **Distribution channels** through which the value is delivered. Key questions: How can the value be effectively delivered to a customer?
- **Customer relationships** maintained with each segment. Key questions: Which relationships are required to be, or already established? How costly are they?
- **Revenue model** is the structure of revenue streams derived from successfully offered value proposition. Key questions: What are customers ready and willing to pay for? How do they pay/create revenue streams?
- **Key capabilities/resources** required to create and deliver the value. Key questions: What key capabilities does a company require to offer the value?
- **Value configuration (key activities)** to be performed to create and deliver the value (may include activities of all components: distribution, customer relationships, etc.) Key questions: What key activities does a company require to offer the value?
- **Partnerships (key partners)** needed to effectively generate value. Key questions: What are the key partners?
- **Cost Structure** is the structure of costs resulted from value generation processes. Key questions: What are the main costs, most costly capabilities/activities? [15, 16]

1.6 Claimed contribution

The master's thesis presents a multifaceted analysis of identity management and business models of today's electronic payment, credit card and online banking solutions in order to design potentially successful cross-border and multi-party accepted identity saving costs and simplifying market. The thesis establishes strong ground for future researches in cross-border identity management and contributes to better understanding of the nature of digital identity and its economic and cultural implications. The contribution comprises the following elements:

- Analysis of market forces, economics and business models of identity management along with other related aspects such as usability, security, width and speed of distribution, privacy issues;
- Analysis of explicit and implicit requirements and "ecosystem" needed to enable cross-border and cross-organization identity and its fast dissemination;
- Analysis of the actual situation with IdM in "online-banking" sector and Norwegian BankID initiative;
- Design of potentially successful business model and optimal architecture for IdM system serving cross border and cross organizations;
- Defining roadmap for future research.

1.7 Thesis outline

The thesis has been split into several chapters to align with research framework and to provide transparent and easy-to-follow structure of the report. The research consists of three different stages of different studies where each chapter of main part (Ch.3-5) represents one stage. Multiple-case studies (Ch.3 & 4) end with a section of conclusions highlighting key findings and drawn from cross-case analyses. The general structure of the thesis is depicted in the figure 3.

The chapters outline is as follows:

- **Chapter 1** is the current chapter introducing the research problem and method;
- **Chapter 2** highlights the state of the art in cross-border identity management and identity ecosystem researches with an overview of relevant major EU projects, and U.S. NSTIC strategy;
- **Chapter 3** presents detailed study of Norwegian BankID system, national id numbers as well as historical background. Then the Norwegian experience in IdM put in international context, where it's compared to large-scale IdM solutions in Germany, Austria, Sweden, and Denmark;
- **Chapter 4** presents an analysis of existing cross-border inter-bank systems (Credit Cards and VISA in particular, SWIFT and 3SKey Service, IdenTrust);
- **Chapter 5** describes the design of potentially successful business model and architecture;
- **Chapter 6** concludes the studies with key results;
- **Chapter 7** proposes future work.

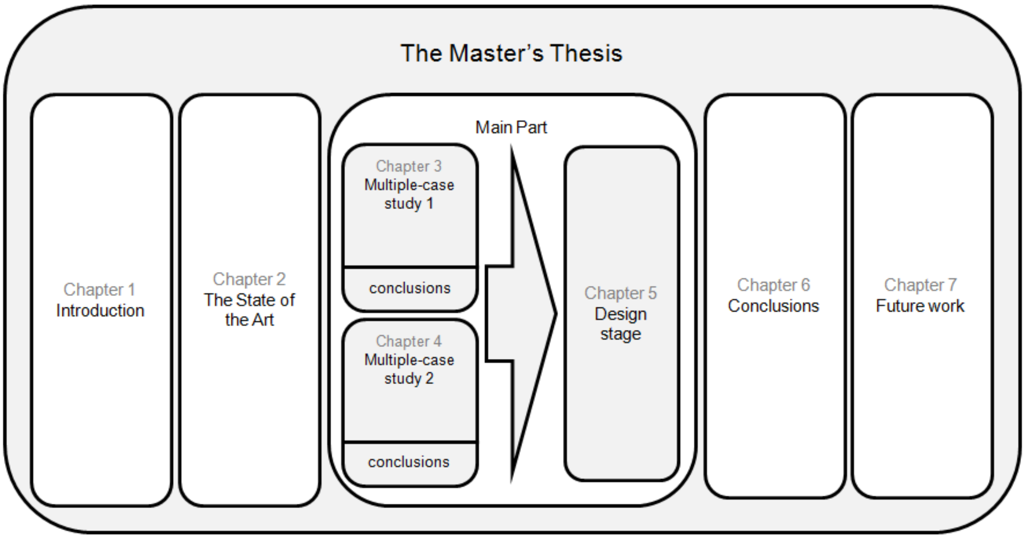


Figure 3: General structure of the thesis

2 The State of the Art

The one of fundamental works in the field of identity management is the paper "The Laws of Identity” by recognized expert Kim Cameron [17]. The laws were justified and validated via the open discussion between experts. Among the first, this paper highlighted the problem of so called identity one-offs and the need in the common interoperable identity layer. However, the single simplistic digital identity as a universal one-fits-all solution is hardly possible due to very different interests of different stakeholders. The unifying identity metasystem as a kind of abstract identity layer was suggested as solution of the problem. However, such identity metasystem should correspond to 7 basic laws of identity in order to create multi-party accepted unifying identity metasystem.

1. User Control and Consent

   Technical identity system must only reveal information identifying a user with a user’s consent.

2. Minimal Disclosure for a Constrained Use

   The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

3. Justifiable Parties

   Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

4. Directed Identity

   A universal identity system must support both "omni-directional” identifiers for use by public entities and "unidirectional” identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

5. Pluralism of Operators and Technologies

   A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

6. Human Integration

   The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

7. Consistent Experience Across Context

   The unifying identity system must guarantee its users a simple, consistent, experience while enabling separation of contexts through multiple operators and technologies.[17]

Besides the laws, Cameron introduced another important concept – a claim-based identity. Nowadays, this concept is a basis for most of user-centric identity management systems or technologies as well as most of federated identity management systems. A claim is an assertion by one subject about itself or another subject that is considering as being "in doubt” before the claim approval. The claim usually represents a certain attribute of an identity. A number of claims might be combined in a set of claims which can be considered as a digital identity where each claim represents an attribute of it. Finally, Cameron defines a digital identity as a "*set of claim made by one entity about itself or another entity*" [17]

The identity management is "*the combination of technical systems, rules, and procedures that define the owner-ship, utilization, and safeguarding of personal identity information. The primary goal of the IDM process is to assign attributes to a digital identity and to connect that identity to an individual.*"[18] ISO/IEC JISC 27 describes the identity management life-cycle as comprised of following steps:

- Identity choice, provisioning and enrollment;
- Identity authentication;
- Binding identities with attributes;
- Identity certification;
- Identity change;
- Unbinding of attributes from identities;
- Identity revocation;
- Controls. [19]

There are four distinct technology models of IdM system architecture: Siloed, Centralized, Federated, and User-Centric . The "siloed" identity system is designed and operated in a separate manner. It's not connected to any other identity management system and operated within one security domain. In this model, a user has to have as many identities as mane accounts (s)he has. The centralized model implies the existence of single repository, serving as the only central source of ID data. A user has only one ID to access all accounts. In the federated model, there are many identity providers interconnected and sharing data between each other. In a single sign on scenario, a user can authenticate to the identity provider and this authentication will serve for the whole federation. Alternatively, if the single sign on is not used in the federation, a service provider relies on identity provider which authenticates the user. Finally, the user-centric model implies that user has full control over data and may choose an identity to use and data to disclose. User-centric model usually implies also high level of privacy protection. The service provider, in this case, relies on authentication done by identity provider[1]. [1] The features of each model are presented in appendix 6.

2.1 User-centric and privacy enhancing IdM technologies

The big step towards user-centric identity framework was made by by Kim Cameron, Reinhard Posch and Kai Rannenberg in 2008. They proposed the common architecture framework of a user-centric identity metasystem along with the overview of metasystem requirements in the light of multilateral security. [20] This architecture has been already implemented by Microsoft in a number of their product and technologies such as CardSpace identity selector for managing Information Cards and in the access control service

[1] Herein and further in the text we will consider user-centric ID as issued by an identity provider excepting self-asserted identities.

of their cloud platform Azure. Latter provides interoperability and identity transformation function via security token service inside the cloud, transforming identities from different IdP to a standard form and providing basic function for identity federation using SAML security tokens.[21]

However, user-centric identity solutions are possible not only on an architectural level but also on the level of cryptographic protocols. Recently, two technologies were honored in European Identity Award for outstanding projects, innovations and advancements in the field of digital identity management held during the European Identity Conference 2010 [2] and got few other awards. These technologies are Identity mixer protocol (also known as Idemix) developed by IBM within EU project called PrimeLife [22] and U-Prove technology [23, 24] originally developed by company called Credentica, which then was acquired and became a part of Microsoft in 2004. These cryptographic protocols are aimed to realize an efficient anonymous credential system. U-Prove technology allows building the user-centric identity management system based on use of asymmetric crypto-algorithms enabling claim-based identity with privacy enhancing by design. Besides, U-prove can be easily integrated into existing identity metasystems such as information cards (an identity meta-system based on interoperable standards of issuance and authentication) without hampering its functions and bring security and privacy assurance to the next level.[25]

Psychology is another important aspect of information security influencing number of solutions and different decisions. [26]. One of the biggest psychological obstacles in a way to commonly used identity is usability of identity [27]. Identity management (IdM) system will succeed only if users find it easy to correctly and securely configure and use. The initial integration and support of IdM system by default in any OS/browser without any additional installation is also important. It's important for designers of such a system to remember is that cognitive scalability is key to the success of identity management systems along with technical scalability. "*Identity management scheme designers must be cautious about reducing one user's burden while simultaneously increasing users' total workload or mental overhead. When calculating the costs, designers of any one scheme have a tendency to underestimate them by focusing only on one user interacting with one IdP. Instead, we should analyze the burden placed on users by the system as a whole.*" [27] Even though user consent is one of the 7 laws of identity is important to remember that too much consent might have an opposite impact on a security level. A user cannot evaluate too much information when it's needed and by providing them 10-15-20 attributes/claims to consent on transfer all we got is only overwhelm them. Thus, it's crucially important to present the information in reasonable amount and caching it when it's possible. Yet, protocols must support mutual authentication instead of "redirect-based" identity management (e.g. OpenID) making it the ideal infrastructure for phishing for an adversary. "*Today's interfaces and security indicators are inconsistent across browsers and operating systems, increasing the risk of user error due to unfamiliarity*" [27] Typically, users are not good at risk assessment and cannot decide on the way whom to trust and not to trust. Thus, designers should perform security reviews and usability analyses before deploying systems as well as introduce and develop common trust models with policies in order to benefit users and RPs. [27]

[2] European Identity Conference 2010 http://www.id-conf.com/eic2010

2.2 National Strategy on Trusted Identities in Cyberspace and OIX

The need in development of identity management systems and its important role in critical infrastructure protection were recognized in a high level both in Europe and, recently, in U.S. In April 2011, the White House in collaboration with the National Institute of standards and technology (NIST) released the National Strategy for Trusted Identities in Cyberspace (NSTIC) which defined the notion of "identity ecosystem".[28, 29]

The identity ecosystem is defined as realization of strategy vision of NSTIC: "*Individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation.*"[28] It consists of participants, policies, processes and technologies needed for secure and trusted identification, authentication, and authorization across diverse transaction types. The execution components of the Identity ecosystem are as follows:

- An individual is a person participating in an online transaction. This component is assigned with the highest priority;
- A non-person entity (NPE) is an organization, software, hardware, or service involved in or support a transaction;
- The subject of transaction;
- A digital identity is a set of attributes representing a subject;
- Attributes of the identity;
- An identity provider (IDP) which is responsible for establishing, maintaining, and securing the digital identity. These includes: revocation, suspending and restoring if it is needed;
- An enrolling agent performing verification and enrollment;
- Credentials issued by identity provider to a subject to provide evidence of the identity;
- An identity medium which can store the credentials;
- A relying party which can select and trust the identity and attribute providers of their choice;
- An attribute provider (AP) which is responsible for establishing and maintaining identity attributes;
- Participants are those subjects, identity providers, attribute providers, relying parties and identity media who are taking part in a given transaction;
- A trustmark is used to indicate that a product or service provider has met the requirements of the Identity Ecosystem, as determined by an accreditation authority.[28]

The policy foundation of the Ecosystem is comprised of different component (Fig. 4 (Source: [28])):

- The Identity Ecosystem Framework is the overarching set of interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms that structure the Identity Ecosystem;

- A steering group administering the process for policy and standards development;
- A trust framework developed by a community whose members have similar goals and perspectives;
- An accreditation authority assesses and validates identity providers, attribute providers, relying parties, and identity media, ensuring that they all adhere to an agreed-upon trust framework;
- A trustmark scheme determining compliance with the Identity Ecosystem Framework.[28]

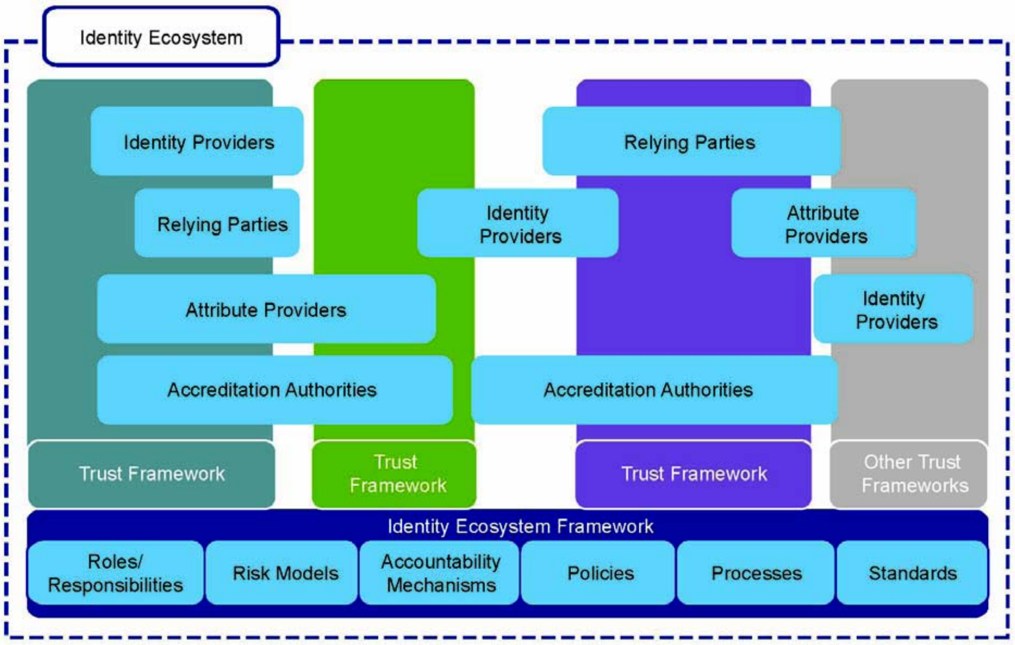


Figure 4: NSTIC: Multiple trust frameworks within the Identity Ecosystem Framework

Open Identity Exchange Group

The Open Identity Exchange[3] group was formed in response to the NSTIC. It is the non-profit organization founded by major identity providers including Google, AT&T, PayPal, Equifax, VeriSign, Verizon, CA, etc. It is a central organization for Identity Ecosystem with the goal to provide trusted framework and interoperability for trusted identity management based on two widely known user-centric technologies, namely OpenID and Information cards.[30, 31] The basis of OIX is Open Identity Trust Framework model - a set of of technical, operational, and legal requirements and enforcement mechanisms for parties participating in exchange of identity information. (Fig. 5 (source:[30]))

The trusted framework considers the following roles: Policymakers (deciding the technical, operational, and legal requirements for governed IdMS), OITF Providers (translating the requirements into their own blueprint for the trust framework), Assessors (evaluating and certifying Identity providers and relying parties against the set of requirements), Auditors (checking participants compliance with policies), Dispute resolvers

[3] Open Identity Exchange (OIX) http://openidentityexchange.org/

(providing dispute resolution services). The framework also distinguish different services by required level of protection and level of assurance. [30, 31]

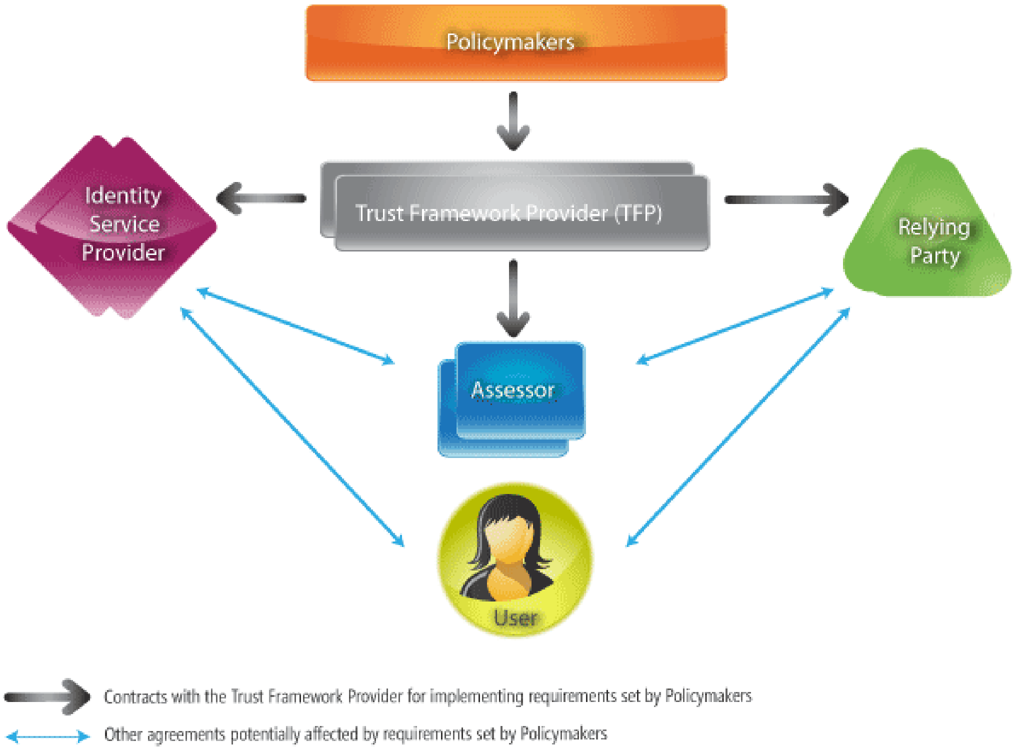

Policymakers
Identity Service Provider
Trust Framework Provider (TFP)
Relying Party
Assessor
User
Contracts with the Trust Framework Provider for implementing requirements set by Policymakers
Other agreements potentially affected by requirements set by Policymakers

Figure 5: NSTIC: Open Identity Trust Framework model

2.3 Cross-border IdM

The cross-border interoperability of public services and related security issues have been addressed by various European projects and researches. The European Commission released the specification of European Interoperability Framework 2.0 [32] which identifies the need for interoperability on four distinct levels:

- Legal interoperability;
- Organizational interoperability requiring process coordination so that different organizations achieve agreed and mutually beneficial goals;
- Semantic Interoperability for precise meaning and compatibility of exchanged data;
- Technical Interoperability to link different systems and services together.

The interoperability of identity management has also been of interest for researchers. [33, 34] The ENISA Risk Assessment report[35] on security issues in cross-border electronic authentication identified the three key differences between domestic and cross-border security systems (Fig. 6 (Source: [35])):

- The domestic systems are homogeneous with respect to technologies, while cross-border ones are not;

- In contrast to domestic, cross-border systems are governed by two separate set of laws;
- The cross-border systems are potentially open to non-participant, while domestic ones 'know' all participants of the system and so are closed.

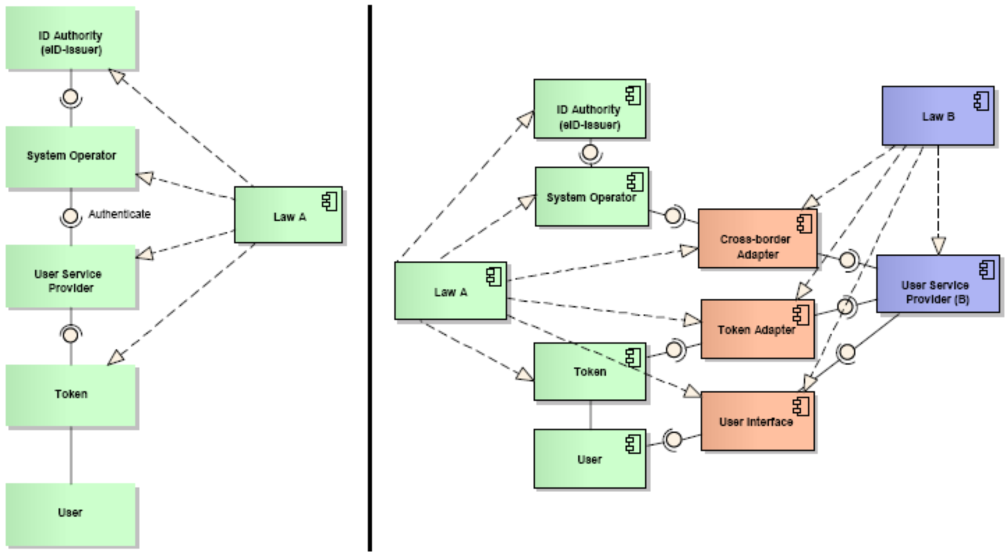


Figure 6: Generic models of domestic (left) and cross-border (right) authentication

STORK[4] is one of the major EU projects researching cross-border identity management systems. It's aimed to develop and implement EU-wide interoperability platform for eID on top of existing national eID infrastructures. Two models for interoperability have been suggested in the course of this project: middle-ware and Pan European Proxy Service models for eID. The former model implies that a software component at the user side performs transformation of the ID, while in the latter model an intermediary proxy performs this function.[36, 8, 37, 38]

Other EU projects addressing IdM researches are:

- PARSIFAL is aimed to developing long term visions, research roadmaps, scenarios and best practices for critical infrastructure protection;[5]
- SSEDIC provides platform for the stakeholders of electronic identity; [6]
- PEPPOL researches seamless cross-border eProcurement, connecting communities through standards-based solutions;[7]
- TAS3 researches & developes a trusted architecture and set of adaptive security services[8]

[4] Secure Identity Across Borders Linked (STORK) https://www.eid-stork.eu/

[5] Protection and Trust in Financial Infrastructures (Parsifal) http://www.parsifal-project.eu/

[6] Scoping the Single European Digital Identity Community (SSEDIC) http://www.eid-ssedic.eu/

[7] Pan European Public Procurement Online (PEPPOL) http://www.peppol.eu/

[8] Trusted Architecture for Securely Shared Services (TAS3) http://www.tas3.eu/

There is also an initiative towards interoperable identity in electronic banking. The EBICS standard (Electronic Banking Internet Communication Standard) was developed by a group of the German financial organizations and aimed to provide an electronic banking standard for corporate clients to allow online banking with multiple banks. Today, it's used by all French and German banks for the inter-bank secure data transmission. The standard does not present any special requirements of the concrete architecture of the system, but rather represents the protocol of communication. The fundamental features of the standard are:

- "Transmission of professional data (commercial transactions) via order types using established bank-specific formats;
- Expansion of the "DFÜ Abkommen" with the possibility of the "Distributed ElectronicSignature (VEU)";
- Specification of the EBICS-specific protocol elements in XML;
- Transmission of messages via http ("Internet-based"); utilisation of TLS for basic transportation security between the customer's and the bank's systems, using TLS server authentication;
- Cryptographic safeguarding of each individual step of a transaction via encryption and digital signatures at the application level." [39]

3 Analysis of the Norwegian BankID IdM Model in International Context

3.1 Digital Identity Management in Norway: past and present

Norway has a long tradition of population registering dating back to 1623 when churches started to maintain books with basic data about citizens such as birth date, marital status, migration status, and death date. However, the electronic National Population Register ("Folkeregister" in Norwegian) roots in so called local registers. These registers were maintained by local authorities on volunteer basis starting from the year 1906 and became obligatory in the year 1924. In 1916, the Central Birth Register("Sentralt fødselsregister" in Norwegian) had been introduced to the public and became an alternative to still existing church books. Next remarkable step in developing the national register is the period of occupation in 40es. The Reich Commissariat of occupation forces obliged to maintain mandatory population registers in all municipalities since 1 March 1943. Later, in 1946, this initiative had been adopted by the Parliament of Norway ("Stortinget" in Norwegian) and stipulated in the Law about Public Registers ("Lov om folkeregistre" in Norwegian). In 1964, the central National Population Register and the Norwegian Birth Number (NBN, "fødselnummer" in Norwegian) had been introduced. [40]

The Norwegian Birth Number is a type of Social Security Number(SSN) provided by the government to all residents and citizens. It had been introduced in 1964 and will expire in the year 2039. Being registered once, it cannot be changed later unless it's been authorized by the National Police Directorate. A NBN is assigned by the National Population Register governed by the Norwegian Tax Office ("Skatteetaten" in Norwegian). The number consists of 11 digits where first 6 digits represent the date of birth, next three - an individual number, and last two are check digits. The individual number is chosen from a certain range depending on a century of birth and, additionally, contains information about sex so that males get odd numbers and females get even ones. It's worth to note that such system implies unique identification of only people born between 1854 and 2039. [41]

All NBNs are stored in the registry maintained by the National Population Register. It's associating a certain NBN with a certain entity along with personal information such as full name, address, place of birth, citizenship, work and residence permits, and family relations. As of year 2008, the registry consisted of approximately 7 million NBNs. An access to the registry may be granted by the Central Office of the National Population Register ("Sentralkontoret for Folkeregistering" in Norwegian). Today the national registry is used by all public authorities, the Norwegian Bureau of Statistics ("Statistisk sentralbyrå" in Norwegian), banks and insurance companies, various employers, private organizations and individuals. Public authorities can apply for full access, others can request only limited access providing less sophisticated search opportunities (e.g. "exact search" only). [42, 43, 44]

The NBN is used in a vast of online services from governmental to banking ones. By means of the MinID identification numbers are used to access online public services.

The MinID requires entity's NBN, personal password and one-time code derived either from SMS to registered mobile phone number or a PIN-code letter. Thus, after successful authentication and authorization a user gets access to online services provided in health, education, financial (e.g. tax-office, pension information), and social sectors as well as a number of other public services.

In 2008, the Government claimed about developing a public infrastructure to manage and verify different digital identities currently in use. The 1st version of digital identity gateway (referred as to "ID-porten" v1.0), operating as an interoperability hub for various digital identity solutions from different authorities, has been introduced in 3rd version of MinID. It employs SAML2.0 in order to provide federation facility. [45] In autumn 2010, a number of MinID users exceeded 2.3 million as DIFI[1] claimed.[46]

The NBN is used as a primary identifier in a variety of online services, including online banking. To authenticate their customers all of Norwegian banks and local branches of international banks employ interoperable cross-banking solution called the BankID.

3.2 The BankID IdM Solution

The Norwegian BankID solution is a widely used identity management system allowing customers registered in Norway, having the single identity, authenticate in online banking services, sign documents, and identify themselves in online public & e-commerce services.

A number of application of the BankID continues growing. Thus, recently introduced BankAxess solution extended a number of possible applications by enabling to use the BankID in order to perform electronic payments directly from one bank account to another. [47] In April 2009, the Norwegian Ministry of Finance issued the regulation which made possible to use electronic authorisation to open a new customer relationship with a bank or an insurance company. It allowed the BankID community to respond quickly with novel functionality of the BankID allowing Norwegian bank customers, first in the world, to open or switch bank-accounts and even banks instantly. The feature bears enormous potential for simplifying business processes and cost-savings. [48]

3.2.1 BankID Infrastructure

BankID Common Operational Infrastructure (COI) (Fig.7 (Source: [49])) has been developed and is now operated by the Norwegian Banks Payment and Clearing Centre ("Bankenes Betalingsentral" a.k.a "BBS"). BankID infrastructure is coordinated and governed by BankID Community consisting of three participants: banks issuing BankID and actively participating in development and employment processes; Banks' Standardization Office ("Bankenes StandardiseringsKontor" or "BSK") setting the policy, standards and security requirements; the Norwegian Financial Services Association and the Norwegian Saving Banks Association coordinating activities in the community, organizing work with the BankID and is responsible for development and administration of infrastructure. BankID COI is based on "Regulations for BankID" which, in-turn, regulates also the trust between banks in the inter-bank regulations. Later, in January 2009, the banking industry established a new common administrative unit for BankID (named 'BankID Norge') for better management of BankID activities and the COI, and promoting the BankID solution.

[1] Norwegian Agency for Public Management and eGovernment

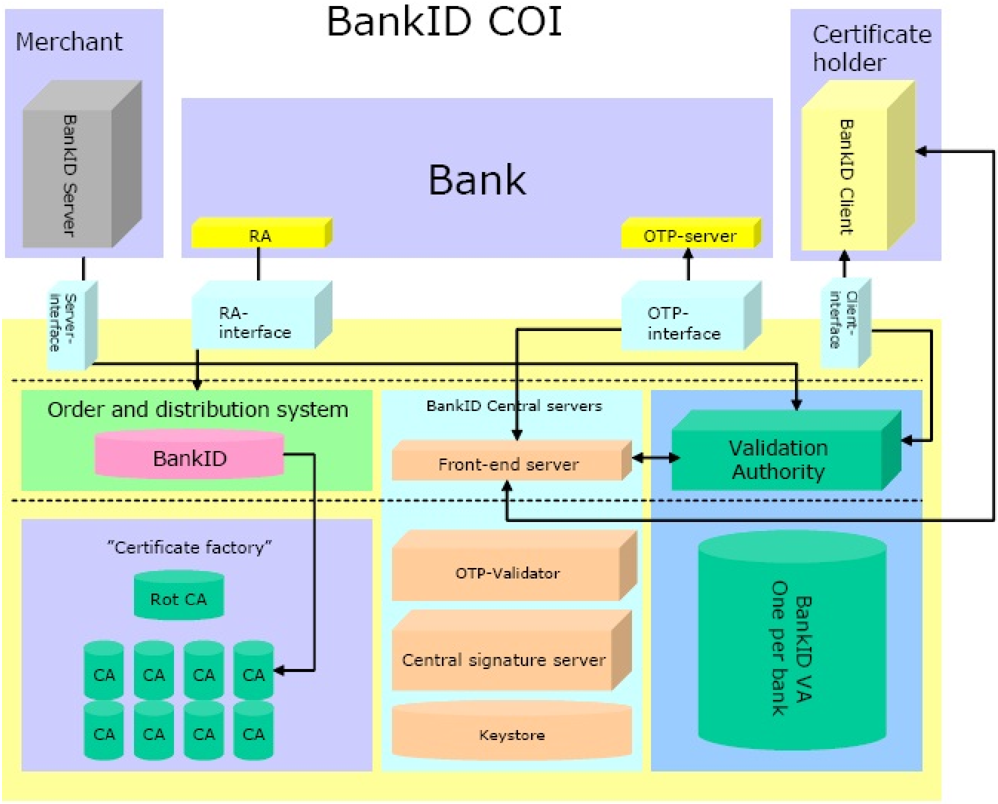


Figure 7: BankID Common Operational Infrastructure

On the architectural level, BankID is based upon Public Key Infrastructure (PKI). However, it is rather PKI substitute than its pure implementation. The infrastructure is divided into two main parts: the central infrastructure operated by the Norwegian Banks Payment and Clearing Centre; the distributed infrastructure spanning banks, merchants, and customers (certificate holders).

Core functions of distributed infrastructure enable the usage of BankID via providing its acceptance, authentication and signing functions along with administration function for banks. All the functions are executed in the client or merchant side. At the same time, the central infrastructure provides all necessary interfaces to the distributed infrastructure and executes functions related to certificate life-cycle management along with one-time password (OTP) validation and providing central storage and use of private and public keys. [49]

The Root-CA is jointly owned by the Norwegian Financial Services Association and the Norwegian Saving Banks Association and used to issue certificates to level-1 CA owned by bank-members or groups of banks, acting also as RA. The certificate of BankID Root-CA is valid for 26 years with 14 years renewal period, while the level-1 CA's certificate is issued for 12 years. Both certificates require the key length of at least 2048 bits RSA.

Three different types of customer certificates are in use: personal certificates for private persons; employee certificates for the enterprise customers; merchant certificates for online services willing to use the BankID for one of the scenarios. The first type implies also the special parameter referred as to PID (personal Identifier) which is unique for each person and exists in all certificates owned by the entity. However, a user has right to change PID while requesting a new certificate. End-user certificates are valid for 2 years and the key length is required to be at least 1024 bits RSA. The BankID certification profile is presented in Appendix B, Table 7.

There are two different clients, using the same user interface: locally and bank stored. Locally stored client is the Java-applet pre-installed on user's computer together with personal certificate. A user gets access to BankID by entering username and static password. This client is mainly used by service-providers and holders of employee certificates totaling around 700 active certificates (280 service providers), as of March 2010. [50]

The second type is way more widely used by end-users totaling around 2.5 million active personal certificates (2.2 million customers). [50] The client is Java-applet downloaded by a user each time s/he wants to use BankID. In that case, the user doesn't have a special pre-installed software or information on the computer and authentication is provided by means of NBN, OTP, and user-chosen static password. Since both public and private key certificates are stored in the central infrastructure, BankID differs from a typical PKI implementation. In cases when a user has accounts in more than one bank s/he also gets multiple BankID certificates belonging to different banks. All these certificates are also stored in the central infrastructure. In order to select a certificate, and so a bank to use, user chooses the one from the list of available banks by entering the NBN. Next step requires user to enter static password along with OTP which is either generated by a hardware token or obtained from bank as a list of one-time codes. The code is verified in the central infrastructure as well as the password which is used by central infrastructure to get access to user's private key. Following challenge-response protocol is used for mutual certificates verification between BankID server and client by means of the validation authority. All cryptographic procedures are executed in the central infrastructure which requires the client to transmit OTP and user's static password over the Internet and calls for another difference (Fig. 8 (Source: [3])). [49, 3]

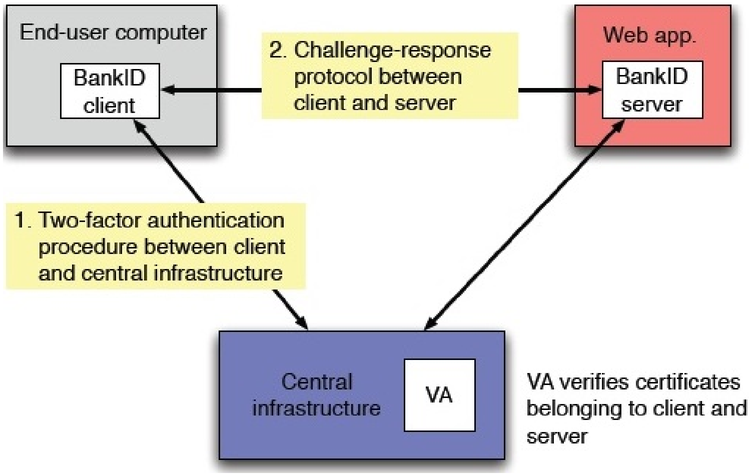

End-user computer
BankID client
2. Challenge-response protocol between client and server
Web app.
BankID server
1. Two-factor authentication procedure between client and central infrastructure
Central infrastructure
VA
VA verifies certificates belonging to client and server

Figure 8: BankID authentication procedure

One more significant difference from X.509 PKI is an absence of trusted third party to resolve non-repudiation issues between a user and the Norwegian banking industry owning and operating the BankID infrastructure. Unfortunately, there is no publicly available information about legal and technical non-repudiation protocols in use. [49, 3]

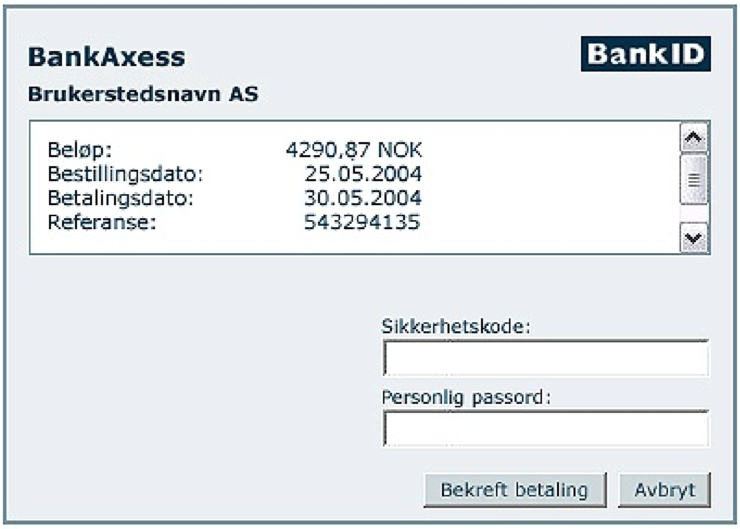
3.2.2 SIM-stored BankID for mobile phones

Recently, SIM-based authentication solution with BankID for mobile phones had been developed by Norwegian banking industry and launched by Telenor in the year 2009. As of March 2010, the service is provided and supported only by Telenor and number of certificates in use total around 9500.

The solution is aimed to provide electronic identity and simple digital signing of short messages (up to 120 characters) storing users' information on a PKI-enabled SIM card of the mobile phone. Key generation procedures take place inside the SIM and, further, is activated in the central infrastructure using the same algorithm as in case of bank-stored BankID client. Issued certificate is valid for 2 years. The signature function is provided in a basic level since SIM application can only produce simple PKCS#1-signatures. [51, 52]

3.2.3 BankAxess

BankAxess is a coordinated electronic payment service based on the BankID and aimed to serve as a supplement to the international payment systems as Visa and MasterCard in the Internet. The service is available to every entity who has BankID and an account in the bank offering BankAxess service. It allows to approve money transfer from buyer's to seller's accounts in the same or different banks, both offers BankID and BankAxess services.[47] As of January 2011, there are 10 such banks, including the largest ones, and almost 150 merchants who provides the payment option. [53, 54]



BankAxess

Brukerstedsnavn AS

Beløp:	4290,87 NOK
Bestillingsdato:	25.05.2004
Betalingsdato:	30.05.2004
Referanse:	543294135

Figure 9: BankID: BankAxess user interface of approval form

3.2.4 Analysis of Norwegian IdM Solutions

Security & Privacy

Public reviews are an essential part of developing and exploitation of any national-wide IdM system.[55] Both MinID and BankID can be undoubtedly considered as such systems. Since the introduction of BankID few independent evaluations took place in order to examine whether the system meets minimum security and privacy requirements.

A reverse-engineering analysis of Java applet, serving as the BankID client, showed the applet is vulnerable for insider attacks and has cryptographic problems related to the protocol between the applet and the signature HSM. Furthermore, the analysis revealed flaws in implementation of public key and symmetric encryption so that RSA with PKCS#1 1.5 padding, employed for public key encryption, doesn't have basic countermeasures to standard attacks on PKCS#1 1.5. Also, no message integrity protection is used in symmetric encryption protocol (3DES in CBC mode with an all-zeros initialization vector). [56]

The risk analysis of the BankID solution, performed in the end of year 2007 and based on publicly available descriptions of the BankID infrastructure, identified significant risk to BankID customers and resulted in 10 observations embracing risks of authentication and non-repudiation services as well as privacy related risks.[3] The results of risk analysis together with mitigation strategies are presented in Appendix C, Table 8. Most of the found issues were claimed to be fixed by in following few month. The initial implementation of BankID infrastructure was vulnerable to Man-in-the-Middle attack by changing initialization parameters in the BankID client applet to address of adversary's proxy placed between a customer and a merchant. The attack was successfully performed in autumn 2007 by a group of researchers from University of Bergen. [57] The Banks claimed the vulnerability had been fixed by November 2007 along with increasing the non-repudiation level. However, information about legal and technical non-repudiation protocols is not publicly available. And since the Norwegian BankID solution is fully owned and controlled by the Norwegian banking association which, in its turn, provides financial services, it's unclear how possible conflicts of interest is to be resolved.

Concentration of main functions in the central infrastructure, along with increasing the manageability of the system, creates risks to availability of the entire system. In this case, the identity provider is a central point of failure and bottleneck for a user access control which is required to be always online. A massive DDoS attack on the central infrastructure may disable the BankID system and enormously damage the main business of many banks and merchants. However, BankID community claimed the system was designed as a high availability service with automatic interruption and disaster recovery technologies with seamless continuation of work on backup system if the main system will fail. [49]

BankID community shows readiness to deal with results of independent evaluations of the system, fixing found vulnerabilities and mitigating risks. As a consequence, it results to better and better security of the system. However, there are still open issues with the BankID infrastructure:

- Legal and technical non-repudiation protocols are not published, neither than its evaluation by independent lawyers and security experts;
- Authentication procedures are remained untouched and still imply transmission of user's OTP and static password rather than process it locally;
- NBN is still used as primary identifier in its direct form.

Being widely used in overwhelming majority of various online services as a primary identifier, Norwegian birth numbers represent a separate problem of increased risks of ID theft and privacy violation. The BankID central infrastructure learns the used signing key along with the name of the merchant. At the same time, the merchant identifies users by their NBNs which creates a privacy flaw. [56] As soon as most procedures are executed in the central infrastructure, it creates a potential to easily track user or services consumed by.

The authentication procedure used in BankID infrastructure requires a customer to enter the NBN first and then to choose a one of customer's bank from the list. It presents the risk of privacy violation via data harvesting. Moreover, this task may be automated in order to create a database of bank accounts belonging to a specific entity with a certain NBN. The database may be extended with any other information harvested from various online services in Norway. Therefore, concentration of all information flows and processing procedures in the one place, the central infrastructure, creates a great risk of profiling either by the system itself or by an insider.

In fact, the research of risks of identity theft in Norwegian online systems showed that automatic data harvesting is possible in many online services and several mobile operators due to a bad design of identification & authentication schemes, and concluded that there is a risk of large-scale identity theft is possible in Norway. Thus, some mobile operators asked customers to select a subscription type, to enter their NBN and right after then the full name and address associated with the NBN was presented. Besides, some authentication schemes ask users to enter NBN first, then the system checks whether the NBN is used and continues the authentication or request to enter another/valid NBN. Here, a script may automatically gather information about NBNs in use. [42]

Analyzing the BankID identity management system against Kim Cameron's Laws of Identity[17], it's clear that some of these laws are not obeyed. Thus, for example, the 2nd law requires "*the solution which discloses the least amount of identifying information and best limits its use*" [17] but, considering aforementioned issues with aggregation of sensitive data and specificities of protocols, the laws are not followed. The 3rd law demands that "*Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship*" [17], and again the BankID infrastructure implies active participation in any procedure performed by or any function used by the user, because overwhelming majority of cryptographic and identity management operations are executed in the central infrastructure.

Acceptance & Interoperability

The most secure solution cannot be successful in the market without interoperability and acceptance by involved multiple parties. Besides, the 5th law of Kim Cameron's laws of identities postulates that "*a universal identity system must channel and enable the interworking of multiple identity technologies run by multiple identity providers.*" [17]

The simplification of the revocation problem of typical PKI and much simpler for implementation technical solution ensured a good acceptance of Norwegian BankID in the market. The BankID system uses the Java applet as a frontend for authentication system allowing operability in all devices which supports Java platform. Besides, transferring of most procedures to central infrastructure, including cryptographic operations, reduced requirements to computational resources.

The acceptance and dissemination levels of the BankID solution are relatively high for the country where total population approximately equals to 4.9 million people. As of November 2009, "BankID surpassed 2.5 million active personal certificates, which are used between 800,000 and 900,000 times per day. SIM-stored BankID constitutes 8,000 certificates, and are currently only available to Telenor customers. 267 organizations have implemented BankID. Approximately 60% are online banks, whereas the remaining 40% are made up by municipalities, online merchants and public institutions." [58] As of January 2011, there are 303 active merchants including 103 banks with online banking facilities and 149 merchants supporting BankAxess payment option. [54] According to the registry of The Financial Supervisory Authority of Norway ("Finanstilsynet" in Norwegian), total number of banking and finance institutions registered in Norway equals to 256, including 153 local banks and bank holdings and 43 branches of foreign credit institutions. The data shows that not every financial and banking organization in Norway either have online banking facility or support the BankID solution. In fact, the reason of such numbers is that several local branches of foreign banks and some local banks employ integrated online banking solution, where the BankID is provided as a one of options for authentication.

A one of goals for the BankID solution is to become a national-level identity infrastructure and to be used in online public services. However, dissemination and acceptance in the services is rather weak. In fact, only 4 municipalities employ the BankID solution to provide easy access to their online facilities. [54] A possible reason is expectations of final implementation of a next MinID version providing ability to handle multiple digital identities and acting as a HUB for these IDs. As for January 2011, the MinID still doesn't support the BankID identity management system as a part of common eID for online public services initiative.

A person, who wants to open an account in a one of Norwegian banks, cannot do it without having the Norwegian identification number or at least temporary D-number issued together with work visas. The same restriction applies to the BankID system. Most of Norwegian banks employ the BankID solution as the one and only method to authenticate their users which makes the system quite isolated to foreigners, since the BankID requires a customer to have the Norwegian identification number or, in other words, to be a resident. The problem is not significant while the system operates in national-level, but it needs to be addressed in a cross-border situation in order to allow the use of system by customers from various countries.

The use of the BankID is limited to the participants and neither provides a federation ability nor support any other identities. The current infrastructure implies only linear growth of the identity management system and represents rather isolated solution than easily integrable one. In contrast to BankID, MinID is designed to provide federation (by means of SAML technology) and interoperability at semantic, organizational, and technical levels as the one of obligatory ICT architecture principles obliged to follow by the governmental directive.[59] Besides, DiFi claimed that MinID solution follows the European Interoperability Framework.[32] As of the end of 2010, the number of users of the MinID exceeded 2.3 million and approximately 20 government departments and 120 municipalities who employ the MinID as an authentication solution for provided online public services. [46]

The acceptance of the MinID solution is comparable to the one of the BankID. Both systems have relatively equal amount of active users and dissemination rate. As of the end of 2010, the number of users of the MinID exceeded 2.3 million and approximately 20 government departments and 120 municipalities who employ the MinID as an authentication solution for provided online public services. [46]

Legal and Cultural Aspects

An IdM system needs governmental support provided by as standardization body, legal framework for development, implementation and exploitation of identity management solutions, and as a strong administrative resource. Although the BankID infrastructure is developed, controlled and operated under supervision of the banking community, banks itself and security requirements of their services are highly regulated by the government. This provides an additional level of trustworthiness to the system which is necessary for large-scale IdM system operating on a national level. In these terms, banking institutions seem to be more than others suitable to act as identity providers in national-level IdM systems and in a cross-border situation in general. Besides, banks are not involved in direct politics[2], which may potentially cause a conflict of interests, not influenced by culture so much and have a high level of trustworthiness at the same time. In fact, the trust in banks as organizations handling personal data is quite high among EU member states. According the "Flash Eurobarometer No 225 - Data Protection", 66% of respondents trust to banks in average in EU and the trust rate is higher than 60% in all countries except Italy and Greece.[60]

A system depends on context in which it operates. Cultural aspects impacts a national level identity management systems and have to be taken into account during development and implementation processes. The baseline of these aspects is public trust in government in terms of citizens' data and privacy protection. A lack of trust in an authority (e.g. governmental department) may slow down implementation, dissemination and acceptance of an identity management system and raise privacy concerns, so requirements to such system. On the other hand, the high level promotes governmental initiatives and simplifies its implementation. Historically, Norway has a tradition of population registering since 1946 when all local authorities have held a local national register of all residents in the individual municipalities. The good acceptance and dissemination of the national identity systems in Norway are based on traditionally high level of public trust in the way Norwegian public authorities handle citizens' data.

In the work "Culture's consequences: International differences in work-related values" Geert Hofstede, the famous Dutch sociologist, suggested a framework for cultural classification and identified a culture as a taxonomy of five dimensions: power distance(PDI), individualism(IDV), masculinity(MAS), uncertainty avoidance(UAI), and long-term orientation(LTO). [61] The cross-cultural analysis of European e-Government adoption showed that countries with high PDI and UAI indices would show lower rate of adoption than countries with low indexes. At the same time, high IDV and LTO indexes indicate the tendency for higher adoption rate.[62] Norway has PDI=31 and UAI=50 which are below the average in Europe, IDV=69 and LTO=44 are above the average. It proves that acceptance and dissemination of governmental initiatives in identity management tend to be at the high level in Norway.

In Norway, the control over systems processing data is performed by the Data Inspectorate("Datatilsynet" in Norwegian) and regulated mainly by the personal data act ("Personopplysningsloven"); as well as regulation on processing of personal data ("Forskrift om behandling av personopplysninger"), e-signature law ("e-signaturloven"), public administration act ("Forvaltningsloven"), framework for authentication and signing in

[2] Although banks are subject of politics of government and may be involved in political actions (e.g. block money transfers or bank accounts as a result of law reinforcement).

electronic communication with and within the public sector ("Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor"), and regulations on held on computer media communication in management ("Forskrift om elekronisk kommunikasjon med og i forvaltningen"). The other legislative acts mainly have a form of standards, official guidelines and formal recommendation enforced by governmental decisions and directives and supported by the public administration act and the anti-discrimination and accessibility act. The political agenda is defined through three key documents:

- Report no. 17 (2006-2007) An Information Society for All (St.meld. nr. 17 (2006-2007) Eit informasjonssamfunn for alle) published by the Ministry of Government Administration and Reform;
- Report no. 19 (2008-2009) A government of democracy and community (St.meld. nr. 19 (2008-2009) Ei forvaltning for demokrati og fellesskap) published by the Ministry of Government Administration and Reform;
- Overall ICT Architecture Principles for public sector version 2.0 (Overordnede IK-Tarkitekturprinsipper for offentlig sektor versjon 2.0).

3.2.5 Norwegian Experience in International Context

For comparative study four countries, each with distinct background and way of IdM, have been selected: Germany[63], Austria[64], Denmark[65], and Sweden[66]. All considered national IdM systems are based on and originate from national registers of population. This shows the tendency to rather continuations and consequent upgrades of existing identity management solutions in the country than introduction of completely innovative solution. Besides, all the solutions use PKI either in typical or modified form as a basis.

According to survey conducted by the Gallup Organization "Data Protection in the European Union - Citizens' Perceptions" in 2008, 70% of Austrian and 65% of German citizens showed to be very concerned about how their personal data is handled, while in Denmark and Sweden the rate is moderate (45% and 46% respectively). Thus, Austrian and German citizens seemed to be the most concerned about data protection among all EU member states and it's reflected in the national eID management systems implemented there. [60]

Germany

Even though Germany has a long tradition of maintenance the national register of citizens since 1876, there is still no national identification number legalized. The first ID card with fingerprints was introduced in 1938 and, initially, was mandatory only for conscripts and Jewish citizens. However, 1 year later it became a standard for every citizen, besides Jewish citizens were assigned to personal identification number used to their administration in concentration camps. The historical context led to ban of such personal identification numbers for citizens by the Federal Parliament and the Federal Constitutional Court. [63]

Citizens in Germany should have either passport or personal ID card having a serial number which cannot be linked to the cardholder. Besides, there are few sector-specific IDs such as social insurance numbers kept by different social insurance companies or taxpayer identification numbers restricted to use for tax collection purposes only.

Recently, Germany introduced the new ID card for citizens. It's aimed to provide signing and identification services to cardholders and may also serve as a photo ID. The application area of the card goes beyond online public, commercial, or banking services and allows to use it for private online activities as well.[67] However, for example, the health sector employs a separate public e-Health solution with its own infrastructure and electronic health cards (eHC).

The one of key features of the new ID card is claim-based model of identity and user-centrism of the entire solution enhancing privacy, usability and the level of security. A user of such card gets full control over data and information flows. Moreover, the user can decide whether remain the identification or signing function enabled and can turn on/off it anytime.

As well as the BankID solution, the new German eID implies mutual authentication and encryption of all communication channels between parties in all steps. Despite the Norwegian BankID solution, the eID cards follows the principle of user consent, notifying the cardholder to whom and what personal data will be transmitted in every step, the principle of minimal disclosure, transmitting only minimum required amount of personal data, allows pseudonymous authentication, enabled by a card-specific and service-specific identifier, and card revocation. Besides, the eID card solution denies use of unique identifiers neither for citizens nor for the eID card. In order to enable mutual authentication, two PKI are used: the one for issuing and validating certificates for service providers and another for issuing and validating certificates and public keys for chips of the cards.[68]

A service provider must apply to the Federal Office of Administration in order to obtain certificate to read a certain data from the eID card. The certificate contains detailed information about the service provider along with the duration of certificate's validity and the purpose of data transmission. This allows selective disclosure of the minimally necessary amount of data to a validated and authorized service provider.

As well as BankID and MinID solutions, the German eID card is technically interoperable solution enabled by the platform-independent AusweisApp software providing easy-to-use application for user online identification and signing documents. The application seems to be more usable than the Java-applet used in the BankID identity management system in a sense that it makes easier to get access to signing service, by means of providing a plug-in for signing and encrypting e-mails to popular e-mail clients, along with better control over the data transmitted to a service provider. The new eID system is easily integrable into and interoperable with other identity management systems and technologies.

Another part of the eID card solution is the eID service used to establish trust in the identification process and acting as a medium between AusweisApp, so user, and a service provider. The service verifies whether a service provider has authorization to access the data from user's ID card and whether the card is valid and not revoked due to the case of identity theft or forgery. The one of distinctive features of this solution in comparison to the BankID is that the eID service may be implemented as logically independent server so that a service provider may choose to set up its own eID server or to use the eID service from a one of trusted providers. The feature allows decentralization of the infrastructure among different parties and so increases the system's availability. Besides, it provides flexibility to service suppliers allowing them to take a decision in compliance with its business model, volume of investment, available resources, and desired security level. The provider decided to run its own eID server must comply with the technical guidelines of the Federal office for Information Security. The stipulations assure required level of security for the eID server. [69]

So far, the new German eID solution is claimed to be the most secure solution with the best level of privacy protection.

Austria

In Austria, the history of public registration started in, approximately, the same time as in Germany, namely, since 1857. Nowadays, there is a mandatory registration of citizens in local registers, which then transmit the information into Central Register of Residents (CRR). The central register was introduced in 2001 and contains information about residents such as full name, sex, date of birth, citizenship, postal address, unique identifier(a kind of SSN) and, for foreigners, also passport data. The SSN contains a 3-digit serial number, a checksum digit and the birth date in a DDMMYY-format. The latter is the reason for restriction of use of the ID number in certain areas due to privacy-sensitivity of that information. Besides, in contrast to other European countries a citizen doesn't have to hold a specific ID card with the personal ID number. Instead, the need of personal identification and a form of the ID is regulated by specific regulations and depends on a sector of use and circumstances of an administrative procedure. This situation led to multiple identification numbers used in Austria, so called Sector-Specific Personal Identifiers (ssPIN) derived from CRR ID, and, ultimately, to the multiple-card model of national identity management system.[64]

The key feature of the Austrian IdM model is the citizen card ("Buergerkarte" in Austrian) which is rather a virtual concept able to be installed on multiple carrier devices and different ID cards supporting the citizen card function by default. This feature enhancing privacy protection of the solution and assures flexibility and compliance with requirements from various stakeholders. As well as BankID or MinID solutions in Norway, the citizen card is aimed to provide basic functions such as digital signing of documents and online transactions and online identification. The absence of obligation to hold the ID card ("Personalausweis") led to situation when only 10% of citizens have chosen to use the ID card over a passport or another official document used to prove the one's identity in Austria. [64]

Likewise the German eID card solution, Austrian ID cards must preserve unlinkability property in order to prevent profiling and privacy infringement. This has been achieved via permission to store only sourcePINs instead of unique personal CCR-number. This personal identification numbers are used to calculate unique sectoral ssPIN used by service providers for authentication purposes. Besides, the measure provides similar to German eID card feature of authorization of data accessed by a service provider. Moreover, the support of various carrier devices assures the technology neutrality and interoperability not merely in software but also in hardware levels. [64] The feature isn't that relevant for Norwegian, Swedish or Danish solutions based on a kind of software certificates, but has the advantage over German eID cards providing only software interoperability and requires a certain hardware device in order to use the ID online.

Since citizen card option is optional, it has to be activated by user in order to use it. As in case of German eID cards and despite the Norwegian IdM solutions, it provides the option for user whether or not to use the function. In turn, the digital signature service is based on a PKI and provided by a Certification Authority coordinating the different types of registration offices (Banks, post offices, local authorities, etc.) [64]

Another specificity of the Austrian solution is isolating of identity management development process out of the stakeholders. Thus, the banks, which, in fact, provide bank cards as tokens for the citizen card function and may be considered as identity providers, are not involved in development process. This represents difference in contrast to Norwegian IdM systems which are either developed by banks (e.g. the BankID) or interoperable with banks' IDs as a part of integrated solution (e.g. MinID).

Denmark

As well as Norway (so far), Denmark doesn't have neither mandatory nor optional ID card for citizens providing software-based identity management solution for online identification and digital signature while regular identities are still passports or driver's licenses. However, as in other considered countries, in Denmark all the data in the passport and the driver's license is derived from the Central Population Register (CPR) established in 1924 and maintained by local municipalities. Later, in 1968, unique personal identity numbers for citizens was introduced. The CPR-number is used in dealings with various public agencies, from health care to the tax authorities. Likewise the Norwegian identification number, CPR-number consists of the date of birth in the DDMMYY-notion and following sequence number reflecting the century of birth and sex of the holder(odd for males and even for females). In CPR registry a lot of private information associated with the ID number such as: name, CPR-number, CPR-number of parents, current/previous address, citizenship, date of birth, membership of national church, place of birth, private and public subscribers to changes in one of these data fields (e.g. universities, police, postal service, etc.) The Law on Personal Data guarantees to the citizens basic rights to know what information is used processed or may be processed. [65]

First, the idea of a citizen's ID card was introduced in 1992 followed by early attempts to introduce such a card. In 1995-2000, different attempts to develop such solution were taken on a various governmental levels but the attempts failed due to privacy concerns. Presented in 2002, the common public certificate standard "OCES" ("Offentlige certificater til elektronisk service" in Danish, "Public Certificates for Electronic Services" in English) was widely supported by public authorities and became mandatory standard for digital signature services. This OCES signature was also used for online authentication. The software certificates contains, among other data, personal identification number(PID) derived from the CPR-number. The PID may, however, be converted to the CPR-number. The largest telecom provider and operator TDC had been chosen as Certification Authority via first tender in year 2002. [65]

In parallel to governmental sector, by year 2000 banks consortium had developed and introduced their own solution called netID and used mainly for authentication in online banking services. The PBS, owned by the National Bank and a number of private banks, became the Certification Authority of the netID.[65]

Later in year 2009, all software solutions based on OCES certificates were combined with netID system into one identity management system NemID rolled out in 2010. The PBS is in charge of development and operation of the NemID. [65] This way represents a kind of similar to Norwegian path of development the identity management system where two mainstream solutions (the MinID and the BankID) is going to be covered by common interoperability HUB for digital identities provided by the MinID.

Sweden

Historically, the population registering in Sweden started in 17th century and personal ID number was presented first time in 1974 and now it's commonly used as a customer number by banks and insurance companies, and by public agencies, from health care to the tax authorities. The number consists of 10 digits: the date of birth in the DDMMYY-notion and following sequence number reflecting sex of the holder. Originally the public register was administered by the Church of Sweden, but by 1991 the task was handed over to the National Tax Authority. [66]

In Sweden, there are two types of eIDs ("soft" on a downloadable file and "hard" on a chip of a plastic card), 4 contracted private providers of eIDs and two official national ID cards. The national ID card "NIDEL"("National ID card prepared for E-Legitimation") is issued by the Police and doesn't include any eID solution; another is provided by the Tax Authority and may include also eID issued by Telia as an option. [66]

Sweden has a tradition to delegate issuance and managing of ID cards to post offices and banks. Thus, all eIDs are issued by contracted private parties and procured by government through "framework contracts" allowing issuance of IDs for a limited time. Online services provided by various public sector departments may accept contracted eIDs, however the actual use of a certain eID is based on business agreement between an identity provider and a department, and usually paid for use per transaction. Current four contracted identity providers, chosen on a tender base, are: "Swedbank" (heading the consortium of banks and representing the Swedish BankID solution), large Scandinavian bank "Nordea", Swedish telecom "Telia", and Steria (representing the IT security business). Provided eIDs are technically identical and based on similar specifications, also they include two certificate for signing and authentication respectively. The eIDs, however, differs at the interface level. Being theoretically accepted by all governmental departments, in practice eIDs are a matter of contract with identity providers and so number of supported identities differ from one service to another. All eIDs are regulated by the Law 2000:832 on qualified e-signatures, however existing eID solutions fulfill the criteria for advanced eID but not for qualified. [66]

The Swedish BankID solution represents services similar to the Norwegian BankID and provides the ID on file, smart card, and, recently, Mobile BankID. According the usage statistic, the Swedish BankID is currently the most used eID with 2.5 million unique users (as of 2010) and accepted by various government services, private companies and banks. Together banks have more than 5.5 million customers. Despite the Norwegian case where every bank is a registration authority and may issue the BankID, in Sweden only ten banks are issuers. The Swedish BankID is developed and maintained by the "Financial ID Technology" owned by most of the BankID member banks. The BankID services are also being sold to various relying parties in public and private sectors, however it's free for users. As of 2009, 1/3 of the population has eID and 75% of them uses BankID. [70, 66]

Despite other countries, the Swedish solution is rather stemming from a market approach with several private eID providers and distributed identity infrastructure. Likewise Norwegian and Danish case, the solutions are mainly software-based but a card may be issued as an option. [66, 71, 72]

Summary

National identity management systems in Norway, Sweden and Denmark represent as software certificates, while Germany, Austria and, optionally, Sweden offer also ID cards to citizens. In that sense, Norwegian software-based solution together with Swedish and Danish differ from common European standards of hardware-based chip-card solutions for identification and digital signature services, as considered to be more secure in comparison to software certificates.[71] However, the Norwegian government claimed to develop national ID cards for citizens as well. Besides, current version of the Norwegian BankID system has the wider area of application than most of considered IdM systems, going beyond basic identification and digital signing services, and provides also ePayment option. Nevertheless, in contrast to German eID card solution, it may not be and, most likely, will not be used for private online activities due to lack of privacy protecting measures.

In spite of more secure solution from privacy protection point of view, the IdM system in Austria has relatively low acceptance among users of the systems and shows a low level of usage of the IDs.[72] Whilst in considered Nordic countries the usage rate is much higher and tends to grow up. The German IdM solution was rolled out in November of 2010 and operates for relatively short period of time to make a reliable evaluation of acceptance rate.

The main influencing factor in development process of German and Austrian IdM solutions was privacy protection, while it, obviously, wasn't the main priority in the development of considered Norwegian and Swedish IdM systems and slightly influenced the solution implemented in Denmark. In its turn, from the beginning both Norwegian solutions were aimed to rather high interoperability and easy implementation of the systems than security and privacy protection.

Privacy and profiling risks, regarding the use of national identification number as a primary identifier, are considered to a variable extent in the considered countries. In Germany, high concerns about privacy protection and specific historic background led to full unacceptance of national identification numbers in any form. In Austria and Denmark, there is a working scheme of national number assignment prohibiting, however, to use numbers without prior modification. At the same time, cultural specificities of Sweden and Norway allowed successful implementation and acceptance of IdM systems fully based on directly used national identification numbers as primary identifiers.

Like in Norway, in Denmark and Sweden the key role of identity providers is played by bank consortiums, while in Germany and Austria the duties of issuance and management of identities are executed by governmental bodies itself. The reason for this is in traditional and cultural aspects of identity management. On one hand, the trust in banks and financial institutions is relatively high in Nordic countries and lower in Germany and Austria, on the other hand both Denmark and Sweden have, historically, a certain experience in delegation of identity management duties to a third party and so bank consortium.[71] In fact, Germany doesn't include banks in either development or execution of the solution, whilst in Austria banks are considered as ones of possible bodies to issue and support the ID, but they are not included into development process too.

Thus, cultural background makes the difference. For instance, considering the possibility of further spreading of the Norwegian BankID system, higher concerns about data protection in Germany and Austria along with avoidance of bank implication may prohibit from its spreading and result in low acceptance down to full ignorance of the system. At the same time, co-operation and integration with Swedish and Danish IdM systems is more likely due to similarities in a cultural background.

3.3 Conclusions: the fundamentals of large-scale IdM systems

3.3.1 The state and perspectives of Norwegian BankID solution

High levels of acceptance & dissemination of Norwegian identity management systems, especially the BankID solution, bear a lot of potential for both national level and cross-border IdM systems. A number of innovative functions and applications pave the way for new opportunities in electronic business processes. The success of BankID is built on government support provided through sound legal framework, specific cultural trust-related background, and effective organizational structure of the solution enabled by the strong interbank cooperation. Close cooperation between banking institutions within the Norwegian Financial Services Association and the Norwegian Saving Banks Association allows the BankID solution to dominate the market. In turn, technological and security features obviously were not handled with absolute care and top priority during the system design. The further evolution of the BankID and steps towards its implementation in a cross-border environment are hardly possible without addressing all open security & privacy issues. Integrability of the BankID also calls for improvements. The solution must provide federation and integration in order to assure flexibility of the infrastructure and to ease its implementation. Switching to the claim-based identity model and adding access control to user's data in certificates could be options. These options help to enhance privacy protection and security level adhering to minimal disclosure principle, and enable better federability and integrability of the entire system.

3.3.2 The seven fundamentals of large-scale IdM systems

Conducted research showed that large-scale identity management systems implemented in critical infrastructures, whether it's a national-wide IdM system provided as a part of e-Government solution or one used for online banking, are following seven minimally essential rules named here as "The seven fundamentals of large-scale IdM systems":

The use of IdM system in "a must" applications and services is a driving forcer to its successful adoption. The "a must" nature may be caused by two reasons: the use of the application or service may be enforced as the only option to perform obligatory actions (there's no way around); or due to the ubiquitous nature of the system. In this sense, banks are powerful influencers needed to be involved in development and exploitation of a national and, furthermore, a cross-border IdM system to assure its successful adoption. Banks provide services which a citizen cannot resist to ignore nowadays. Implementation of such IdM systems in online banking as the primary authentication method is a strong driving force for its acceptance and dissemination. It's easy to trace this tendency by considering the acceptance rate in countries where IDs are either managed by banks or used in their online facilities (e.g. Denmark, Norway and Sweden), in contrast to countries where they aren't (e.g. Germany and Austria). Extrapolating the tendency to international context, the fastest spreading and prevailing identities today are internationally functioning bankcards, enabled by close cooperation between banking and other financial institutions worldwide. Finally, banks traditionally remain a high level of public trust and aren't involved in political and cultural contradictions which make them even more stable identity provider. Therefore, banks' involvement and support are driving forces behind the creation of fast spreading and widely-accepted identity or IdM solution in an international context.

Public trust in IdM operating organization impacts on success of the system itself. Cultural aspects cannot be ignored during either development or implementation of (inter)national IdM system. The keystone to understand the aspects is to research public trust into an IdM operating organization such as government, banks or other public institutions, and especially in a way they handle citizens' data. Culture is a complex matter when it comes to international systems operating cross-border. A successful model implemented and operating in one country might become untrusted in a multicultural international environment.

Security and privacy requirements result from a cultural background. Privacy and profiling risks of use of national ID numbers are considered to a variable extent depending on cultural background. Germany doesn't have national identification numbers due to the historical background and high privacy concerns among citizens, Austria and Denmark don't allow direct use of the numbers, and Swedish and Norwegian solutions employ identification numbers without any prior transformations. Notwithstanding, the direct use of national identification numbers must be avoided in any large-scale IdM system due to the fact that it enables easy and low-cost profiling and creates serious potential privacy-related issues, leading to legal and compliance risks. Prior modification or encryption of the SSN could be used instead.

Interoperability, ease of implementation and ease of use of an IdM system are crucial factors for its success. An IdM solution should follow user-centrism principles, while the infrastructure needs to be developed considering service providers' needs. Otherwise it's hardly possible to achieve high acceptance and fast spreading. In these terms, software-based identities (e.g. certificates and other digital identities; Sweden, Denmark and Norway) show much better acceptance and spreading than hardware-based ones (e.g. ID cards; Austria and Germany). It's stemming from relatively better flexibility, easier implementation, and less costly and time-consuming management procedures (e.g. (de)provisioning, revocation, issuance, etc.) of the former. However, hardware-based IDs typically provide higher security level. Finally, a tendency to interconnect large-scale IdM solutions into a single IdM system proves the need in interoperability and easy federability by design.

Independent evaluations play vital role in IdM system refinement process. An IdM solution, especially large-scale (inter)national wide, requires independent audits and revisions in order to ensure its level of security and has to be open for independent third party evaluation. In that sense, readiness to deal with the results of examination and public availability of system documentation facilitate improvements through independent expert evaluation. Thus, early independent risk analysis and the investigation of client-software of the Norwegian BankID solution resulted in discovering multiple vulnerabilities. Based on the found vulnerabilities, risk mitigation strategies and its implementation by the bank consortium resulted in a new and higher security level. Even a start with imperfect system might be feasible and not necessarily lead to failure of the system.

A legal framework is a backbone of an IdM system. Laws and regulations must be considered carefully during its development process, since legal aspects may become serious prohibiting factor from evolution and spreading of a system in one case or a strong driving factor in another. Sound legal framework facilitates improvements and hardening of an IdM system, and provides opportunities to introduce new functionality. For instance, a regulation issued by the Norwegian Ministry of Finance allowed customers to open or switch banking or insurance accounts instantly. At the same time, excessively strict and complicated rules and laws make it impossible to develop and execute IdM system effectively, without significant costs and/or non-compliance.

IdM system is a sequentially evolving matter. A new solution must ensure the continuation of preceding legacy systems. All considered countries showed a strong tendency to path continuation in respect to nationwide IdM solutions. It means that sequential improvements and upgrades of existing IdM system are more likely than acceptance and further dissemination of either adopted outside solution or suddenly emerged novel one, developed without taking previous implemented systems into consideration.

Overall, an identity management system is a sociotechnical system, as the one comprised of both "socio" and "technical" components. It implies constant interaction between a human and a technical security system, where IdM is a cornerstone. Hence, an IdM system has to take into account differences in culture, privacy-awareness, security-awareness, maturity of users, etc. The IdM operator needs to adjust system to requirements of various group of user to provide them with desired system functionality.

4 Analysis of current cross-border inter-bank systems

Aiming to introduce interoperable identity widely accepted by multiple parties across borders, it's worth to learn from experience of currently existing cross-border systems and IdM solutions.

Today electronic banking is enabled by various interbanking systems widely employed by majority of banks worldwide. Thus, for example, SWIFT ("Society for Worldwide Interbank Financial Telecommunication") provides a de facto standard for worldwide financial messaging exchange between banks and other financial institutions. And IdenTrust provides a common identity platform for organizations which is interoperable across geographies, companies and applications.

Nevertheless, the most widespread identity after a passport is a bankcard[1]. Today everyone who has a bankcard can pay for anything almost everywhere anytime. This is an astonishing example of truly interoperable globally accepted identity. Moreover, these identities have earned a high amount of trust in the IdM system itself. It's a common practice to use only a bankcard to perform payments in either electronic or ordinary stores. It's hard to imagine today's life without bankcards. Often people don't even carry cash and nobody expects the system fails. More and more merchants accept bankcards all over the world, allowing customers from, say, Norway to buy chocolate in a store somewhere at Switzerland without any need to have a currency in the wallet. Therefore, the bankcard IdM model and experience are especially useful in the development of potentially successful cross-border identity for electronic banking.

4.1 Bankcards and VISA

Every day millions of people all over the world use bankcards to perform payments in "online" and "offline" environment. Even though they usually get the cards from different banks, these cards are, in fact, all the same in terms of technology and organizations behind. Today there are four large credit cards unions successfully operating in a global scale: American Express, Diners Club, and the two largest credit card networks – MasterCard and VISA[2]. Although both MasterCard and VISA dominate the credit card market, VISA is especially interesting case because it operates the world's largest payment network in terms of payments volume, total volume, number of transactions and number of cards in circulation. Therefore, the main focus is put on VISA.

4.1.1 Acceptance

VISA cards are widespread all over the world and accepted in more than 200 countries by tens of millions of merchant outlets and 1.8 million ATMs. According to the Nilson

[1] In this paper, the term "bankcard" is used as a collective notion which embraces all types of bankcards including prepaid cards (also known as cash cards), debit cards, and credit cards. The distinction between different types of bankcards is not important in this study.

[2] Here and further "VISA" (stands for Visa International Service Association) is used to denote the whole business and payment network, operating by both Visa Europe and Visa Inc., and "Visa" is for "Visa Inc." Visa Europe is a separate entity licensed by Visa Inc. to operate VISA's trademarks and technology in European region. The organizational structure of VISA will be discussed further

Report credit, debit and prepaid cards totaled 5.73 billion at year-end 2010.[73] As of December 31, 2010, Visa Europe issued 0.41 billion of cards and Visa Inc. issued 1.90 billions, so number of VISA cards totals around 2.31 billions or 40.3% of all bankcards circulating worldwide[3]. The cards are issued and managed by around 4 200 financial institutions in Europe and 15 500 financial institution customers of Visa Inc., totaling around 19 200 financial institutions all over the world who serve as an identity provider in the Visa's payment network, VisaNet.[74, 75]

The numbers clearly show that VisaNet can be considered as most ubiquitous and multi-party accepted IdM system nowadays. This success would not be possible without a sound business model and Visa's unique organizational structure.

4.1.2 Business Model

Although Visa company and its technology stand behind each issued card and each transaction in the payment network, the role of this organization isn't that obvious as it may seem at first. Visa doesn't issue identities (cards), manage related accounts, nor set rates, credit limits and fees for consumers. Neither do Visa interact with consumers or merchants. In general, Visa is not a bank or governmental organization. So, what is Visa, and what does it do?

Business processes

The main business processes of VISA are as follows[76, 75]:

- Managing, licensing and promotions of widely-accepted payment brands Visa, Visa Electron, PLUS, and Interlink;
- Provisioning of transaction processing and value-added services[4] through VisaNet and Visa Processing Services;
- Promotion and enforcement of a common set of operating regulations and by-laws;
- Securing of and investing in the processing payment network, VisaNet, and innovative payment methods and services.

The core business and the main goal of VISA are operating VisaNet to facilitates the secure transfer of value and information between consumers, merchants, and banks[5]. All activities unrelated to processing infrastructure are performed by banks-members of VISA which are acting as either issuers or acquires[6]. A bank-issuer issues cards to cardholders[7], sets fees and iterest rates, provides financial services, manages relationships with consumers as well as financial risks. In turn, a bank-acquirer is responsible for banking relationship with merchants and managing authorization capture and settlement.[76]

[3] For comparison, by the end of 2010 there were only 0.975 billions cards of MasterCard in circulation[73]

[4] For example, risk & fraud management services, consulting services, and education & training services, etc.

[5] VISA also subdivides its consumers (cardholders) and merchants into multiple categories and sets up different rule sets and fees for them to balance interests and security of products in a more effective way. Thus, for example, merchants could be: hotels, restaurants, shops, etc.; and consumers are: private individuals, governments, businesses of various size.

[6] Although it's a common practice for bankcard associations to concentrate business around the processing infrastructure delegating all unrelated tasks to banks and other financial institutions, there are exceptions. For example, American express has been acting as card-issuer for a long time.

[7] Physically, bankcards are made by the VISA itself in accordance with standards on physical security of credit cards. After the cards are produced, they are being provided to bank-issuer, which in turn can associate the bankcard with a certain cardholder through established registration process and KYC policy, and associate account information with the certain card.

Hence, five principal parties are involved into a typical transaction. A transaction process takes place in two stages: authorization (1-8) and settlement (9-12) (Fig. 10).

1. A cardholder either presents a card itself or provides the merchant with the account number, expiration date, billing address, and CVV2;
2. The merchant transmits an authorization request to the bank-acquirer;
3. The bank-acquirer sends the authorization request to VisaNet;
4. VisaNet passes on the request to the card issuer;
5. The bank-issuer approves or declines the transaction;
6. VisaNet forwards the authorization response to the bank-acquirer;
7. Thebank-acquirer forwards the response to the merchant;
8. The merchant receives the authorization and completes the transaction.
9. The merchant deposits the transaction receipt with merchant bank;
10. The bank-acquirer credits the merchant's account and submits the transaction to Visa for settlement;
11. VisaNet facilitates settlement, pays the bank-acquirer and debits the card issuer account, then sends the transaction to the card issuer;
12. The bank-issuer posts the transaction to the cardholder account, sends the monthly statement to the cardholder.[77]

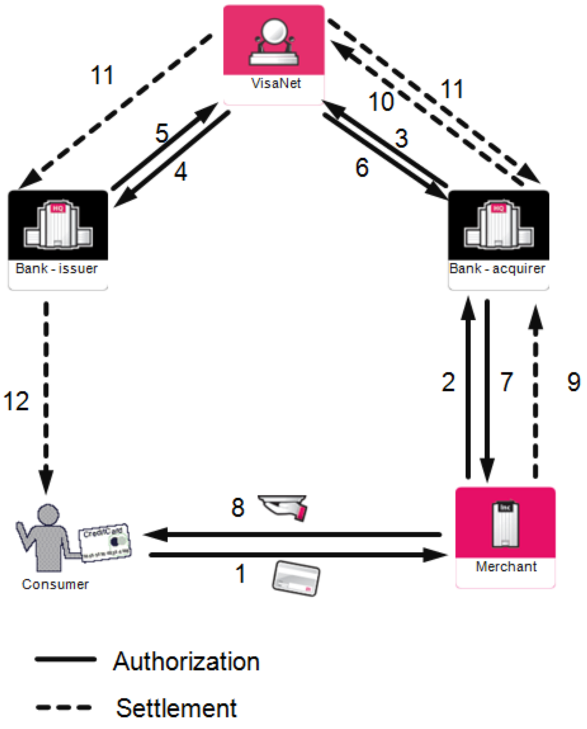


Figure 10: Typical Bankcard Transaction

It's worth noting, that among other counter-fraud measures VISA offers an internal insurance coverage for bank-members to compensate fraud losses. It provides additional assurance of the payment network.

Revenue flows

Bankcard associations, such as VISA or MasterCard, generate revenue flow from fees paid by member-banks based on payments volume, type of transactions and related services[8] (Fig. 11).

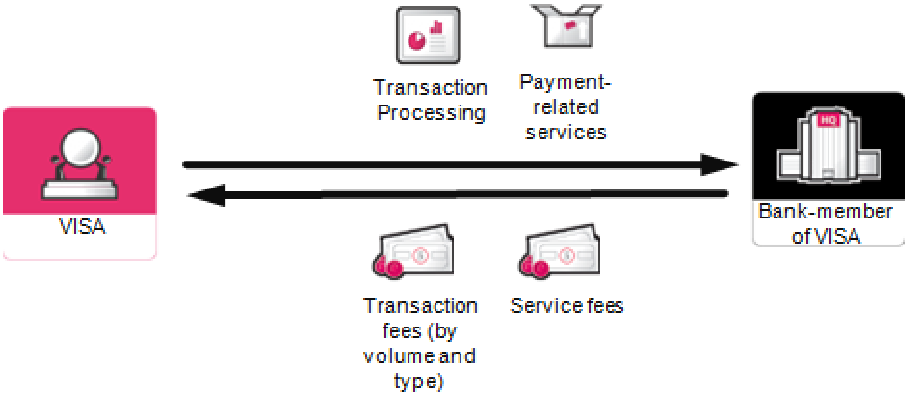


Figure 11: General Revenue Model of a Bankcard Associations

There are also so called interchange reimbursement fees. It is the transfer rate exchanged between bank-acquirer and bank-issuer, and aimed to balance the needs of parties at two-sided credit card market. The interchange fee is not a fixed fee, there are a number of different interchange rates varying by the type of retailer or product, geographical and other aspects. This rate may be a default rate set by VISA or be derived from negotiation between bank-issuer and bank-acquirer. The fee is paid by a merchant to the bank-acquirer within a Merchant Discount Rate (MDR) which may include also processing fee, connection and rental fees as well as acquirer's profit margin. A cardholder doesn't pay any interchange fee.[76, 78]

Therefore, the fees are collected either to cover expenses related to managing of and investing to the payments network, or to balance the two-sided market. The card association essentially may be considered as non-for-profit joint venture, however legally it's a for-profit organization. This low-cost orientation is derived from the specific organizational structure of the business.

4.1.3 Organizational structure

VISA has a unique corporate structure which became one of the factors led the company to success. Today VISA is regionally decentralized company consisting of Visa Inc. with multiple regional divisions and its licensee Visa Europe, which is a separate company. Since 2007, Visa is a publicly traded firm, most of the time in the company history it used to have a membership structure, where members were also owners. However, Visa Europe still remains the same membership structure.[74, 75] Decentralization allows Visa to offer different services for each region to comply better with local regulation and

[8] The full structure of VISA's operating revenue flows is as follows: service revenues, data processing revenues, international transaction revenues, other revenues, volume and support incentives.[76]

regional specificities, while its membership structure[9] allows members to share costs, making the bankcards available to even small financial institutions.

The history of VISA cards began in late 1950s, when the Bank of America decided to roll out their new credit card program to the market under the BankAmericard. However, there was a common for two-sided markets problem also known as a chicken-egg dilemma: merchants didn't want to lose money on processing creditcard transactions if there are not many cardholders, consumers doesn't need cards if they are not widely-accepted. The problem was solved through issuing thousands of unsolicited cards to all households in the test-region, and following aggressive advertising to consumers. Merchants started to accept cards, indicating this by placing a special mark[10]. In order to expand the credit card program further in other regions, the Bank Of America launched a licensing program, which was successful in the beginning but than face operational and organizational problems. Disbalance of power on one side and lack of effective control over the processes in the licensing program were leading it to a precipice.[79]

To provide widely accepted solution companies had to cooperate, and the Bank of America faced a problem of balancing competition and cooperation inside the newly appeared out of licensing program meta-organization of competing financial institution. Obviously, cooperation in the highly competitive environment is only possible through by-laws and regulations aimed to balance interests and providing mechanisms to establish trust inside the organization. Besides the Bank of America held the ownership of the brand, name and marks as well as all the power which ultimately led to distrust and conflicts of interests. The licensing structure simply couldn't compel cooperative behavior. [79]

The problem of competition was solved by Dee Hock, the founder and CEO of VISA, suggested the way to competition within a framework of cooperation via developing the set of principles:

> "*What if ownership was in the form of irrevocable right of participation, rather than stock: rights that could not be raided, traded, bought, or sold, but only acquired by application and acceptance of membership?*
>
> *What if it were self-organizing, with participants having the right to self-organize at any time, for any reason, at any scale with irrevocable rights of participation in governance at any greater scale?*
>
> *What if power and function were distributive, with no power vested in or function performed by any part that could reasonably be exercised by any more peripheral part?*
>
> *What if governance was distributive, with no individual institution or combination of either or both, particularly management, able to dominate deliberations or control decisions at any scale?*
>
> *What if it could seamlessly blend cooperation and competition, with all parts free to compete in unique, independent ways, yet able to yield self-interest and cooperate when necessary to the good of the whole?*

[9] It's worth noting, that the same membership structure, when members are also owners, has been employed also by another industry-leader - MasterCard. Both companies was forced to public offering due to a number of anti-trust cases caused by dual membership of some financial institutions in both joint ventures, VISA and MasterCard association.

[10] Today it's the VISA's logo, back in the days it was the same 3-colored band logo with name BankAmericard on it, instead.

> *What if it were infinitely malleable, yet extremely durable, with all parts capable of constant, self-generated, modification of form or function without sacrificing its essential purpose, nature, or embodied principle, thus releasing human ingenuity and spirit?*" [80]

These principles describe an organization of the whole new type referred to as "chaordic" by Dee Hock. He defined the "chaordic" as " *The behavior of any self-organizing and self-governing organism, organization, or system that harmoniously blends characteristics of chaos and order.*"[80] He believed that decentralized, self-organizing, and self-governing chaordic organizations are more flexible and adaptive, and can provide necessary cooperation framework. In the year 1976, the company called VISA, following this principles, had emerged. From this moment there have been issued only cards branded with name VISA despite of bank-issuer.

4.1.4 System Architecture

VISA operates VisaNet processing payment network which is a core of VISA's business. Under the name VisaNet stands two principal systems: BASE I, realtime and online system, and BASE II, batch-oriented system. These systems serves for authorization, and clearing and settlement respectively. The VisaNet is a centralized[11] and modular payments network with hierarchical local star topology. VISA claims that such centralized architecture provides an ability to view and analyze each authorization transaction in real-time to provide value-added information[12]. There are four data centers worldwide: one is in UK, another one is in Japan, and two US data centers which can serve as redundant and process all world payment traffic. Financial institution and, sometimes, large merchants are connected through VisaNet Access Points acting as gateways to main clearinghouses. [82, 83]

4.1.5 IdM Perspective

From IdM point of view VISA cannot be considered as an identity provider. In fact, the role of an identity providers are served by bank-members of VISA. The role of VISA in this system is rather a trusted third party which stands up in every transaction, assuring validity and acceptance of the identity.

VISA 3-D Secure Protocol

For secure online authentication VISA developed its own XML-based protocol called 3-D Secure and 3-D Secure Service based on this protocol, which later has been adopted by another major bankcard company MasterCard in Mastercard SecureCode. The protocol replaced previously employed SET protocol[13].

The 3-D Secure protocol divides payment systems into three domain (see Fig.12):

- **Issuer Domain** consisting of systems and processes performed by the issuer and its cardholders.
- **Acquirer Domain** consisting of systems and processes performed by the acquirer and its merchants.

[11] In contrast to VISA's centralized network, MasterCard operates contrary structure. MasterCard's BankNet has decentralized peer-to-peer network architecture which is built as a VPN network.

[12] For example, this information can be used in VISA's advanced authorization service acting as anti-fraud neural network to detect behavioral anomalies of consumer's payment activities on account level.[81]

[13] Secure Electronic Transaction (SET) protocol[84] had been developed by VISA and MasterCard in 1990s to secure credit card transactions in the Internet.

- **Interoperability Domain** enables Issuer and Acquirer domains to interoperate.

Essentially the 3-D Secure Service architecture is built as service oriented architecture (SOA), where the Interoperability domain is the core. Typical steps of purchase transaction flow in 3-D Secure protocol are following (Fig. 12):

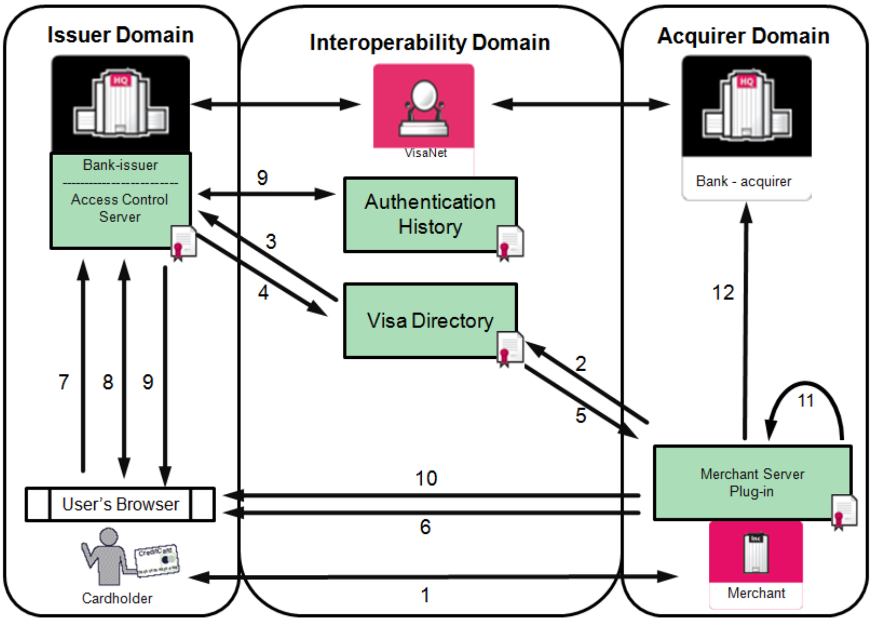


Figure 12: VISA 3-D protocol transaction flow

1. Cardholder submit card information to merchant to finalize purchase;

2. Merchant Server Plug-in (MPI) sends the PAN (and user device information, if applicable) to the Visa Directory Server

3. The Visa Directory Server queries the appropriate Access Control Server (ACS) to determine whether authentication (or proof of attempted authentication) is available for the PAN and device type. If it's not available, processing continues with step 5;

4. The ACS responds to the Visa Directory, indicating whether authentication (or proof of attempted authentication) is available for the card number;

5. The Visa Directory Server forwards the ACS response (or its own) to the MPI. If neither authentication nor proof of attempted authentication is available, the merchant, acquirer, or payment processor submits a traditional authorization request;

6. The MPI sends a Payer Authentication Request (PAReq) to the ACS via the shopper's device;

7. The ACS receives the PAReq;

8. The ACS either authenticates the shopper by using processes applicable to the card number (password, chip, PIN, etc.) or if attempts ACS functionality is available,

creates the proof of authentication attempt. The ACS then formats the PARes message with the appropriate values and signs it;

9. The ACS returns the PARes to the MPI via the shopper's device. The ACS sends selected data to the Authentication History Server (AHS);
10. The MPI receives the PARes;
11. The MPI validates the PARes signature (either by performing the validation itself or by passing the message to a separate Validation Server);
12. If appropriate, the merchant proceeds with the authorization exchange with its acquirer. Following Step 12, the acquirer processes the authorization request and returns the authorization response to the merchant. [85]

Cardholder's prior identification takes place during the enrollment process by the bank-issuer. Transport security and message integrity is provided through the use of SSL/TLS and issuer signature on authentication response. Visa also runs PKI for use in conjunction with various products and services. The certificates are issued to entities participating in vast online transactions (Fig. 13 (source: [86])). [85, 86]

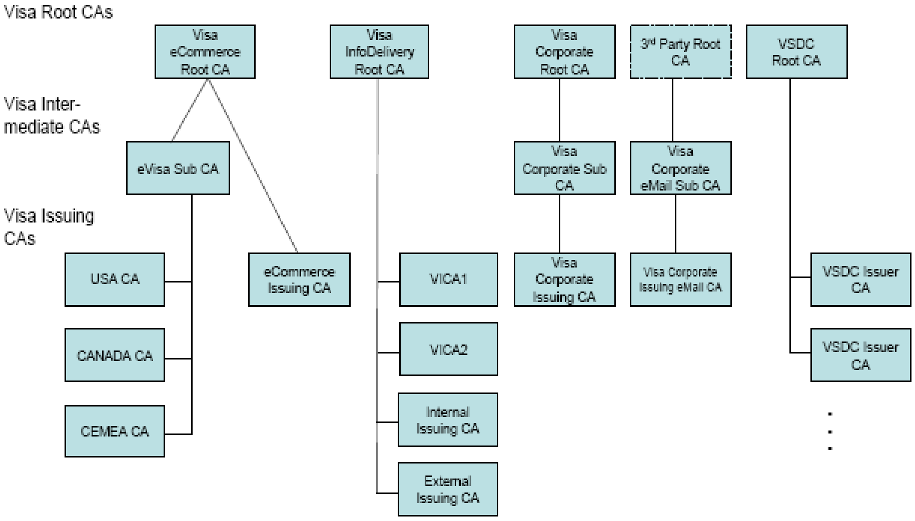


Figure 13: Visa PKI Hierarchies

The identity and its attributes

Each bankcard contains a standard set of attributes including cardholder's name, the name of a bank-issuer (identity provider), brand mark of a payment system (e.g. VISA, Mastercard, etc.), expiration date, class of the ID card (e.g. VISA classic, gold, or platinum), type of the ID card (e.g. debit, credit, prepaid), cardholder's signature, ID card security code (CVC2/CVV2), serial code of the ID card. Bankcard number, in turn, is the primary account number.

The identity is static and cannot be dynamically managed following partial or minimal disclosure principles.

A bankcard expiration period may vary from two to five years.

Privacy and user-centricity

The bankcards are user-centric identities, and all associated activities are performed by a user except issuance and "revocation" of the ID-cards.

The bank-issuer owns and often shares the cardholder data. In general, information about both a purchase and the entity, who makes the purchase, is available to all parties involved into transaction: the merchant, bank-issuer, and merchant's bank. The collection of certain information and assuring traceability of the transaction by banks are required by various anti-money laundering regulations. Parties involved into transaction are responsible for proper protection of processed information and compliance with data protection laws. However, there are quasi-anonymous gift and prepaid cards which can provide certain level of anonymity to the cardholder.

Application areas

Bankcards are used only within one context of payments. They can be used to perform payments either online or offline.

4.1.6 Assuring Interoperability

Due to its decentralized organizational structure VISA is able to effectively comply with Data Protection and Financial regulations in different regions. Each separate division and licensee (Visa Europe) have their own regional operating regulations which are bridged by Visa International Operating Regulations in order to assure legal and organizational interoperability, and enable interregional interchange. The layered structure of regulations and by-laws is depicted in figure below.[87, 88] Significant differences in data and privacy protection laws in EU and US as well as legal implications related to interchange processes are aligned with EU Safe Harbor Privacy Principles.[89]

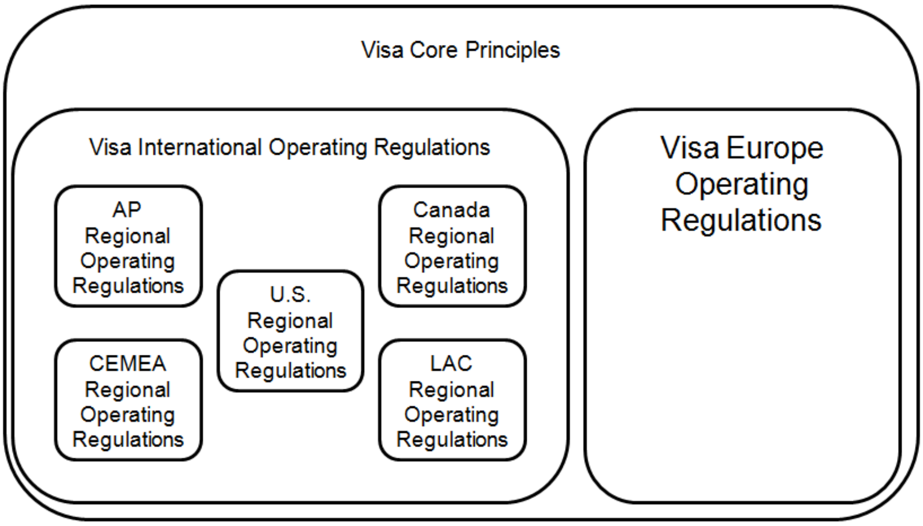

Visa Core Principles
Visa International Operating Regulations
AP Regional Operating Regulations
Canada Regional Operating Regulations
U.S. Regional Operating Regulations
CEMEA Regional Operating Regulations
LAC Regional Operating Regulations
Visa Europe Operating Regulations

Figure 14: The layered structure of VISA regulations

Interoperability at semantical and technological levels are assured via internal technological standards on protocols, data exchange and message structure, and supported by international standards[14]. Moreover, the ID cards itself are standardized on hardware

[14] For example, ISO 8583 on message structure, ISO/IEC 7812 on bank card numbers, ISO/IEC 7816-3 on the transmission protocol between chip cards and readers, etc.

level as often have single EMV chip, a globally standardized integrated circuit card.

4.2 SWIFT and 3SKey

History of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) dates back to 1973 when 239 banks in 15 countries joined together to create a communication link between banks worldwide. SWIFTNet is a backbone of today's financial world, providing de-facto standard for secure exchange of financial messages between banks and other financial institutions worldwide. Additionally, SWIFT provides corporate treasures of large organizations with tools for electronic bank-account management (eBAM). Among the variety of SWIFT product, from the IdM point of view the main interest is of recently announced 3SKey service, allowing corporates to authenticate and manage multiple banking relationships within a single ID.

4.2.1 Acceptance

As of the end of 2010, SWIFT interconnects 726 corporates and around 9000 financial institutions in 209 countries.[90] The 3SKey service was launched in October of 2010. During the prior pilot phase it had been adopted by few large companies and major banks in France and Germany. Currently, the service is available for all SWIFT users through standardized international platform which, in turn, may facilitate its further spread out.

4.2.2 Business Model

In essence, SWIFT is a member-owned cooperative providing secure electronic message exchange between its clients, mainly financial institutions. It doesn't perform clearance, settlement, account management or any other processing function but transport.

Organizational structure

Likewise bankcard associations, SWIFT is non-for-profit member-owned joint venture under Belgian law whose members are mainly financial institutions. Despite the total amount of over 9000 financial institutions interconnected by SWIFT, only around one-third of them are member-shareholders. In contrast to initial bankcard associations organizational structure, it's possible to be a user of SWIFT services for institutions who are not-eligible for shareholding. [91, 92] SWIFT users are organized in three user groups as defined in SWIFT corporate:

- Supervised Financial Institution (incl. members-shareholders);
- Non-Supervised Entity active in the financial industry;
- Closed User Groups and Corporate entities[15]. [93]

It's not possible to access SWIFT network and value-added products without being a member of the SWIFT community. Historically, it became one of the drivers for fast membership growth in 1990s.[94] At the same time, this and high costs related to membership are the factors preventing small banks and businesses from participating in the SWIFTnet message exchange network. Moreover, a corporate has to meet a set of strict eligibility criterion in order to become a member of the SWIFT community.[92]

From the beginning, when the SWIFT just started development of network, the member-ownership had a unique structure. Members were given shares based on their traffic volume and use of the network. Each share also obliged the shareholder to give a loan (up

[15] Corporate clients are connected to the SWIFT network through the banks.

to $1000 per share) to SWIFT which allowed them to repay costs in development phase. Besides, they charged all members an entrance fee[16]. [94, 91]

Today, the company has three divisions representing three main regions: Asia Pacific, EMEA, and Americas. This allows to adjust marketing and legal policies according to regional specificities. All daily operations are delegated to four operation groups including: marketing group, IT operations group, stakeholder relations group, and finance and administration group.

Business processes

The core corporate functions are facilitating secure and reliable message exchange among users of SWIFTNet as well as to set up and maintain standards. The standardization and regulation activities has always been of the same importance as managing their primary product - messaging network. Since the 3SKey service is in the focus, further we will consider business processes and specific model related solely to this service.

The 3SKey solution allows corporate treasurers to access multiple banks within a single token with PKI certificate. In order to enable the service, SWIFT mediates between banks (referred to as 3SKey subscribers) and corporates (referred to as 3Skey users). It provides inactive token to the subscriber(1) which, in turn, redistributes it to the user(2). Latter activates the token at 3SKey portal(3) [17], which generates an anonymous certificate on the 3SKey token(4), containing only unique ID. Next, the subscriber has to associate the user with this anonymous certificate(5). Therefore the identity is only known to the bank-subscriber and the user. Finally, the corporate may use this certificate to sign documents and files exchanged with this 3SKey subscriber[18] either via SWIFTnet or any other channel (e.g. the Internet) (Fig. 15). [95]

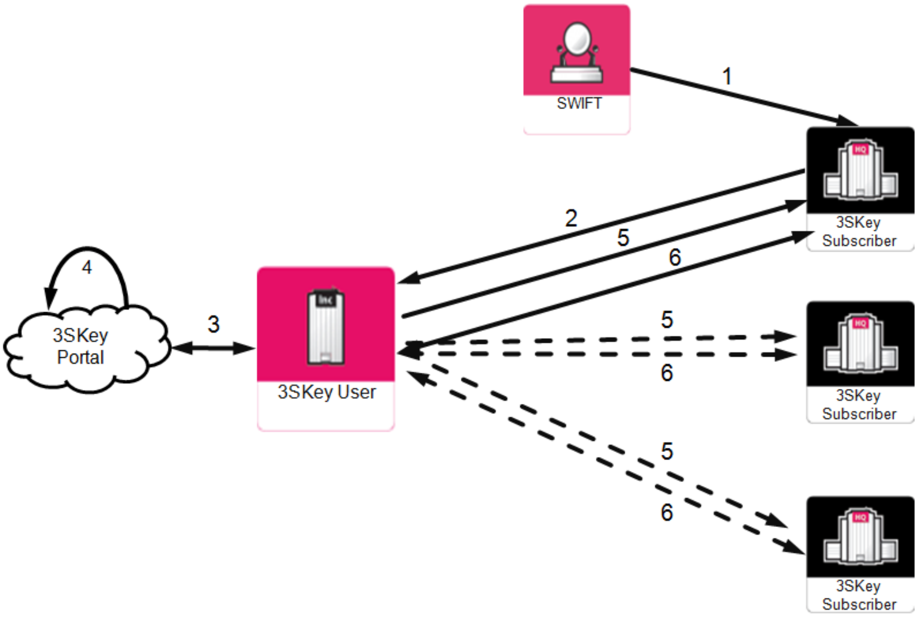


Figure 15: SWIFT 3SKey solution

[16] In fact, both an entrance fee and "*annual financial contribution*" exist to present day.
[17] The activation process doesn't require any identification information
[18] In order to use the ID with other subscribers, activation step has to be repeated with each 3SKey subscriber.

In a nutshell, SWIFT is responsible for service provisioning through management of the PKI infrastructure and issuance certificates; while banks redistribute tokens to users, link users to tokens, and perform signature verification afterwards.

Revenue flows

End users, typically corporates, have to buy the service from 3SKey subscribers and therefore are not considered in revenue flows derived from the 3SKey service by SWIFT. The 3SKey subscribers, besides general fees[19], pay to SWIFT the following charges for the use of 3SKey service (Fig. 16):

- one-time service fee for the subscription by 3SKey subscribers to the 3SKey service;
- yearly recurring fee for subscription by 3SKey subscribers to the 3SKey service;
- one-time fee for the supply of the 3SKey tokens.[95]

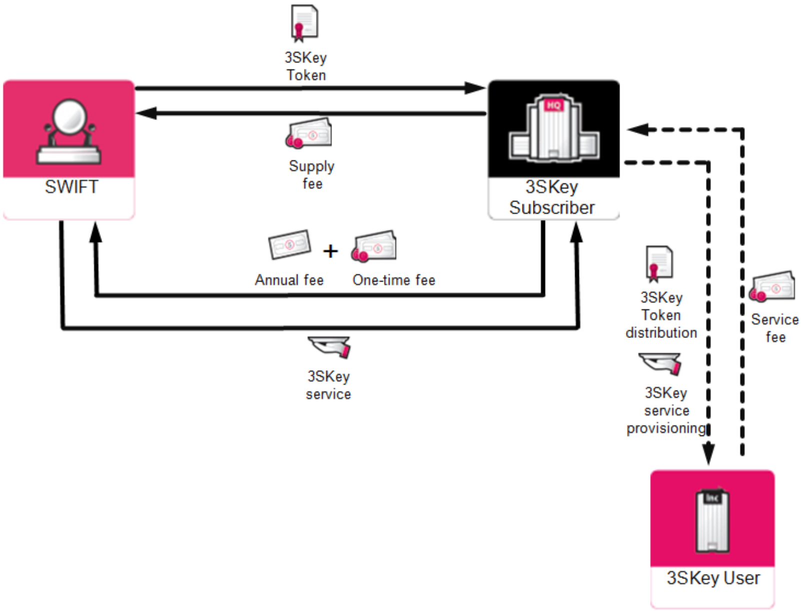


Figure 16: SWIFT 3SKey Revenue Flows

4.2.3 System Architecture

The 3SKey solution is a typical PKI implementation. Its centralized infrastructure consists of 5 main components (Fig. 17 (Source: [96])):

- SWIFT PKI;
- 3SKey tokens;
- 3SKey portal (the certificate management facility);
- 3SKey certificate revocation check facility;
- 3SKey developer tookit. [95]

[19] E.g. annual fee paid by all bank-members based on network usage and/or an entrance fee for initial connection to the SWIFT network

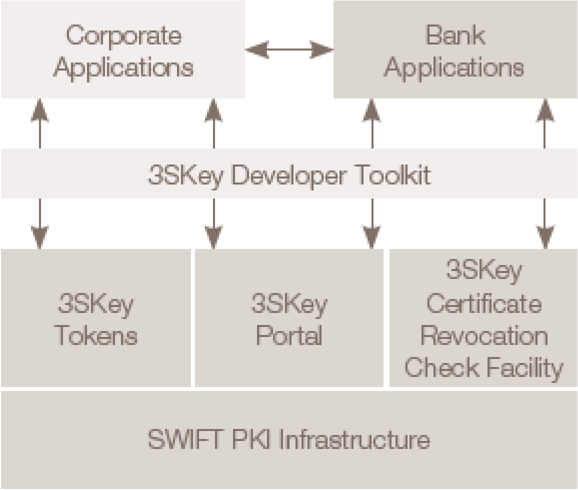


Figure 17: SWIFT 3SKey Components

4.2.4 IdM Perspective

In 3SKey system, SWIFT acts as a trusted third party. In terms of PKI, SWIFT executes the roles of certification and validation authority, and a bank-subscriber is registration authority. The trust model is hierarchical and typical for any PKI implementation. The root CA in this case is SWIFT.

The identity and its attributes

The ID is X509V3 certificate supporting PKCS #7 v1.6 [97, 4] formatted signatures. The issued ID is valid for 3 years.

Each identity has following attributes: the distinguished name of the certificate containing the unique id number[20], certificate serial number, the issuer of the certificate (SWIFT), the date of issuance, the expiration date, the object identifier of the token's certificate; token serial number. [98]

Each token storing the certificate has an access control realized by means of password protection. The 3SKey Service supports SHA-256 with RSA encryption as a signature algorithms length. The RSA key is of 2048 bits length.

Privacy and user-centricity

Even though the users of 3SKey solution are corporates only and the notion of privacy cannot be applied to a legal entity, it can be replaced with confidentiality following the same principles of privacy.

The identity is user-centric and has a certain level of confidentiality protection through pseudonymous certificates, which allow the identification of certificate-holder only to specific parties after the prior association process.

Application areas

The identity can be used for authentication, digital signing and encryption. Application scenarios include electronic bank account management, and signing and exchange of electronic documents.

[20] The distinguished name has the following format: cn=corp<nnnnnnnn>, ou=section_n, ou=personalid, o=swift, c=ww. The "cn" field is the unique ID number of the certificate

The application area and number parties using the certificates are limited to members of the association.

4.2.5 Assuring Interoperability

Because of its common centralized infrastructure, and the use of single standardized technology, interoperability issues for SWIFT 3SKey service can generally exist within the levels of legal and organizational interoperability. SWIFT overcame these issues in a similar way to VISA did. SWIFT organized business in three separate divisions and this allowed to adjust operational and legal regulations to a region specificities. The differences in data protection laws between EU and US is aligned through the Safe-harbor directive. In turn, organizational interoperability is solved through a membership structure and internal regulations for all participants in the system.

Besides, the significant achievements in development standards for financial systems and message exchange formats led to semantical and technological interoperability of SWIFT solutions in general, throughout financial services.

4.3 IdenTrust

IdenTrust was founded in 1999 by a group of financial institutions, including few major players such as Citigroup and ABN AMRO. The company operates a PKI-based Trust Infrastructure to provide authentication, encryption and digital signing services to its clients.

4.3.1 Acceptance

There are no publicly available operational statistics regarding usage, acceptance, and dissemination rates of IdenTrust products, neither do they disclose information about the number of participants in IdenTrust network.

Nevertheless, IdenTrust claims that its identities are globally interoperable and legaly accepted in around 175 countries through the set of rules[21] developed and agreed to by 55 financial institutions worldwide. [99]

4.3.2 Business Model

IdenTrust is responsible for management of the IdenTrust Trust Infrastructure, based on PKI, and PLOT framework to provide secure and compliant business-to-business platform for data exchange. It doesn't store, settle, nor validate exchanged data between users, but solely validates their identities.[100] IdenTrust also provides digital certificates solutions for US and UK governments as a part of deployed critical infrastructure protection programs : ACH BACSTel IP in UK, and ACES/ECA in US.

Among other products, the IdenTrust Trust Prime is of special interest in this case study. It provides corporate treasurers with the cost-effective electronic bank account management solution, allowing them to manage accounts and signatories via secure exchange of electronic documents, single identity for multi-bank authentication, and non-repudiation. [101]

Organizational structure

IdenTrust is for-profit organization. It was founded by major banks, but it has traditional hierarchical organizational structure with headquarter in the US, and international

[21] This rule set is referred to as P.L.O.T. - policies, legal and operational framework - and will be discussed in more details further.

offices in EU and Japan. The company offers a single set of products all over the world, while interoperability provided via the PLOT framework.

Business processes

IdenTrust facilitates secure data exchange between users without processing transfered data. The main business processes are related to maintenance a set of legal and operational regulations known as PLOT and core infrastructure management. The participation in network services has a membership structure, where IdenTrust provides services through the bank-members who adopted the PLOT framework and got connected to the IdenTrust network.

The signatures of all parties participating into a transaction are validated by IdenTrust in order to provide mutual authentication. To validate certificates in real-time, IdenTrust banks require the serial number and name of the issuer of the digital certificate. The IdenTrust Trust Network doesn't perform any centralized routing in order to assure confidentiality and privacy protection of data exchanged between the bank customers on either end of the transaction. [100] The data flow of a typical transaction is depicted in figure 18 (Source: [100]).

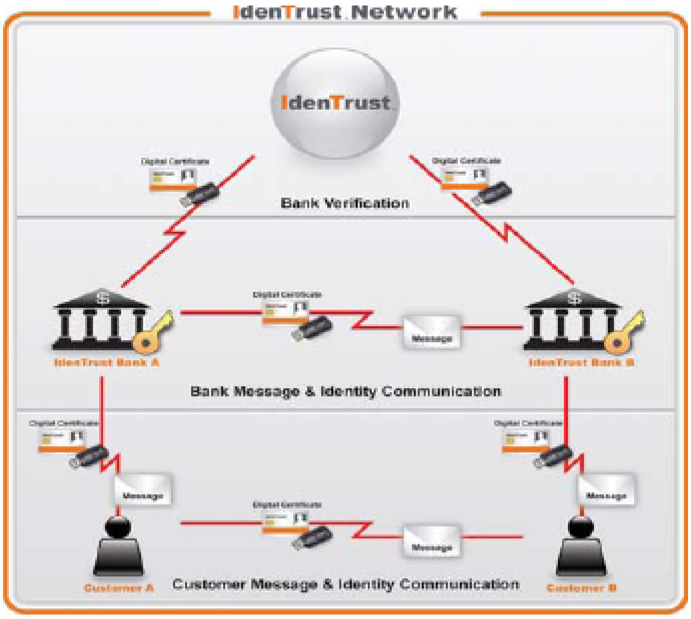


Figure 18: IdenTrust Transaction Data Flow

In order to get connected to the network, the following actions should be performed:

1. Customer register with a member-bank by agreeing necessary Terms & Conditions specified in the IdenTrust rule set;

2. The bank validates the the information through customer identification process with KYC policy;

3. The bank sends an activation information and the fulfillment package to the physical address of applicant via out-of-band delivery channel (e.g. postal service);

4. The applicant generates and retrieves digital certificate using the activation information via entering the delivered activation code at activation portal of certificate management center;

5. The user can then use issued ID to authenticate at bank-IdP's web-based portal in order to manage signatories, bank accounts, or legal entities.[99]

The usual account opening transaction, for example, is performed in six step after signing the account opening request form step by step by: requester, approver, and authorizer on the corporate side, and then compliance, relationship and implementation officers on the relying bank side.[101, 102]

Revenue flows

Most revenue flows is derived from three main sources: an entrance fee for joining IdenTrust Network, annual subscribtion fee, and individual transaction charges (Fig. 19).

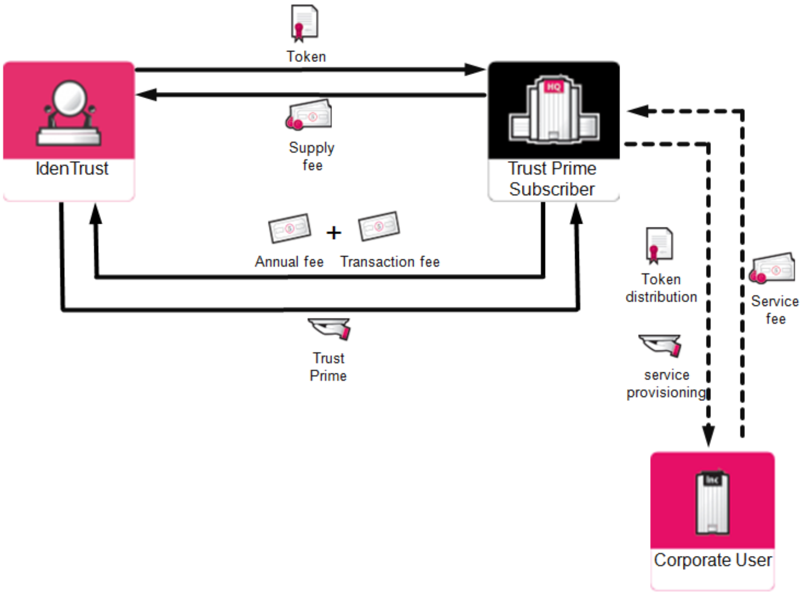


Figure 19: IdenTrust Revenue Flows

4.3.3 System Architecture

The IdenTrust Trust Network is a centralized PKI-based infrastructure. It consists of 2 principal categories of components:

- The IdenTrust Infrastructure, including Certificate Authority (CA), OCSP Responder, Hardware Security Module (HSM), Subscribing Customer Key Storage and Sub-system, Digital Signature Messaging System (DSMS), amd Transaction Coordinator (TC).

- Relying Customer applications required to correctly accept and process IdenTrust credentials. This category includes but not limited to operating systems, custom applications (e.g. Trust Prime application), etc. [103]

4.3.4 IdM Perspective

From the IdM perspective, IdenTrust acts as a trusted third party and IdP. In terms of PKI, IdenTrust executes the roles of certification and validation authority, and acts as a root CA, while a bank-client is registration authority responsible for identification of its customers through the KYC policy procedures.

The identity and its attributes

The Identity is a X.509 v3 SSL certificate. IdenTrust provides two types of Trust Network Certificates: computer certificates, bank certificates for authenticating the identity of the users. The detailed information about the certificates is classified as confidential and not available for public review.

Privacy and user-centricity

The identity is user-centric and may be considered as confidential in respect to data protection. However the certificate holder can be easily identified not only to parties exchanging data, but to the network operator as well.

Application areas

The identity can be used for authentication, digital signing, or encryption. Application scenarios include electronic bank account management; documents, payment files, and invoices signing; and securing access to web-servers.

The application area and number of parties accepting certificates are limited to bank-members (service and identity providers), participating in the network.

4.3.5 Assuring Interoperability

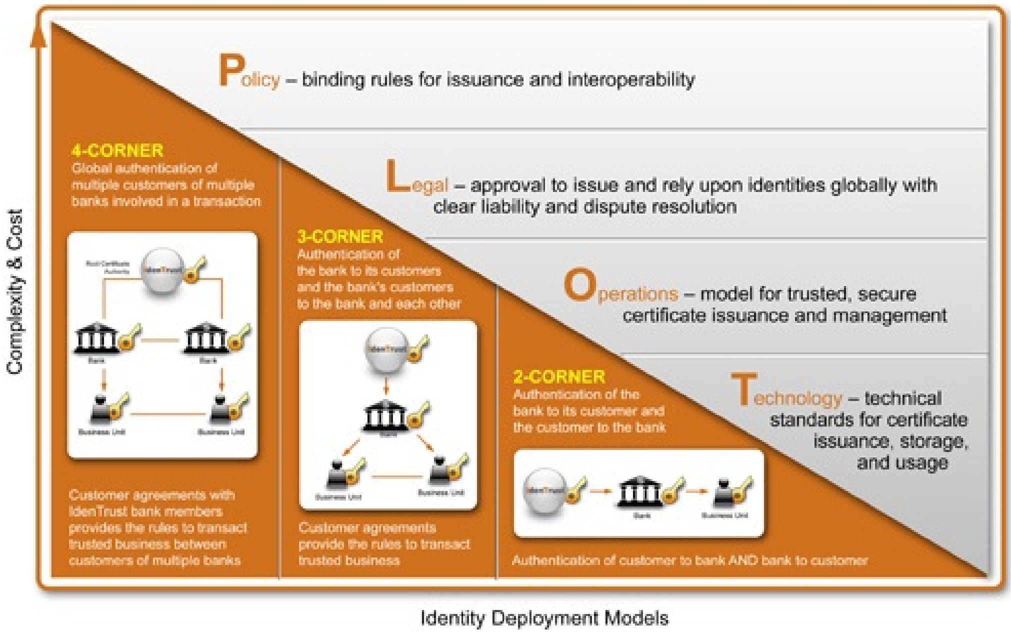

Policy – binding rules for issuance and interoperability
Legal – approval to issue and rely upon identities globally with clear liability and dispute resolution
Operations – model for trusted, secure certificate issuance and management
Technology – technical standards for certificate issuance, storage, and usage
Complexity & Cost
4-CORNER
Global authentication of multiple customers of multiple banks involved in a transaction
IdenTrust
Bank
Bank
Business Unit
Business Unit
Customer agreements with IdenTrust bank members provides the rules to transact trusted business between customers of multiple banks
3-CORNER
Authentication of the bank to its customers and the bank's customers to the bank and each other
IdenTrust
Business Unit
Business Unit
Customer agreements provide the rules to transact trusted business
2-CORNER
Authentication of the bank to its customer and the customer to the bank
Bank
Business Unit
Authentication of customer to bank AND bank to customer
Identity Deployment Models

Figure 20: IdenTrust P.L.O.T. framework

One of the central operational task for IdenTrust is to assure cross-border interoperability of the Trust Network Infrastructure in both organizational and legal levels.

In order to align the IdM system within various regulations worldwide[22], IdenTrust in collaboration with bank institutions developed so called PLOT framework (Fig. 20 (Source:[104])). PLOT is intended to covers developing and deploying of the Trust Infrastructure.

The possible interoperability issues on semantical and technological levels has been overcome through the use of single PKI implementation and same standardized certificates across contexts and products.

4.4 Conclusions

IdM system creates value through a value network, rather than a typical value chain.[23] The value of an IdM system is in effective mediation between relying parties (e.g. service providers, merchants) and entities (e.g. identity-holders, cardholders). The economics of IdM and assets (both tangible and intangible) need to be analyzed from different perspectives of various participants contributing to creation networked value. Moreover, another important characteristic of a value network has to be taken into account: value networks create business ecosystem which ultimately facilitates growth of its components. Thus, SWIFT, IdenTrust and VISA solely concentrate their business over IdM related tasks, leaving creation of added value products to its customers, participating in ecosystems. rather than on ensure the interoperability of IDs, compliance and interoperability on various levels, and the security of identity through the control over production of the physical token/card, management of secure infrastructure, and standardization and regulations of operational activities.

An identity management system is a two-sided market.[24] Typical identity management system has three corners: a relying party, an identity provider and an entity. At early stages of implementation of an IdM system, an identity provider is interested in fast and wide spread out of identities in order to provide access to a service to as many people as possible. However, it constantly faces a chiken-egg problem: users will want to get and use ID only if there are enough relying party willing to accept it; on the other hand, relying party doesn't want to suffer additional losses from implementation and integration of an IdM system until enough customers use the identities. Therefore, business operating an IdM system (typically it's also an identity provider) has to always balance interests of both sides in order to keep equilibrium in the system and allow its growth and dissemination.

An identity management system is a subject of network effect, when a user of the system affects value of offered system. The more customers use the system, the more popular it becomes. It's clearly seen in example of SWIFT network, where the number of members in the society, and so number of participants in the network exchange, grew exponentially throughout the history. The network effect is comprised of cross-side and often same-side one. Cross-side network effect implies that service providers will more likely adopt the IdM system if it has a large base of users on the other side. The same-side effect implies that growth of number of participant on the same side increase system's

[22] IdenTrust claims compliance with number of regulations such as: Sarbanes-Oxley (SOX), the Single European, Payment Area (SEPA), the Markets in Financial Instruments Directive (MiFID), Know Your Customer (KYC) and Know Your Customer's Customer (KYCC) policies, USA Patriot Act, Electronic Signature Laws in EU and US, US - EU Safe Harbor Directive, and United Nations, World Trade Organiztion, and FATF guidelines

[23] There are three principal ways to configure value[105]: value chain[106], value network [107, 108, 109], and value shop[105, 110]

[24] More on two-sided markets: [111, 112, 113, 114]

value for the same side.[111] This principle may be extrapolated to all components of an IdM system: technology [25], semantic of ID [26], and so on.

Membership structure (associations) of organization is a very promising way to provide legal and organizational interoperability and balance interests of participants. As histories of success of VISA and SWIFT have shown, the most effective way to balance interests in the association, and overcome legal, organizational and operational issues is the association and so called "chaordic" type of organization. In contrast to VISA, which chosen membership-owning organizational structure solely to overcome organizational and operational issues, SWIFT made this choice also to pay out development of their messaging network SWIFTnet.

Neutral trusted third party organizations, such as associations, allow to build trust into a system easier. As it was shown in previous chapter, IdM systems acceptance and usage are influenced by cultural specificities, especially public trust in IdM operator, to a high degree. The important role of cooperation and membership structure is in building trust in the IdM operating organization. Financial institutions separately may not trust to nor follow guidelines of their competitors, but they trust the established meta-organization (e.g. VISA or SWIFT). Besides, the associations and memberships allow to build public trust into system and the IdM operator on user side.

The mark/sign of trust. This feature stems from the previous one. Although the trust is built in the IdM operating organization, the sign (in a form of logo, brand or trademark) is the representation of this organization behind and the trust in it. All considered systems use the same mark for their IDs. This allows customers to identify quickly the service providers accepting a certain ID, they, in turn, can accept the ID signed electronically and marked with the logo/brand of the IdM operating authority. At first glance, it may seem rather obvious and not relevant, however the history of VISA [79] proved the importance of single sign through the negative experience of licensing program when card-issuers weren't required to mark the card with a single logo. The same we can apply for digital identity management systems, denoting the significance of the single mark for successful adoption of the system.

Overall, the business model is an essential element which bridges all influencing factors and system features, adjust to user's interests and ultimately create value. The business model is aimed to leverage interests in a complex set of interactions between different parties.

[25] The more popular technology, the more systems use it

[26] The more spread out and standardized an identity, the more systems use the same structure, the more often semantical interoperability is possible among various IdM systems, and, consequently, the more system can be interconnected and integrated enabling wider spread out of IDs

5 Design of Architecture and Business Model

This chapter describes value creation process, proposed design of potentially successful business model and architecture needed to enable cross-border interoperable IdM system in electronic banking. Herein, the proposed system is referred to as "EBIMS" [1].

5.1 Design of Optimal Business Model

5.1.1 Market Forces

Business models are designed for and operated in a specific environment which has to be taken into account to compose a competitive business model. There are seven general groups of stakeholders that are either targeted at the same market, involved in operations, or require certain functionality from the EBIMS (Fig. 21). In turn, the stakeholders can be divided into three categories based on the type of involvement: operation & use (active actors), supervision & audit (passive actors), and competition. All together the stakeholders facilitate creation of the required ecosystem for the EBIMS.

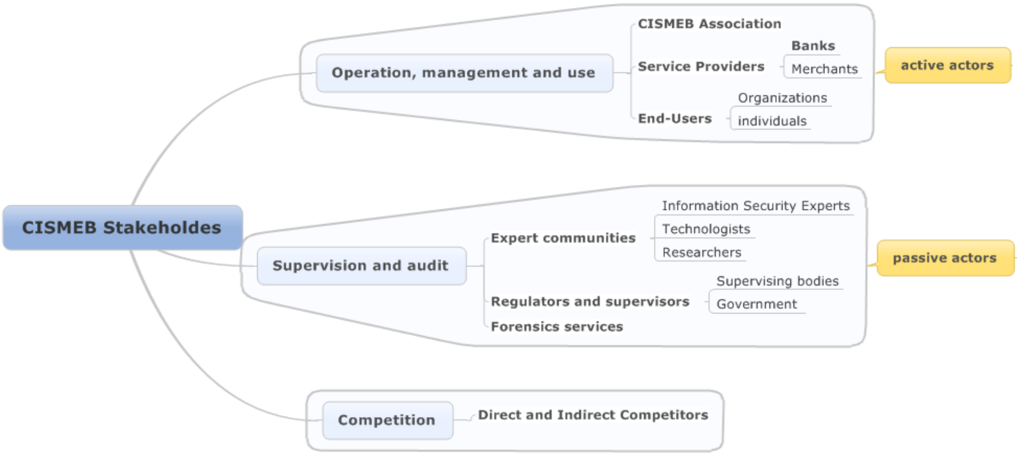


Figure 21: EBIMS: Stakeholders

EBIMS Association

EBIMS Association is a central body operating the EBIMS platform. It's a trusted neutral organization of a membership-type, where banks are members, owners and users of the system. Likewise credit cards associations, the banks have relation with the EBIMS rather than with each other. The organization is responsible only for activities and operations related to the management of the EBIMS platform and value-added services. All unrelated activities are performed by bank-members. In essence, the platform operator provides services to banks which in turn re-distribute the service to its customers, connecting them to the IdM platform.

[1] EBIMS stands for "Electronic Banking Identity Management System" and is used for simplicity, replacing "cross-border interoperable digital identity management system for electronic banking services"

Banks

Banks and other financial institutions providing e-banking services are interested in reliable, effective and secure access control and authentication of their users. Banks are the most active participants of proposed system, acting as identity providers and/or service providers as well. The banks are especially interested in easy integrability of the system in the e-banking service, as well as minimal operational costs related to management of infrastructure. They are responsible for the following processes:

- Initial registration and identification of customer in accordance with KYC policy and anti-money laundering regulations ;
- Identity provisioning to a customer;
- Relationship management with the users and customer support;
- Following policies, guidelines, standards and by-laws of the IdM.

Users

Users is a group of stakeholders which can be divided in two categories: private individuals and organizations. The whole group is primarily interested in using secure e-banking services with the capability to manage multiple accounts within a single ID and to initiate/terminate relationships with different banks across borders and electronically.

Merchants

Merchants is a special type of organizations decided to use value-added platform services in addition to account management functions. For example, the EBIMS can be used as a payment option to accept direct payments from buyer's to merchant's accounts, or a third-party service may decide to use the EBIMS and accept the IDs for customer's authentication, and so on. Merchants are connected to the system through a bank-member of the EBIMS Association.

Experts Communities

As shown in Chapter 3, the expert communities play a vital role in the development and evolution of IdM systems. There could be at least three different experts communities: the community of information security experts, technologists, and research community, who are interested in the capability to conduct independent evaluations, researches and examinations of the EBIMS infrastructure and services (e.g. security evaluations). Evaluations ultimately lead to improvements of the system and added value.

Regulators

Typically governments and supervising committees[2] act as regulators and supervisors of the market. Each of two actors has specific interests different from each other's, but they are both involved in general regulation of financial activities in cross-border environment, audit and supervision of related risk management, setting responsibilities and liabilities, as well as regulations of security measures and authentication methods in online banking. [115, 116]

[2] For example, the Electronic Banking Group of the Basel Committee on Banking Supervision of Bank for International Settlements

Forensics services

Banks are traditionally highly regulated institutions obliged to comply with number of anti-terrorist and money-laundering regulations, requiring traceability of transactions and accounts along with capability to identify account owners. The forensic services might be represented by police or any other law reinforcement agency.

Competitors

Competitors is the strong market force influencing the strategy of value offering and pricing. Competitors don't effect an IdM system directly, but have to be considered in the business modeling process as they are targeted at the same market and offering competitive products.

In particular, there are two strong competitors currently in the market, which operate operating across borders: IdenTrust and SWIFT (studied and described in the previous chapter). However, target markets intersect only in the segment of corporate users, while the EBIMS is targeted at private individuals as well. The Norwegian BankID solution is a competitive product inside of one country. For the segment where products intersect, there different strategies allowing platforms to be either incompatible between each other, fully interoperable, or integrated to a various extent[3].

5.1.2 Scenarios

The EBIMS should support the following basic scenarios:

- Identity provisioning and initial registration (Issuance of the ID to a new user);
- Establishing of new relationship between the bank and the ID holder;
- Termination of the relationship;
- Authentication and authorization for account management operations (e.g. opening, closing, placing orders, authorizing payment orders etc.);
- Revocation/recovery of compromised identity.

5.1.3 Value creation

The EBIMS creates main value from two distinct sources: the inherent value from the offering an secure access control service for a single user-bank relationship, and the network value from a platform. The latter is created by the platform bringing together four key customer segments: banks providing and accepting IDs, organizations holding and using the ID for electronic bank account management, users using the ID to access electronic banking services, merchants holding and using the ID as well as accepting user IDs to accept direct payments. The business model should be balanced and beneficial for these groups of customers.

The market is comprised of two principal sides: the users holding and using ID (organizations, and private individuals) and the service providers accepting the ID (e.g. banks selling e-banking services; merchants using the payment service option based on the EBIMS[4]) .

[3] However, a migration strategy to the new EBIMS platform and plan for its implementation are beyond the scope of this thesis and require a future work. Therefore compatibility with other systems is not considered in details.

[4] Depending on chosen strategy of value proposition, merchants could be considered as a third side, and the market - as a three-sided market. This is so when, for example, the payment service is considered separately from the IdM platform.

Due to the network effect the fast spread-out and acceptance of the ID will be triggered after number of customers using the IdM system achieved a critical mass. Additionally, the network effect can serve as a barrier for competitors to enter the market. However, the initial dissemination and adoption of the system depends heavily on offering and pricing balanced between two sides. Otherwise the "chicken-egg" problem occurs, when the lack of users on one side of the market prohibits adoption and acceptance of the service by another side - banks. This problem can be overcome by subsidizing one group of customers on one side of the market's sides through free or inexpensive value proposition. Usually the subsidized side is the more price-sensitive one. [111, 112, 113, 114]

In addition to typical for all IdM systems cross-side network effect, the EBIMS platform may be a subject of same-side network effect due to distinct environment conditioned by specific regulation of the financial sector, high level of standardization activities, and limited number of suppliers. The same-side network effect is created when increase of number of users on one side attracts more users of the same side. The effect is relevant for one side: the more banks and merchants use the platform, the more attractive it is for other banks and merchants to join; on the other hand, the increase of users will not have direct impact on the attractiveness of the platform for the same side of the market, since usage of e-banking services and payment transfer is possible without participating in the EBIMS.

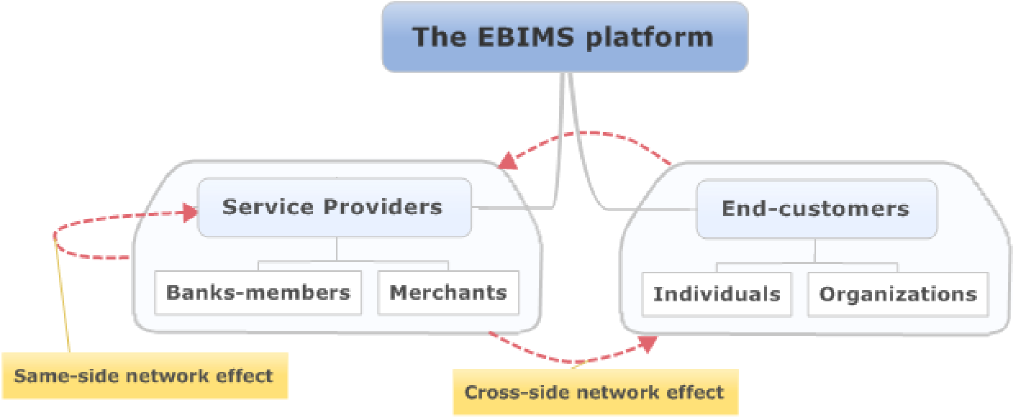


Figure 22: EBIMS: Two sides of the market

Besides the main economic value generated from the EBIMS platform and value-added services, parameters of the system add value as well. Privacy protection is one of them. The differences in cultural background between countries lead to different levels of concerns about privacy as well as different levels of trust in the authority operating an IdM system. These factors impact the acceptance, usage and dissemination rates of the system which ultimately impacts its value. Greater control over personal data and privacy protection measures can add additional trust in the system, and so facilitate its acceptance and growth of the platform. Besides, the research of supply-side perspective of IdM systems with enhanced privacy[117] proved this and showed that, ultimately, such systems have higher demand which compensates investments in privacy enhancing technologies (PET). The privacy enhancing adds value to the service, but users are not always willing to pay for this an additional charge. [118]

Privacy is often associated with anonymity. However, the highly regulated environments such as financial sector require to know their customers and anonymity in such system is not possible. Instead pseudonymity can be an option. It implies that only justified parties can link an identity to the real entity while for others the ID remains anonymous. This protects user's privacy and provides necessary traceability at the same time. Therefore, privacy protection can be provided by means of control over personal data flows, control over justified parties accessing data, and reducing risk of profiling.

The general structure of value network is depicted as a graph in figure 23. The graph presents the value network as a set of economic entities (nodes) connected through transfer of offerings (links). The purpose of the whole network is to deliver a common value proposition to customer segments of the market. [107]

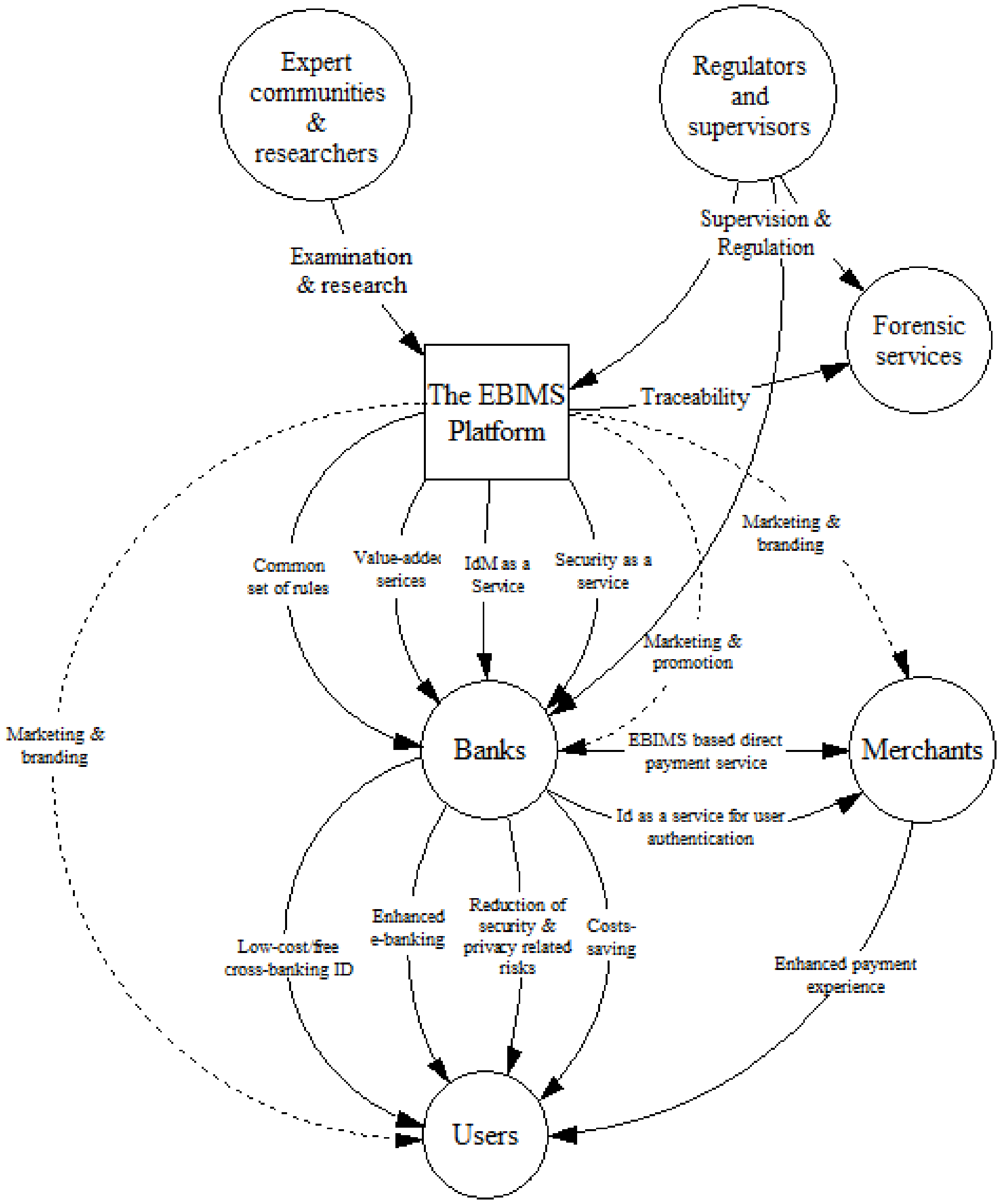


Figure 23: EBIMS: General structure of value creating network

5.1.4 The 9-component Business Model of EBIMS[5]

Customer segments

Key questions: Who is a customer? Whom is a company creating value for?

There are four key groups of target customers of the EBIMS platform[6]:

- Organizations and private individuals composing the "service consumers" category;
- Banks and merchants composing the "service providers " category.

Value Proposition

Key questions: What does a company offer and what problems does it solve? What is the value delivered to the customer?

The main value proposition offered to all customer segments is the cross-border interoperable identity management system EBIMS. The value proposition can be viewed as a set of elementary offerings composing a the service. The offerings to each customer segment are presented and described in the table below.

Offerings	Description	Segment
Cross-border Interoperable IdM platform	The platform is the primary value, enabling secure authentication and access control for cross-border electronic banking services as well as creating basic for new value-added platform services. E.g. providing Id-as-a-Service for third parties (merchants), or direct payment option.	All
Framework for cooperation	The platform is operated by the EBIMS association providing a cooperative framework for competitors in a form of common set of rules, policies guidelines and standards necessary to abide by all members of the associations.	Banks
Reduction of Security & privacy related risks	Simplifying identity management for individual users and increasing overall security level, protecting private and confidential information for all groups of users, selling additional insurance programs to banks in order to cover risks related to ID theft and fraud caused by the IdM system's potential vulnerabilities (except if the customer is responsible for occurred incident).	Organizations, Merchants, Private Individuals
Usability, flexibility & convenience	The single ID significantly increases convenience, ease of use and ease of implementation of the service. It allows to perform all account-management and account-opening operations electronically with low efforts and low costs. In addition, the use of single IdM platform leads to increased usability and consequently greater adoption and increased value of related services such as e-banking, for example.	All

[5] The design follows recognized business model design framework proposed by Alexander Osterwalder [15]. The names of components and basic elements are used in accordance with the proposed ontology.

[6] Depending on a pricing policy, whether price differentiation exists, the service consumers of each segment may be subdivided further to, for example, premium and standard customers provided with IDs of different privileges and limitations. For expositional simplicity the customers will be considered as four principal segments.

Free/low-cost ID	The IDs are offered for free to individual users and at low-cost price model for organizations and merchants	Organizations, Merchants, Individuals
Costs saving	Reduction of costs related to identity and account management procedures due to the single customer ID.	Organizations, Merchants, Banks
Expansion market	Banks and merchants can potentially offer services to a bigger total consumer market due to cross-border interoperability of the EBIMS.	Merchants, Banks
Value-added services	Provisioning of value-added services: trainings & education, risk and fraud management, consulting, certification, insurance program, etc.	Merchants, Banks, Organizations

Table 1: EBIMS business model: Value proposition as decomposed to elementary offerings

Distribution channels

Key questions: How can the value be effectively delivered to a customer?

The value is delivered to customers through the own standardized EBIMS platform and a set of rules necessary to abide by all members. The four distinct stages of channel, grouped by the stages of the customer's buying cycle, are as follows:

1. **Awareness**: At this stage, the company attracts customers by means of marketing and promotion of the platform directly and through the partners;

2. **Evaluation**: The EBIMS Association helps customer to evaluate the product by publishing information about the platform, results from independent researches and evaluations made by expert communities as well as audit results from supervision authorities;

3. **Purchase**: The EBIMS platform is offered to customers on two levels: 1st - tier customers (banks), and 2nd - tier customers (organizations, merchants, and private individuals). Hence, purchase stage is performed in two steps: the EBIMS association sells connection to the IdM platform to the banks by joining them to the association, then banks provides the customers with IDs and sells value-added services to merchant-partners by contracting.

4. **After sales**: The EBIMS Association provides support of its direct 1st-tier customers by means of such value-added services as consulting, trainings and educations. The banks, in turn, provides support of 2nd-tier customers through customer support service, trainings, etc.

Customer relationships

Key questions: Which relationships are required to be, or already established? How costly are they?

The platform operator manage customer relationships directly with banks-members of the EBIMS Association through communities and co-creation. Latter implies that banks have a right of participation in governance and development processes, balancing power and interests inside of the organization as well as maintaining the rule set of internal and external regulations, economic fees, dispute resolution procedures and so on.

In its turn, banks provide security as a service to 2^{nd}-tier customers and take responsibility for managing relationship with customers. Support is provided through personal or dedicated personal assistance, online self-service, policies, guidelines and best-practices.

Key capabilities/resources

Key questions: What key capabilities does a company require to offer the value?

The key resources are presented in the table 2.

Resource	Resource type	Description
IdM platform	Tangible	The EBIMS platform is the main asset & resource required to offer IdM and related services
Set of regulations	Tangible	The framework of regulations, standards, policies and guidelines is the resource which enable organizational & legal interoperability of the IdM platform as well as the cooperation required to deliver trusted and widely-adopted IdM platform.
Brand	Intangible	The role of brand is especially important for acceptance of such large-scale cross-border system. Outlined in previous chapter importance of alliances and associations for building trust in the IdM operating authority showed on example of VISA, that brand is the representation of the organization behind and the trust in it.
Partnerships	Intangible	Partnerships are traditionally important resource in value networks as co-creators of the economic value.

Table 2: EBIMS business model: Partnerships

Value configuration (key activities)

Key questions: What key activities does a company require to offer the value?

The organization is responsible solely for operations directly related to management and development of EBIMS platform. The key activities are presented in the table 3.

Activity	Activity level
Development, managing, and securing the EBIMS identity infrastructure	Primary activity
Balancing power and interests inside of the association	Primary activity
Development, maintenance and enforcement of common framework of policies, regulations, by-laws and standards	Primary activity
Provisioning of IdM service	Primary activity
Compliance and interoperability assurance	Support activity
Provisioning of value-added services	Support activity
Platform promotion & marketing, including contract management	Support activity

Table 3: EBIMS business model: Key activities

Partnerships (key partners)

Key questions: What are the key partners?

The value network defines the parties needed to be considered as partners. The parties, contributing to value creation either directly or not, are presented in table 4:

Partner	Strategic importance	Degree of competition	Degree of integration	Description
Banks	high	high	high	Banks-members are key partners, forming cooperative joint venture to provide the EBIMS platform and enable strategic partnership between traditional competitors (banks).
Merchants	medium	low	medium	The strategic cooperation of EBIMS Association with major merchants will boost adoption and dissemination of the platform. The cooperation can be enabled by agreements and contracts through banks acting as agents.
Expert communities	medium	none	low	Expert communities and researchers examine the platform and facilitate its improvement and development
Supervisors & regulators	medium	none	low	Regulators and supervisors influence the offerings through regulation and audit of compliance

Table 4: EBIMS business model: Partnerships

Cost Structure

Key questions: What are the main costs, most costly capabilities/activities?

Due to specific membership structure, EBIMS Association operates low-cost business model with cost-driven approach, outsourcing all unrelated activities to 1st-tier customers. The structure of costs inherent from key activities and recourses:

- Infrastructure maintenance;
- Advertising, marketing and promotion;
- Administrative costs;
- Consulting and researching fees;
- Compliance costs;
- Personnel.

Revenue model

Key questions: What are customers ready and willing to pay for? How do they pay/create revenue streams?

The revenue streams are summarized in the table 5.

Revenue stream	Stream type	Pricing method	Description
Connection fee	one-time revenue	Negotiation or fixed price	Connection fee (entrance fee) is paid once by a financial institution for connection to the EBIMS platform and joining EBIMS association
Annual membership fee	Recurring revenue	Subscription with price differentiation	The fee is paid by bank-members annually.
Annual service fee	Recurring revenue	Differential	The fee is paid by bank-members annually for required EBIMS services or amount of transactions.
Value-added services	Recurring revenue	Fixed list-price	The revenue is generated from selling value-added services: risk & fraud management services, consulting services, insurance program, education & training, etc.
ID provisioning and recovery fees	One-time revenue	Differential pricing	The fee is paid by an organization or a merchant to get an ID (initial registration stage). The basic IDs are issued for free for private users and with low-cost price for organizations. The price depends on type of entity (organizations and merchants may be further differentiated to offer different prices for large corporate and subsidized prices for small businesses) and type of the privileged ID (e.g. the ID may be limited on different levels for the amount of transaction, number of users linked to ID, additional services available (may be chosen later), amount of established relationships with different banks, etc.) Differentiation is based on assessment of related risk and market price. The recovery fee is paid by a user for stolen ID.
Non-compliance fees	One-time	Fixed list prices	The fee is paid for non-compliance.
Usage & transaction fee	Transaction	Pay-per-use or subscription	The fee depends on types of transaction, entity, and service/module used. Examples: 1. A percentage taken from direct payments of different volume (direct payment service provided to merchants) in a way of credit card interchange fees. 2. A subscription-based or transaction based fee paid by third party service provider (a merchant) to use the EBIMS ID to authenticate users at their online services. 3. A transaction based + subscription fee for interconnection of a proprietary authentication solution with the EBIMS platform. 4. General infrastructure usage fee paid annually based on the network usage statistics (amount of transactions and type). 5. The service API is opened to third party developers so that they can integrate their services with the EBIMS platform to use authentication services and will be charged per one API call/transaction.

Table 5: EBIMS business model: Revenue streams

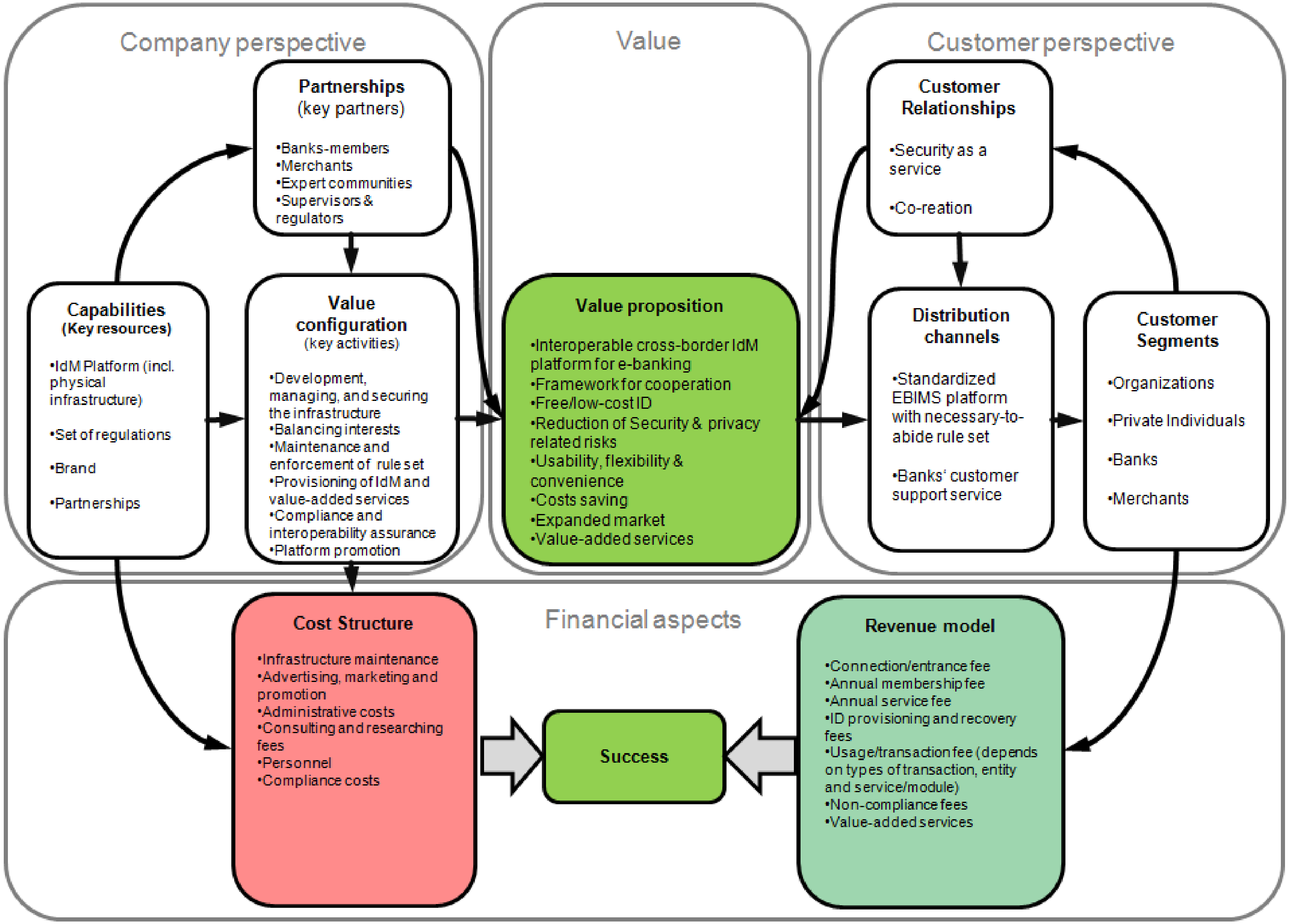

Company perspective
Partnerships
(key partners)
•Banks-members
•Merchants
•Expert communities
•Supervisors & regulators
Capabilities
(Key resources)
•IdM Platform (incl. physical infrastructure)
•Set of regulations
•Brand
•Partnerships
Value configuration
(key activities)
•Development, managing, and securing the infrastructure
•Balancing interests
•Maintenance and enforcement of rule set
•Provisioning of IdM and value-added services
•Compliance and interoperability assurance
•Platform promotion
Value
Value proposition
•Interoperable cross-border IdM platform for e-banking
•Framework for cooperation
•Free/low-cost ID
•Reduction of Security & privacy related risks
•Usability, flexibility & convenience
•Costs saving
•Expanded market
•Value-added services
Customer perspective
Customer Relationships
•Security as a service
•Co-reation
Distribution channels
•Standardized EBIMS platform with necessary-to-abide rule set
•Banks' customer support service
Customer Segments
•Organizations
•Private Individuals
•Banks
•Merchants
Financial aspects
Cost Structure
•Infrastructure maintenance
•Advertising, marketing and promotion
•Administrative costs
•Consulting and researching fees
•Personnel
•Compliance costs
Success
Revenue model
•Connection/entrance fee
•Annual membership fee
•Annual service fee
•ID provisioning and recovery fees
•Usage/transaction fee (depends on types of transaction, entity and service/module)
•Non-compliance fees
•Value-added services

Figure 24: EBIMS: Business Model Prototype

5.2 The Prototype of EBIMS Architecture

In this section the prototype of EBIMS solution is proposed and specified at the architectural level.

5.2.1 Architecture and technology models

From the technology point of view, the identity management system interconnecting different parties can be of three general types: centralized, federated, and user-centric. The centralized model implies one central authority which authenticates user to a single account and stores all user's data. The user and the accessed system are in the same security domain. This model puts a burden of security and identity management on the single identity provider, designating a single point of failure for the whole system. Federation models imply that data is stored by different identity providers and maybe shared between them. The federation model interconnects different security domains. The user-centric model puts user in the control over data flows and choosing an identity provider. This also shifts the liability to the user. [1]

In general, an architecture of a system can be either logically distributed or centralized[7]. Let's consider first the case of decentralized federation model.

Federated architecture allows to interconnect IdM systems of different parties. In a typical federation model, a relying party relies on the identity provider (IdP) to authenticate user, requesting authorization every time it's needed. At the same time a data object, access to which is controlled by RP, has to be linked to the identity issued by the IdP. In case of unrecoverable loss of that ID or termination of relationship between the IdP and the user, latter will lose access to the data object on RP side because the user cannot be authenticated with the same ID any longer.

Putting this scenario in the context of cross-border IdM for e-banking, the identity provider is a bank "A" and the relying party is a bank "B". Both provide e-banking services to their customers. If a customer opened an account in the bank "B" using the ID issued by the bank "A", the account is linked to this ID. In order to grant access to this account, the bank "B" has to request the bank "A" for authorization each time when user authenticates using the ID. However, if the relationship between the Bank "A" and the user is terminated[8], than the ID issued by Bank "A" cannot be longer used by the user to access accounts opened in other banks. If the user had relationships with more banks the problem was even more serious. Obviously differences in lifecycles of different members of federation can create significant obstacles and risks for reliability of the system. The figure 25 shows simplified authentication process in case of bank-to-bank decentralized federation model.

In addition, the heterogeneous nature of various implemented IdM systems, lack of operational and semantical interoperability, disbalance of power inside of the decentralized federation as well as establishing trust and legal compliance require bilateral agreements between banks to overcome these issues. However, such model is not scalable and cannot meet basic requirements.

[7] It's noteworthy that centralized architecture implies only centralization on the logical level through central point of management and governance of the system. On the physical, infrastructural level, such a system doesn't necessarily need to be centralized as well, in fact it's very often distributed in order to provide better robustness.

[8] For example, the bank can go bankrupt, be liquidated, or the customer can terminate relationship with bank due to losing trust. On the other hand, there could be a case when a bank may want to revoke access to the bank account and terminate bank-customer relationship due to the big customer's debt.

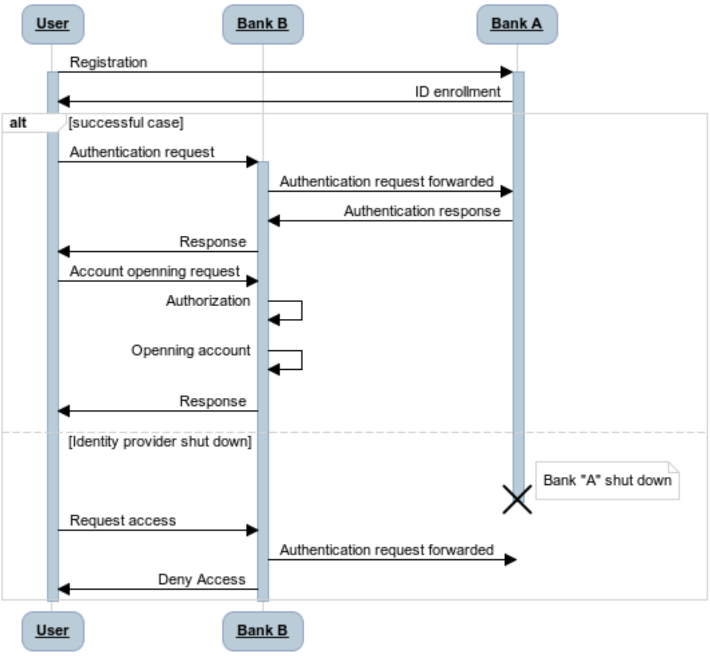


Figure 25: Problems of bank-to-bank decentralized federation model

Obviously, logically centralized architecture conform to basic requirements better than distributed one. The EBIMS association is chosen to act as central trusted identity provider in this system, while the registration of users and provisioning of IDs are delegated to the banks. The technology model is chosen as a combination of user-centric and federation models. In order to ease implementation and provide more flexible and agile solution, the system needs to be developed as a service-oriented architecture.

5.2.2 Architecture overview

The system consists of three principal domains:

- Interoperability domain with centralized infrastructure managed by the EBIMS Association;
- Service providers including banks and third-party service providers (merchants);
- User domain including private individuals and organizations.

The banks-members are connected to the EBIMS Platform through access point servers which provides access control and mediation between banking information system and the central platform. According to STORK, this model of interoperability is called identity-proxy.[8] The merchants (incl. third-parties using the EBIMS platform for authentication in their online services) are connected to the central platform through the bank acting as an agent and and re-distributor of security services offered by the EBIMS. The merchant uses the software plug-in "Merchant IdM Module" to connect to the bank providing IdM services of the EBIMS platform. This model of interoperability between the bank and the merchant is called middleware model, according to STORK.[8]

Each bank's information system interacts with the platform through the identity gateway unit which is the client to access point servers. Merchants' and banks' systems consist of front and back offices. The front office is a set of interfaces and end-customer services and presents service components directly accessible by and interacting with a user or the platform. The back office provides support functions of authentication, authorization, audit and includes a local registry storing required users' data associated with a specific identity which has been issued by EBIMS and registered to a certain user by the bank.

The EBIMS platform has four distinct layers (Fig. 26):

- **Access layer** provides connectivity, interoperability and controls access to the EBIMS;
- **Interface layer** provides access to platform services and its administration. Additionally, the layer gives access to API for external developers and technology suppliers, so that they can integrate their products to and reuse the platform services;
- **Service layer** represents platform services and decision points. It is the main layer consisting of five main services which execute following key functions:
  1. **Issuance service** is a service responsible for management of ID including issuance, registration, and recovery procedures;
  2. **Policy service** manages policies associated with a certain issued ID;
  3. **Validation service** enables the revocation of compromised identities;
  4. **Security token service** is the front-end service. It manages ID authentication and authorization procedures as well as provides identity transformation to assure semantical interoperability;
  5. **Security monitor service** provides monitoring, fraud detection capabilities and assures security of the platform.
- **Infrastructural layer** includes the platform infrastructure, core capabilities (e.g. key management, platform administration, etc.) along with registers, repositories, and stores for the platform services. The registers are divided in two categories: the central register with information about issued pseudonymous identities, and service registers used by the platform services for information storing and processing.

User always authenticates through a bank, including the authentication&authorization at third party services. For example, user request authentication at a merchant's service, which in turn requests the user interface authentication form from the bank. Next, user authenticates to a bank through this interface, then bank proves the authenticity of user's credentials to a merchant. The merchant is interconnected with the bank through the "Merchant IdM Module" plug-in.

The centralized type of architecture allows traceability and identifiability of the users identity, but the platform doesn't store any user's data or identity attributes containing personal information. A user can choose parties to interact with and data to disclose, so that only justifiable parties are in a possession of necessary user's information.

Even though the EBIMS is a distributed on the physical level and it doesn't store any private information which could be stolen or lost in case of security incident, a centralized architecture can potentially pose a risk of profiling by tracking the use of identity. This risk can be mitigated using PET technologies such as U-Prove [23, 25, 24] or Idemix [22, 119], allowing to protect user's privacy on cryptographic level.[9]

[9] Although, the choice of specific technology and development of detailed protocol for the EBIMS IdM solution are not the goal of current research, they need to be covered in future work.

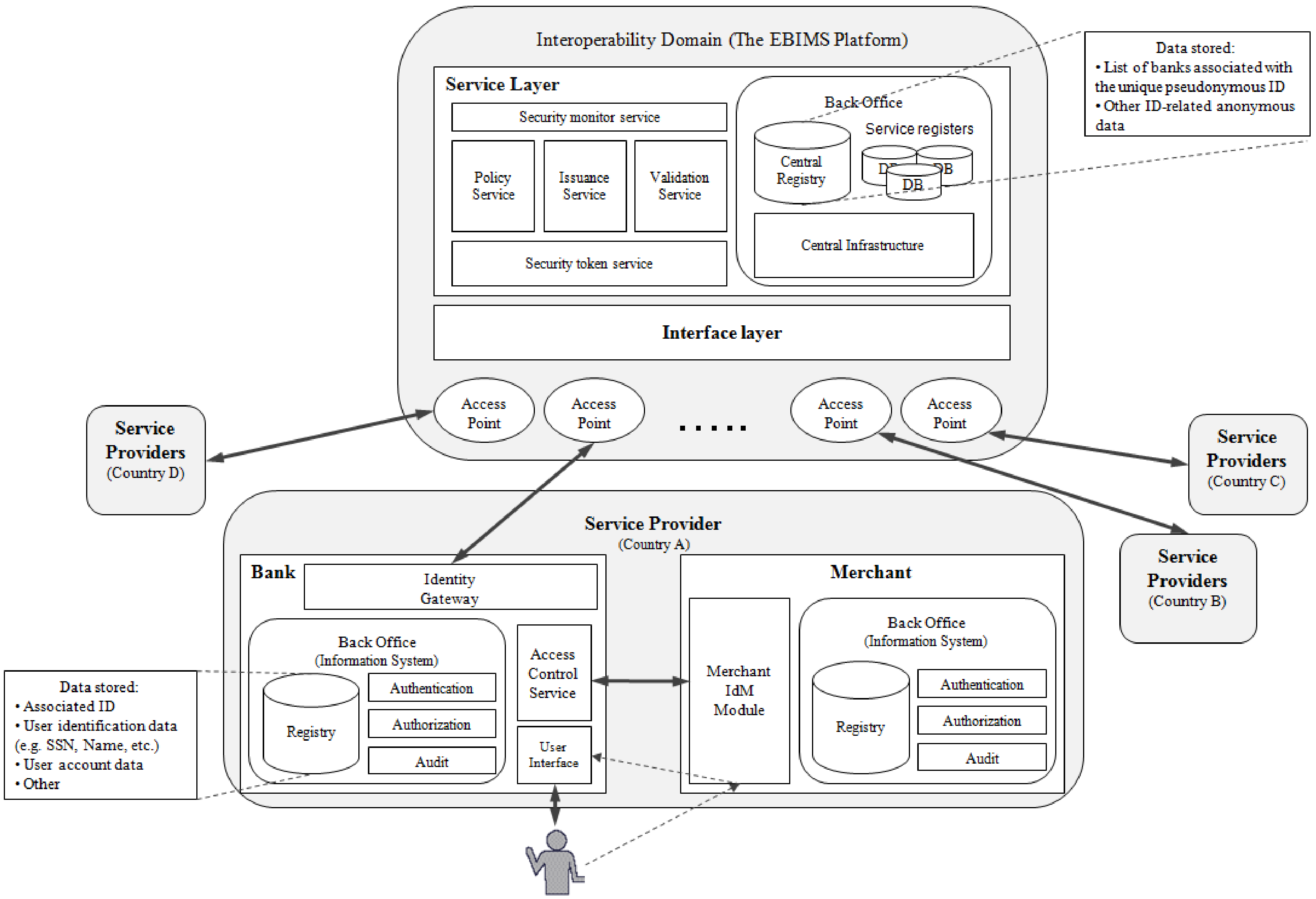


Figure 26: EBIMS: Architecture Prototype

5.2.3 Protocols of basic scenarios

In this section the process flows and general protocols of basic scenarios are described. The goal of the section is to describe the steps by which a process is performed rather than define detailed technical protocol of interaction.

Initial registration and enrollment

The processes are performed via the following steps:

- **Step 1:** A customer goes to a branch-office of a bank-member of EBIMS Association for initial registration. The customer provides necessary documents for identification and performs necessary actions in accordance with KYC policy;
- **Step 2:** The bank registers customer's information in the "back-office" database;
- **Step 3:** The bank requests[10] a pseudonymous ID from EBIMS;
- **Step 4:** EBIMS issues pseudonymous ID with unique identification number, associates it with the bank-registrar holding the personal information of this user, and sends the ID to the bank;
- **Step 5:** Bank associates the ID with the customer's data in the DB;
- **Step 6:** Bank provides the customer with the ID/credentials.

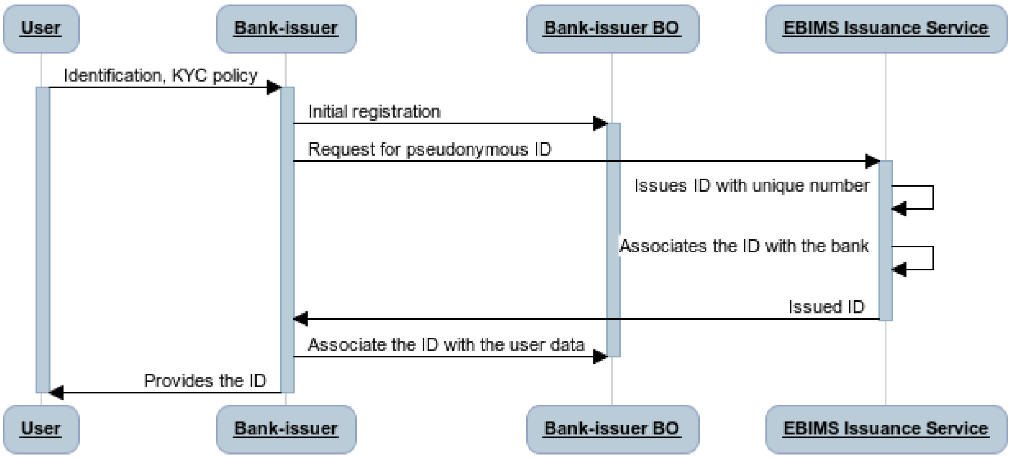

User
Bank-issuer
Bank-issuer BO
EBIMS Issuance Service
Identification, KYC policy
Initial registration
Request for pseudonymous ID
Issues ID with unique number
Associates the ID with the bank
Issued ID
Associate the ID with the user data
Provides the ID
User
Bank-issuer
Bank-issuer BO
EBIMS Issuance Service

Figure 27: EBIMS: Initial registration and enrollment processes

User authentication and authorization

Authentication and authorization are two paramount operations of any security system. Overwhelming majority of functions provided by e-banking services require to be authorized. In particular, the authentication and authorization are needed to cover variety of bank account management operations such as: account opening, closing, placing orders, sign orders, etc.

The following steps define authentication and authorization processes:

[10] Here and further in the text, all requests exchanged between different parties are signed by the requester.

- **Step 1:** User request authentication to a bank;
- **Step 2:** The bank forwards requests for authentication&validation of the ID to EBIMS validation service (following response is discrete: either approved or denied access);
- **Step 3:** If the ID is valid and successfully authenticated, the user requests authorization to access e-banking service or to perform account management operations;
- **Step 4:** Depending on type of the operation, the access is either granted by local authorization system or may require the authorization from the EBIMS platform;
- **Step 5:** The user receives either access or denial error message.

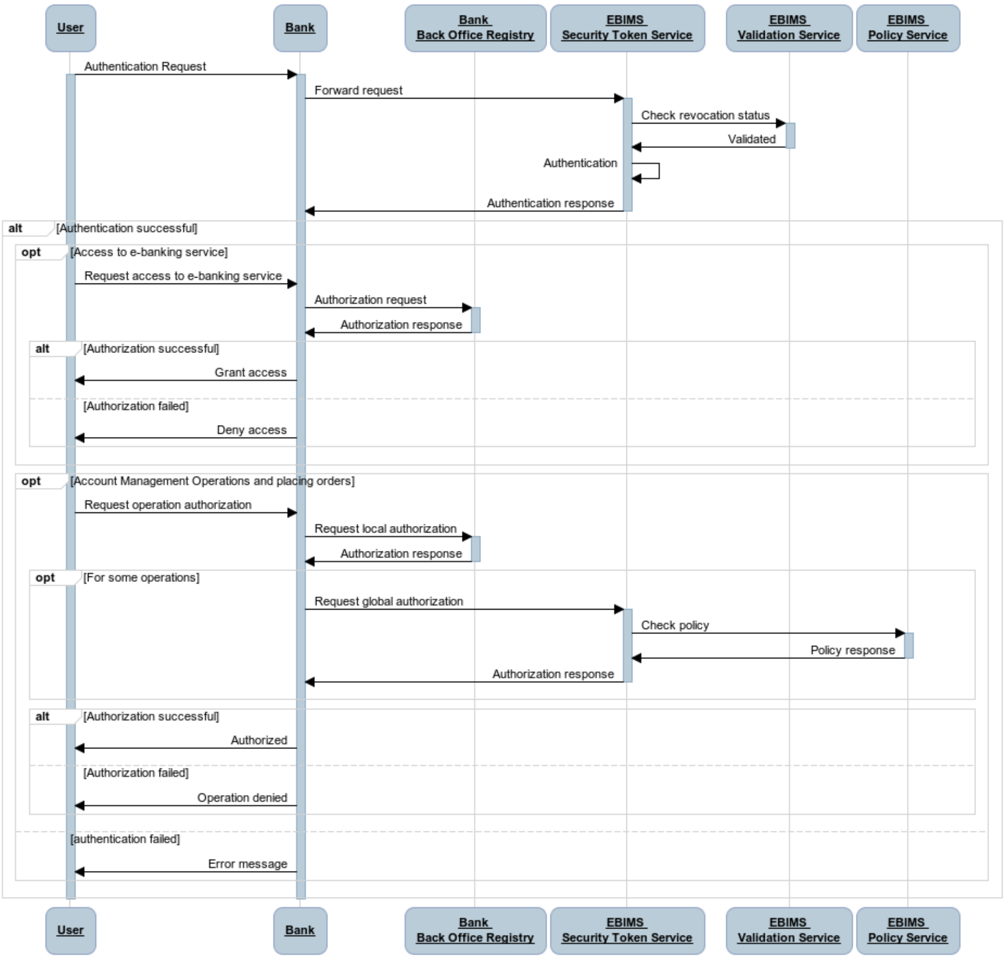


Figure 28: EBIMS: User authentication and authorization processes

Establish new relationships with another bank, using this ID

The steps are as follows:

- **Step 1:** The user requests registration to another bank's e-banking service using the ID;

- **Step 2:** The bank requires the user authentication,
- **Step 3:** The bank forwards user authentication request to EBIMS security token service (ESTS). The following response is discrete: either approval or denial;
- **Step 4:** If the user is not yet a customer, the bank starts registration process. The bank sends registration request to EBIMS Issuance service (EIS);
- **Step 5:** EBIMS Issuance service (EIS) requests the policy service(EIP) for the authorization. The policy service checks database against the policy associated with the ID (e.g. limit of number of associated banks, other restrictions or privileges) and responds with either approval and denial message to the EIS, which forwards it to the Bank-requester;
- **Step 6:** If the EIP approves the registration, the Relying Bank (the requester) initiate registration process. If the personal user data is stored in the identity attributes then go to step 11. Otherwise, the bank send request to the EBIMS for the user identification data.[11]
- **Step 7:** EBIMS checks for the record of banks associated with this ID and forwards the request to the first bank in the list[12];
- **Step 8:** The EBIMS sends request for the user data to the bank-issuer, which, in turn, checks its "back-office" DB, extracts necessary user information, sends it in response to the EBIMS in encrypted form;
- **Step 9:** EBIMS forwards response to the relying bank;
- **Step 10:** The relying bank receives user information, and decrypt it;
- **Step 11:** The bank sends registration request to the "back-office" system;
- **Step 12:** The request is checked for authorization by the local policy server, and if the registration is authorized the request is hold for manual approval by an approval officer[13];
- **Step 13:** The approval officer of relying bank reviews and then either approves of rejects the user's request;
- **Step 14:** If the request is approved then the bank registers the user's information in the "back-office" DB and associates the ID with the customer;
- **Step 15** The bank responds to the user with either confirmation or rejection message.

Full process flow is depicted in figures 29 and 30.

[11] The choice of whether to store user private identification data separately or in the ID attributes depens on chosen technology. The technology must be chosen in a way that private identification data is cryptographically protected and not available without access control.

[12] Very likely it is the bank where user received the ID during the initial registration procedure.

[13] An approval process may take place in few steps depending on the type of user. For example, organization may require more checks by bank before the registration is allowed. In this case, the approval process will require few signatures by different bank officers.

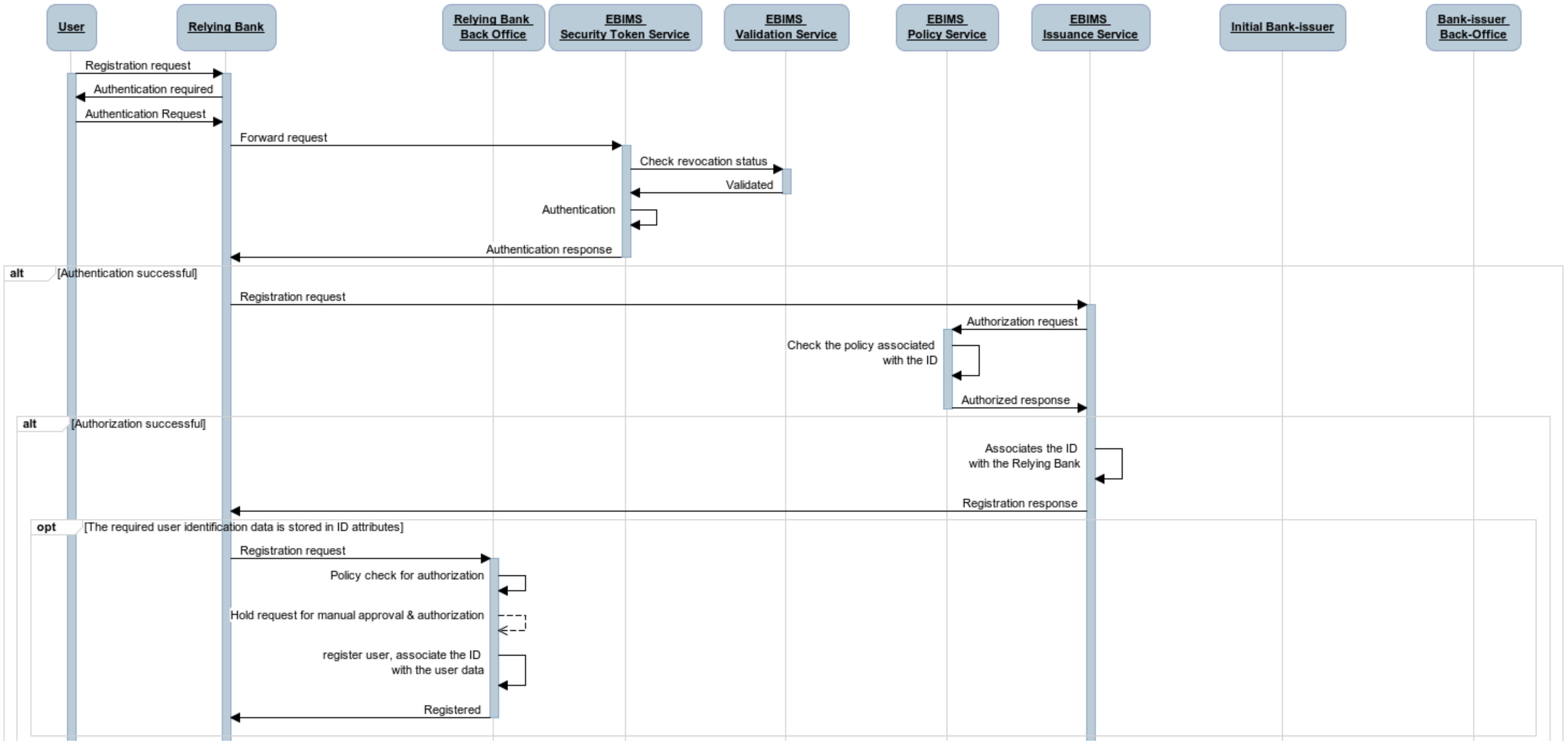


Figure 29: EBIMS: Establish new relationships with another bank. Part 1

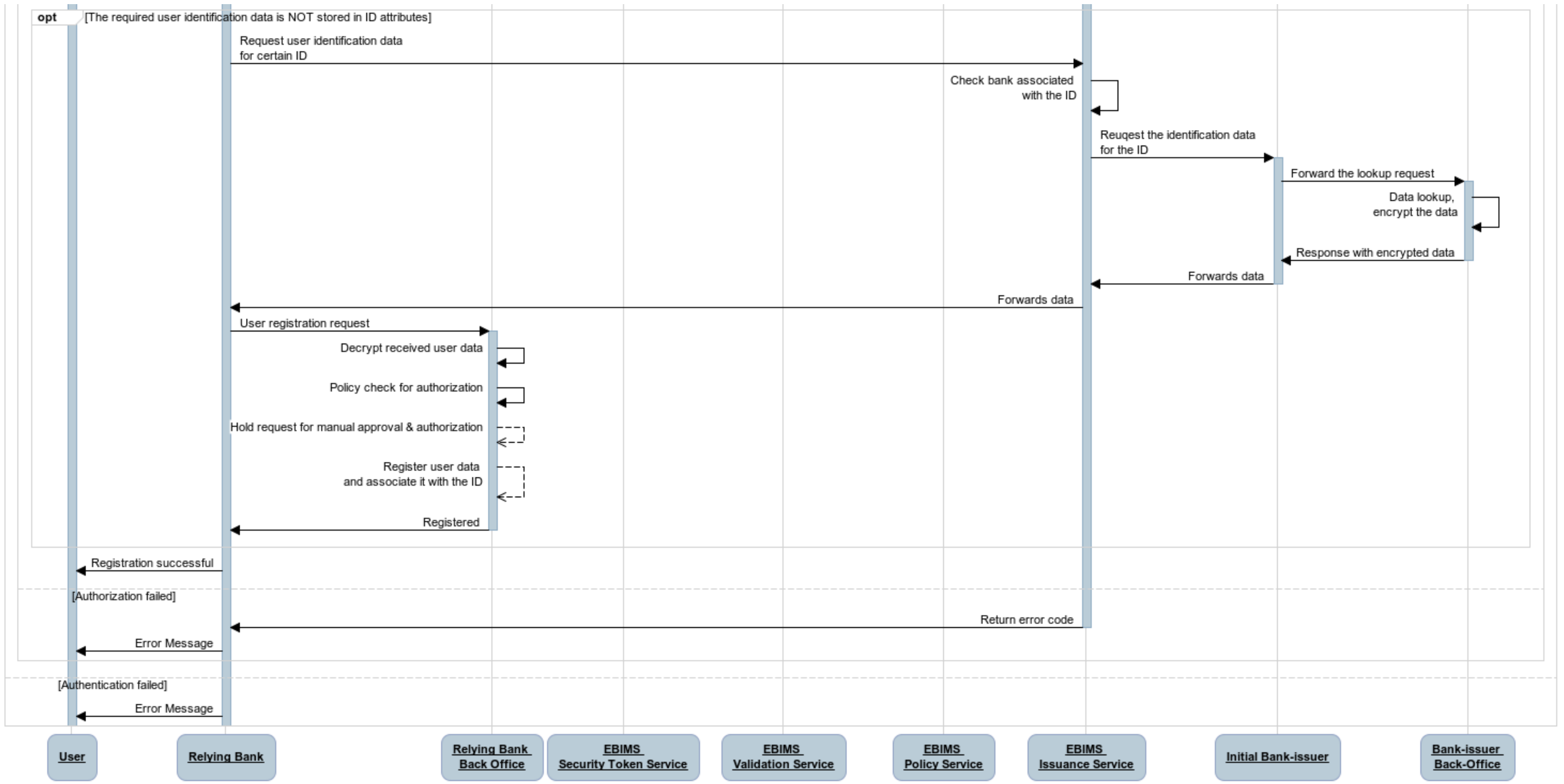

opt
[The required user identification data is NOT stored in ID attributes]
Request user identification data for certain ID
Check bank associated with the ID
Reuqest the identification data for the ID
Forward the lookup request
Data lookup, encrypt the data
Response with encrypted data
Forwards data
Forwards data
User registration request
Decrypt received user data
Policy check for authorization
Hold request for manual approval & authorization
Register user data and associate it with the ID
Registered
Registration successful
[Authorization failed]
Return error code
Error Message
[Authentication failed]
Error Message
User
Relying Bank
Relying Bank Back Office
EBIMS Security Token Service
EBIMS Validation Service
EBIMS Policy Service
EBIMS Issuance Service
Initial Bank-issuer
Bank-issuer Back-Office

Figure 30: EBIMS: Establish new relationships with another bank. Part 2

Revocation

The revocation process is performed as follows:

- **Step 1:** The user either visits or personally contacts one of the bank with already pre-established relationship and request revocation of the compromised ID;
- **Step 2:** The bank identifies user following KYC policy or any other established way;
- **Step 3:** The bank requests the EBIMS validation service for ID revocation;
- **Step 4:** The EBIMS revokes the ID, re-issues pseudonymous ID with the same unique identification number, and sends it ID to the bank;
- **Step 5:** Bank provides the customer with the new ID/credentials.

Since the number can be preserved during revocation procedure, the already established associations with other banks remain untouched.

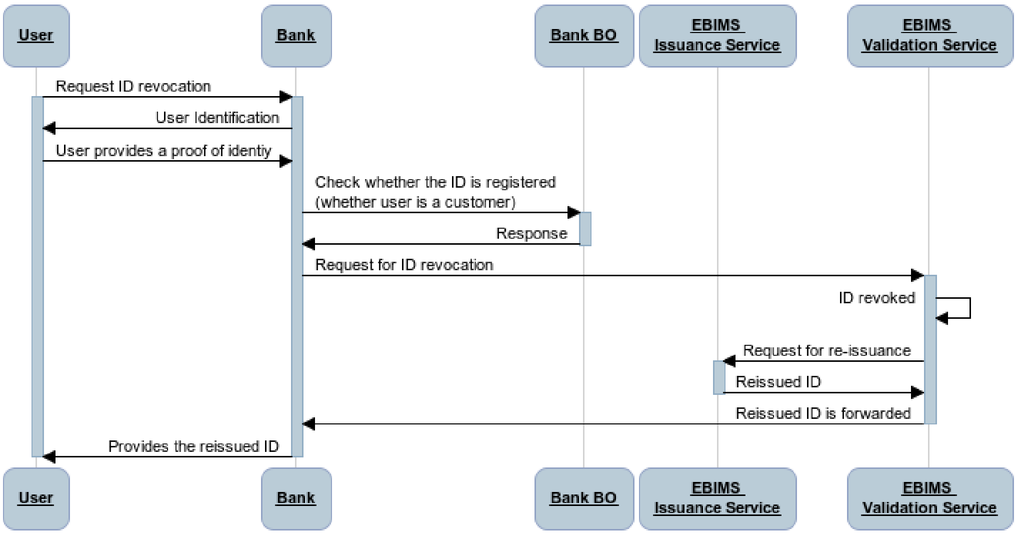


Figure 31: EBIMS: Revocation

Termination of relationship

The termination of relationship ("de-registration") may be caused by different reasons. For example, the bank can go bankrupt, be liquidated, or the customer can terminate relationship with bank due to losing trust. On the other hand, there could be a case when a bank may want to revoke access to the bank account and terminate bank-customer relationship due to the big customer’s debt. The termination process can be initiated after organizational and administration issues are resolved and all user accounts are closed at the moment. The process will follow these steps:

- **Step 1:** The user sends signed termination request to the bank;
- **Step 2:** The bank requires user authentication;
- **Step 3:** If the authentication is successful, the termination request is forwarded to the Back-office system and held for approval;

- **Step 4:** If the request is approved, it's forwarded to the EBIMS Issuance service;
- **Step 5:** The EBIMS deletes the association between the ID and the bank from the database and responds with the confirmation message;
- **Step 6:** User receives a confirmation or an error message.

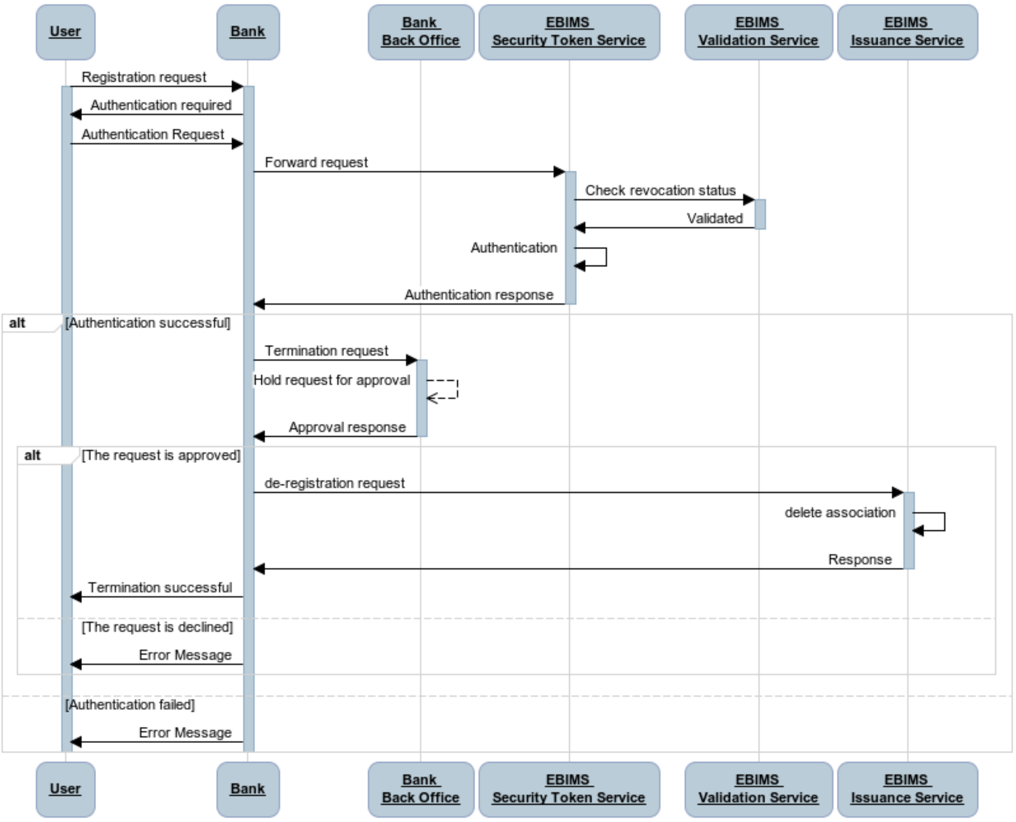


Figure 32: EBIMS: Termination of relationship

6 Conclusions

This master's thesis aimed to study the topic of interoperable identity management system for electronic banking which could successfully be adopted and used by multiple parties across borders. The goal was not just to present yet another technical solution, but to research also what could make an IdM system potentially successful and accepted by multiple parties.

To achieve the goal, the thesis approached the topic from different perspectives and researched various aspects of identity management systems, taking into account both external and internal factors. This required of us to embed two qualitative multifaceted multiple-case studies considering identity management on different levels.

6.1 The summary of results

First, we analyzed current identity management solutions in Europe investigating the different experiences in identity management system on example of national-level IdM solutions; national ID numbers have been traced back to the roots to define the principles influencing adoption and evolution of IdM systems throughout the history of its development. The key case in this multiple-case study was the Norwegian experience and in particular the BankID solution, which then was analyzed in international context. The goal of this research was to explore the environment for future system and identify influencing factors stemming from differences in legal, cultural and historical backgrounds. In this study we found that:

- The use of IdM systems in "a must" applications is a strong motivator to its successful adoption. This "a must" applications may be of either enforced-to-use or ubiquitous nature. In this sense, banks are powerful influencers needed to be involved in development and exploitation of a national and, furthermore, a cross-border IdM system to assure its successful adoption;

- Cultural aspects and public trust in IdM operating organization impact on success of the system considerably;

- Security and privacy requirements result from a cultural background. Thus, privacy and profiling risks are considered to a variable extent depending on cultural and historical background. The direct use of national identification numbers enables easy and low-cost profiling and creates privacy-related issues, leading to legal compliance risks. Prior modification or encryption of the SSN could be used instead;

- Interoperability, ease of implementation and ease of use of an IdM system are crucial factors for success of the IdMS;

- Independent evaluations by expert communities play vital role in IdM system refinement process. Therefore openness of specifications and public availability of basic system documentation is almost as important for IdM system as it is for crypto-systems. Otherwise the development and evolution of the system can be obstructed, and ultimately problem of the "Lemon market"[1] may occur.;

- A legal framework is a backbone of an IdM system which should be considered carefully throughout the IdM lifecycle. It may become serious obstacle for IdM system in one case or a strong driving factor in another;
- An IdM system is a sequentially evolving matter. Sequential improvements and upgrades of existing IdM system are more likely than acceptance of suddenly emerged solution, developed without taking legacy systems into consideration.

Second multiple-case study was targeted to definition of possible enablers and disablers of the successful system operation in the diverse environment. The requirements and features of current cross-border inter-bank systems, such as VISA, SWIFT, and IdenTrust, have been studied. The goal of this multiple-case study was to identify success factors as well as architectural, business and organizational models of different systems. The research showed that:

- Business model makes difference. Although the acceptance, speed and breadth of dissemination of an IdM system depend on a variety of factors and system features, the business model is the element which bridges all of those, adjust to user's interests and ultimately create value. The business model is an essential part which is aimed to leverage interests in a complex set of dependencies and interrelation between different parties.
- IdM system creates value through a value network, rather than a typical value chain. An IdM system creates value via mediation between relying parties (e.g. service providers), entities (e.g. ID holders), and complementary market-players contributing value creation.
- An identity management service is a two-sided market[2]. In typical IdM system there are three corners: a service provider, an identity provider and an entity. The identity provider - operator of IdM platform - has to leverage interests between ID-holders on one side and service provider on the other side in order to assure the adoption and acceptance of IdM system.
- As a consequence of previous two features, an identity management system is a subject of cross-side and often same-side network effects.
- Membership structure (associations) of organization is a very promising way to provide legal and organizational interoperability and balance interests of participants via cooperative framework for competitors.
- Neutral trusted third party organizations, such as associations, allow to build trust into IdM system easier for both competitive identity and service providers and users. The trust in IdM system is represented by a single sign/mark.

[1] The "Lemon market" is a situation characterized by asymmetry of information, when the seller knows more about a product than the buyer. In our case the seller is the identity provider (IdMS operator), and the buyer is identity-holder (the user of the system). The asymmetric information ultimately lead to the problem of quality uncertainty. George Akerlof, whom discovered and described the Lemon Market effect, was awarded the Nobel Memorial Prize in Economics. [120]

[2] Depending on strategy and value configuration the market may be considered as three- and multi-sided.

Overall, success and so effectiveness of an IdM system depend on much more than just a strong security. An IdMS is a complex sociotechnical system composed of both “social” and “technical” elements and implying constant interaction between a human and technical security system. The IdM operator needs to adjust system to requirements of various group of user to provide them with desired system functionality; improve usability and security of the solution. The success factors depicted as the structural map in the Figure 33. The 1st layer represents six groups of factors consisting of various requirements and system features. The arrows show additional interdependencies.

6.2 The prototypes of business model and architecture

Ultimately, results of the research were used to design prototypes of business model and architecture for cross-border identity management system for electronic banking. The business model is designed and described from four perspectives: analysis and description of value creation and proposition, customer and company perspectives, as well as costs and revenue models. In addition, the analysis of market forces and identification of stakeholders of suggested system was performed to describe the business model environment. In support to business model, we also proposed the design of architecture for the considered IdM system following SOA principles to improve integrability, flexibility and effectiveness of the system. This design defines the structure of the solution along with service components on architectural level, besides the process flows and general protocols of basic scenarios were described to explain essential business processes. It’s likely that designed system will be successful as it’s based on the identified factors from multifaceted research, however it requires complete risk analysis before investments.

The state and perspectives of Norwegian BankID solution

High levels of acceptance & dissemination of Norwegian identity management systems, especially the BankID solution, bear a lot of potential for both national level and cross-border IdM systems. A number of innovative functions and applications pave the way for new opportunities in electronic business processes. The success of BankID is built on government support provided through sound legal framework, specific cultural trust-related background, and effective organizational structure of the solution enabled by the strong interbank cooperation. Close cooperation between banking institutions within the Norwegian Financial Services Association and the Norwegian Saving Banks Association allows the BankID solution to dominate the market. In turn, technological and security features obviously were not handled with absolute care and top priority during the system design. The further evolution of the BankID and steps towards its implementation in a cross-border environment are hardly possible without addressing all open security & privacy issues. Integrability of the BankID also calls for improvements. The solution must provide federation and integration in order to assure flexibility of the infrastructure and to ease its implementation. Switching to the claim-based identity model and adding access control to user’s data in certificates could be options. These options help to enhance privacy protection and security level adhering to minimal disclosure principle, and enable better federability and integrability of the entire system.

Overall, the BankID solution could serve as a basis for proposed IdM platform. The principal similarities in organizational structure, architecture and business model don’t require drastic changes for adoption of suggested design or its core components.

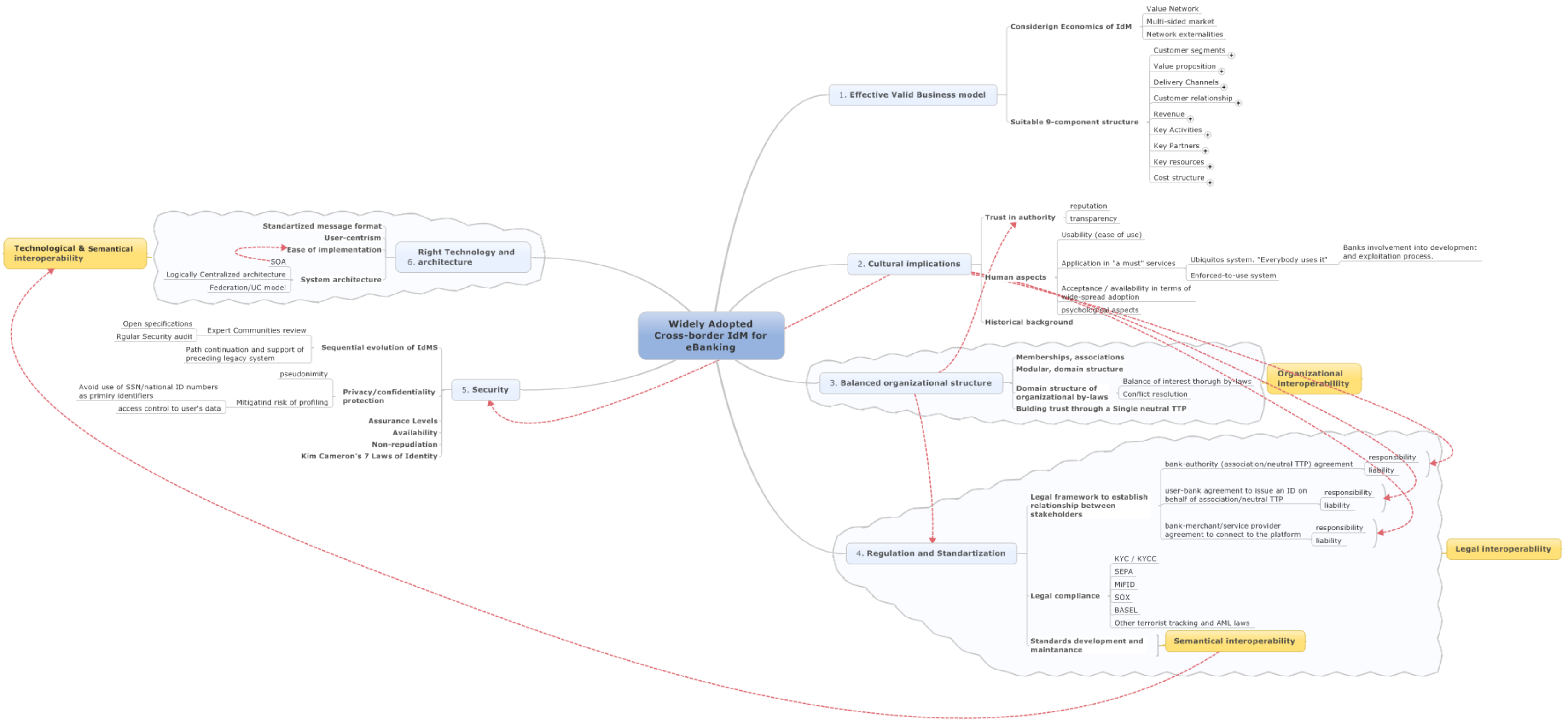

Widely Adopted Cross-border IdM for eBanking
1. Effective Valid Business model
Considerign Economics of IdM
Value Network
Multi-sided market
Network externalities
Suitable 9-component structure
Customer segments
Value proposition
Delivery Channels
Customer relationship
Revenue
Key Activities
Key Partners
Key resources
Cost structure
2. Cultural implications
Trust in authority
reputation
transparency
Human aspects
Usability (ease of use)
Application in "a must" services
Ubiquitos system. "Everybody uses it"
Banks involvement into development and exploitation process.
Enforced-to-use system
Acceptance / availability in terms of wide-spread adoption
psychological aspects
Historical background
3. Balanced organizational structure
Memberships, associations
Modular, domain structure
Domain structure of organizational by-laws
Balance of interest thorugh by-laws
Conflict resolution
Bulding trust through a Single neutral TTP
Organizational interoperabiliity
4. Regulation and Standartization
Legal framework to establish relationship between stakeholders
bank-authority (association/neutral TTP) agreement
responsibility
liability
user-bank agreement to issue an ID on behalf of association/neutral TTP
responsibility
liability
bank-merchant/service provider agreement to connect to the platform
responsibility
liability
Legal compliance
KYC / KYCC
SEPA
MiFID
SOX
BASEL
Other terrorist tracking and AML laws
Standards development and maintanance
Semantical interoperability
Legal interoperablity
5. Security
Sequential evolution of IdMS
Expert Communities review
Open specifications
Rgular Security audit
Path continuation and support of preceding legacy system
Privacy/confidentiality protection
pseudonimity
Mitigatind risk of profiling
Avoid use of SSN/national ID numbers as primiry identifiers
access control to user's data
Assurance Levels
Availability
Non-repudiation
Kim Cameron's 7 Laws of Identity
6. Right Technology and architecture
Standartized message format
User-centrism
Ease of implementation
SOA
System architecture
Logically Centralized architecture
Federation/UC model
Technological & Semantical interoperability

Figure 33: The structural map of influencing factors

7 Future work: Towards interoperable cross-border digital ID in e-Banking

Despite the amount of analysis and design work done, there are still research challenges to be addressed and future work to be done in a way to interoperable cross-border digital identity for electronic banking. This master's thesis project is a first step in this direction. Future research in areas of IdM dynamics, economics and business modeling can contribute better understanding of the nature of digital identity and its key features, as well as facilitate development of the IdM solution for e-banking proposed in this project. The roadmap for future research work is depicted in the figure 34 and presents three roads: research of economics, research of dynamics and features of IdM systems, and risk analysis. Finally, this three roads lead to development of implementation and migration strategies as well as detailed infrastructure and protocol.

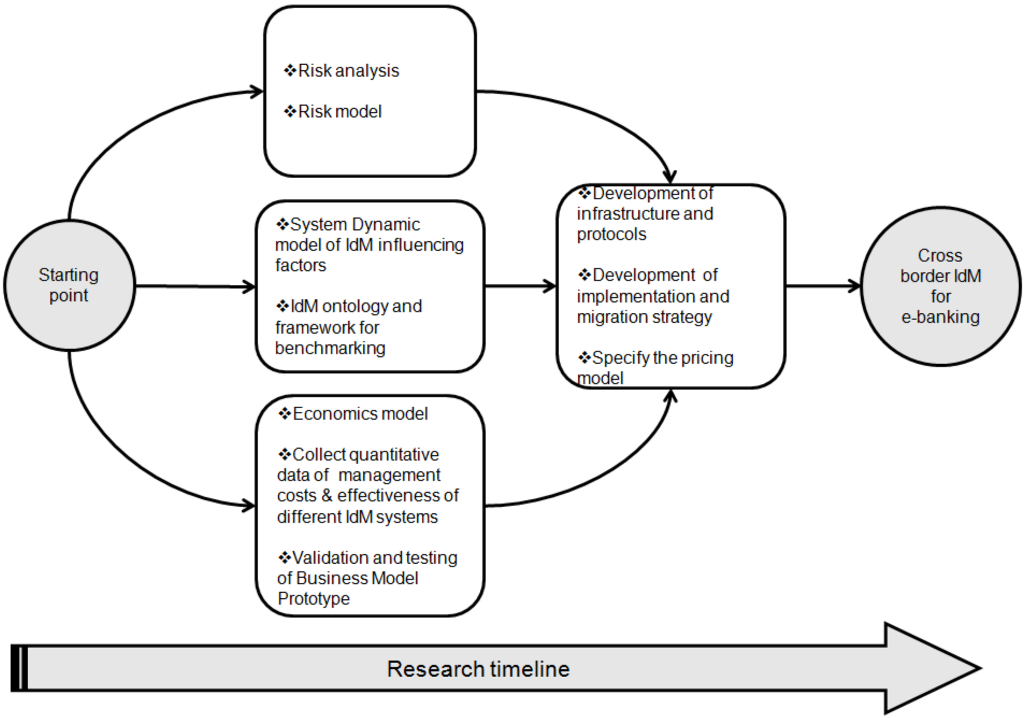

Starting point
❖Risk analysis
❖Risk model
❖System Dynamic model of IdM influencing factors
❖IdM ontology and framework for benchmarking
❖Economics model
❖Collect quantitative data of management costs & effectiveness of different IdM systems
❖Validation and testing of Business Model Prototype
❖Development of infrastructure and protocols
❖Development of implementation and migration strategy
❖Specify the pricing model
Cross border IdM for e-banking
Research timeline

Figure 34: Future work roadmap

7.1 Risk Analysis

Perhaps the risk analysis is the most important research which should be conducted before the implementation of the proposed IdM system or any other large-scale IdM system. Single ID may be too risky to use, since it's the only key needed to many doors. The large-scale system being widely adopted and multi-party accepted will quickly become "too-big-to-fail" system. What are the risks associated with single ID for multiple banks? What is the risk model? The same questions should be asked to any large-scale IdM system and especially a cross-border one.

7.2 Dynamics of IdM: Generic System Dynamics Model of IdM

In this project we identified the parameters, factors, and requirements influencing the adoption of IdM systems and asigned them with priority. The system dynamic model and research of strength of these factors will contribute to better understanding of nature of an identity and identity management systems.

7.3 Economics and Generic Economic Model of IdM

The economics of information security has been addressed in number of studies and the importance of economic incentives is recognized among th society, but economics of IdM systems remain to be quite poorly studied despite the great significance of this area and its important role in information security.

In this project there have been identified basic economic features and value creation of IdM systems. Further research of these features in more details will give a lot of benefits. Thus, the research and development of justified mathematical and economical models are needed. Among other method, application of the game theory to the analysis may be useful. The goals of project are as follows:

- Impact and interdependency analyses between IdM processes, requirements and parameters;
- Economic analysis of IdM and related processes;
- Development and validation of mathematical and economical models for IdM.

It's likewise important to research and collect quantitative data related to costs of management & effectiveness of different IdM technologies, model, etc. This will allow to predict and calculate effectiveness of applied a technology or model and to construct a valid simulation model. Furthermore, this kind of data will help to specify the pricing model better and so to highlight competitive advantages of proposed business model.

7.4 Validation and testing of the business model prototype

When the economic model is design, the next step to continue the move towards cross-border IdM in e-banking is testing and validation of proposed business model prototype. The work on this stage has to be completed in collaboration to stakeholders and should include both research qualitative and quantitative methods. Additionally, a complex economic analysis of the business model is required to be performed (e.g. SWOT analysis, other methods).

Detailed competitors analysis is to be conducted in order to identify "winners" and "losers" after the implementation of the business model and to adjust the strategy.

7.5 IdM Ontology and Benchmarking Framework

One of the research questions identified during this project and left for future work is choosing right technology for the proposed EBIMS system and protocols to use. In order to do it, an analysis and examination of currently existing IdM models and technologies is needed. Development of a single benchmarking framework would contribute not only to this specific IdM system to be developed, but to general researches in the field of identity management.

The more and more models and architectures of IdM systems become available and there's a growing need in examination of these systems in terms of security, privacy protection, manageability, flexibility, etc. Various reference architectures, IdM technologies, and models require to be studied in order to develop a set of metrics and a multi-level benchmarking framework for IdM systems. The lack of sound benchmarking framework turns a market of IdM solutions into a "Lemon Market", when there's no established way to ensure quality and security of an IdM system. This leads to the need in a single benchmarking framework for IdM systems developed from scientific point of view.

There are following goals of this research:

- Classyfing of current IdM technologies (e.g. CardSpace, Higgins, Shibboleth, SAMLv2, Liberty Alliance, OpenID, OAuth, etc.) and models (federated, centralised, user-centered, etc.);
- Identifying, classyfing and justifying of a set of requirement & parameters on three levels: environment, system and system components & technologies;
- Evaluation of current IdM technologies;
- Developing a benchmarking framework for evaluation and ontology of identity management.

7.6 Migration and implementation strategy

The aforementioned research blocks pave the way to the final step comprised of two main parts:

- Development of implementation and migration strategies taking into currently implemented legacy systems;
- Design of protocols, physical infrastructure and specifying architecture on component and operational levels.

As a part of the research, topology and network structure should be covered. Real life topology is not a tree/ring/whatever simple hierarchy! However, currently most widely employed technology for IdM is PKI which is hierarchy-based by design. Other technologies also often consider hierarchical model of trust. What topology and network structure is better in what case? The Internet is the robust and fast developing network which became ubiquitous. From the Graph theory point of view, it's a free-scale network. Graph theory distinguishes two general models of random graphs: Erdős–Rényi model and Albert-Barabasi model. Both have pros and cons. What else can we gain from application of graph theory to Identity infrastructure design?

A Features of IdM technology models

	Siloed	Centralised	Federated	User-Centric
Method of Authentication	The user authenticates to each account when he wishes to use it.	The user authenticates to one main account.	The user authenticates to an identity provider, with this one authentication serving for the federation.	The user authenticates to identity providers, and service providers have to rely on that authentication.
Location of Identity Information	Identity information is stored in separate service provider accounts.	Identity information is stored in the one main account, a super account.	Service providers in the federation keep separate accounts in different locations. They may have agreements for sharing information.	Identity information is stored by identity providers chosen by the user. The user can help prevent the build-up of profiles that others hold about him.
Method of linking accounts/ learning if they belong to the same person	There is no linking between accounts and no information flow between them	Linking between accounts is not applicable. (A user's full profile resides in that single place.)	The identity provider can indicate what identifiers for accounts with federation members correspond to the same person	Uses of cryptography can prevent linkages between a user's different digital identities, leaving the user in control.
Trust Characteristics (who is dependent on whom, for what)	The user is reliant on the service provider to protect their information, even if limited. The absence of information sharing has privacy advantages.	The user is reliant on the service provider to maintain the privacy and security of all of his or her data.	Users have rights from contracts, but they may be unfamiliar with options. The federation has leverage as it is in possession of the user's information.	Users can keep accounts separate and still allow information to flow, but bear greater responsibility.

Vulnerabilities	Siloed systems offer the advantage of having limited data on hand, thus creating less of an incentive for attack. They also have a better defined and stronger security boundary to keep attackers out and limit exposure from failures	The central party controls the person's entire profile; other entities have little to check that profile against, and an insider could impersonate the person or alter data. Currently there is no way to safeguard data after it has been shared	Users have little input into the business-partner agreements. Some service providers will set up federation systems to exploit users. Currently there is no way to safeguard data after it has been shared	Concentration in the market for identity providers could leave them with much power. Currently there is no way to safeguard data after it has been shared.
Convenience	Siloed accounts are inconvenient for users and service providers due to multiple authentications, redundant entry of information, and lack of data flow.	This arrangement is easy for the user since he or she only has to deal with one credential to call up the account and since he or she has to authenticate just once.	Other members of the federation avoid the burden of credential management. Organisations that provide services to a user can coordinate service delivery.	Users may be ill-equipped to manage their own data (also a vulnerability) and may need training and awareness-raising

Table 6: Features of IdM technology models (Source: [1])

B BankID Certification Profile

Fields	Norsk betegnelse	Field type	Value/comments
Version	Versjon	Standard, Mandatory	Indicates that the x509 v.3 format is used
Certificate Serial Number	Sertifikatets Serienummer	Standard, Mandatory	Serial number from the issuer
Signature Algorithm	Signatur-algoritme	Standard, Mandatory	sha1RSA
Issuer	Utsteder	Standard, Mandatory	Name of issuer of BankID
Validity	Gyldig fra	Standard, Mandatory	Date
Validity	Gyldig til	Standard, Mandatory	Date
Subject	Sertifikatholder (emne)	Standard, Mandatory	Name of subscriber
SubjectPublic KeyInfo	Offentlig nøkkel (fellesnøkkel)	Standard, Mandatory	Binary coding of subscribers public key, with parameteres
Certificate Policies	Sertifikatpolicy (sertifikatkriterier)	Standard extention, Mandatory	OID for the certification policy under which the certificate is issued
Bank Name	Bank navn	Private extention, Mandatory	Name of the bank that has entered into the BankID agreement with the subscriber.
Bank Reg Number	Bank register nummer	Private extention, Mandatory	Four digit number that identifies the bank that has entered into the BankID agreement with the subscriber.
Authority Information Access	Sertifikat-kontrollør (Informasjonstilgang for instans)	Standard extention, Mandatory	URL-adress that points to a validity authority service that shall validate the status of the certificate.
Subject Directory Attributes – Date of Birth	Fødselsdato	Standard extention, Mandatory	Date of birth of the subscriber
Authority Key Identifier	Nøkkelversjon for utsteder (Nøkkelidentifikator for instans)	Standard extention, Mandatory	Hash-value of issuer's public key
Subject Key Identifier	Nøkkelversjon for sert. holder (Nøkkelidentifikator for emne)	Standard extention, Mandatory	Hash-value of issuer's public key
Key Usage	Bruk av nøkler	Standard extention, Mandatory, Critical	Limitation on use must be followed by a computer program that uses BankID keys and certificates. Three different certificates with their own bitmap is defined. Non-repudiation, or Digital Signature/Key Agreement, or Key Encipherment/Data Encipherment

Qualified Certificate Statements	Kvalifisert sertifikat erklæringer	Standard extention, Mandatory	Reference to statement that this certificate is issued as a qualified certificate and any limitations on value on transactions.
Subject Alt Name	Alternativt Navn	Standard extention	The subscriber's email address (There are no BankIDs at the present stage that are issued with the use of this field).

Table 7: BankID: the certification profile (Source: [2])

C Risk Analysis Results of BankID Solution

Number	Analyzed Object	Observation	Risk Mitigation
1	Authentication Service	Because the authentication procedure in BankID utilizes NBNs and denies an end-user access after a few wrong login trials, it is particularly vulnerable to DDoS attacks—just like the authentication procedures in the other Norwegian Internet banking systems. The potential DDoS attacks represent a growing risk to end-users and web site owners.	The policy of using NBNs to identify customers and denying them access after a few wrong login trials must be changed because it enables efficient DDoS attacks on the application layer, potentially affecting more than two million customers in the near future.
2	Authentication Service	The end-user authentication in BankID is no stronger than the two-factor authentication used in many older Internet banking systems.	A new end-user authentication solely based on the end-user's public-private key pair will increase the strength of the authentication beyond what is possible with traditional two-factor authentication.
3	Authentication Service	Combined phishing/MitM attacks can be used to steal sessions initiated by BankID customers because it is possible to change the addresses to which the BankID client connects.	Transactions should be authenticated for BankID to become more robust against combined phishing/MitM attacks.
4	Authentication Service	BankID is potentially vulnerable to combined DDoS/phishing attacks where customers are tricked into entering one-time PINs and passwords on fake Internet banking sites.	Passwords and PINs should not be transmitted from a BankID client to the central infrastructure and should only be used locally by the end-user to give the client access to the end-user's PKI credentials.
5	Authentication Service	A BankID server utilizing an encrypted PKCS#12 file to store the private key is potentially vulnerable to well-known password attacks to decrypt the file, and DoS attacks where malware deletes the file.	All web applications using BankID should employ HSMs to store private keys.
6	Non-repudiation Service	The non-repudiation service in BankID gives a bank an advantage over its customers during conflicts involving repudiation of digital signatures because the customers cannot rely on help from a trusted third party.	The Norwegian banks should release information about the technical and legal non-repudiation protocols. In particular, the banks need to publish their dispute resolution procedures.

7	Non-repudiation Service	Only web sites utilizing HSMs to store and use private keys can support a high level of non-repudiation.	Web site owners wanting to use the service must invest in HSMs to store cryptographic keys.
8	Non-repudiation Service	The security-through-secrecy policy of the BankID-member banks gives them an advantage over their customers during conflicts because the customers and their lawyers have no access to technical information about the non-repudiation service.	See mitigation strategy for risk# 6
9	Non-repudiation Service	The end-user authentication in BankID limits the degree of non-repudiation. The strength of the authentication should be increased before customers digitally sign contracts concerning large-valued assets.	The strength of the authentication should be increased to improve the level of non-repudiation.
10	Privacy risks	The Norwegian banking community controls an ID system with the potential to build detailed profiles of roughly half of the Norwegian population as long as the BankID authentication utilizes X.509 certificates and NBNs. The BankID customers don't know how their personal information is utilized.	The BankID system should be reviewed by independent privacy experts before it is allowed to become a de facto national ID system. Identified weaknesses in the privacy protection should be carefully examined and mitigated. In the long run a new authentication procedure, not using X.509 certificates and NBNs, should be introduced to minimize the system's negative effect on the end-users' privacy.

Table 8: BankID: Risk Analysis Results (Source: [3])

Bibliography

[1] de Brisis, K., Mansfield, N., & Rundle, M. The role of digital identity management in the internet economy: a primer for policy makers. Technical report, Organisation for Economic Co-operation and Development, Directorate For Science, Technology And Industry, Committee For Information, Computer And Communications Policy, 2009.

[2] September 2010. Norsk bankid sertifikatpolicy for banklagrede kvalifiserte sertifikater til personkunder (personbankid), v 1.4.

[3] Hole, K. J., Tjøstheim, T., Moen, V., helge Netl, L., Espelid, Y., Klingsheim, A. N., Er, B., Nsis, G. E., Hole, K. J., Tjøstheim, T., Moen, V., helge Netland, L., Espelid, Y., & Klingsheim, A. N. 2008. Next generation internet banking in norway.

[4] Hammerli, B. M. & Arendt, H. H. 2009. Challenges for the protection of critical ict-based financial infrastructures. In *ISSE 2008 Securing Electronic Business Processes*, Pohlmann, N., Reimer, H., & Schneider, W., eds, 319–326. Vieweg+Teubner.

[5] Sullivan, K., Gresser, J.-Y., & Hämmerli, B. D2.2 identity management and protection in critical financial infrastructures topics. Technical report, Parsifal Project, June 30, 2009.

[6] Llarena, R., Morrow, S., Gresser, J. Y., Sullivan, K., Hämmerli, B., Arendt, H., & Buschman, T. March 22, 2010. D3.6 gap analysis and future needs report.

[7] Rossler, T. & Tauber, A. 2010. The spocs interoperability framework: Interoperability of edocuments and edelivery systems taken as example. In *ISSE 2010 Securing Electronic Business Processes*, Pohlmann, N., Reimer, H., & Schneider, W., eds, 122–130. Vieweg+Teubner.

[8] Leitold, H. & Zwattendorfer, B. 2010. Stork: Architecture, implementation, and pilots. In *ISSE 2010 Securing Electronic Business Processes*, Pohlmann, N., Reimer, H., & Schneider, W., eds, 131–142. Vieweg+Teubner.

[9] Rannenberg, K. & Royer, D. 2009. Open challenges — towards the (not so distant) future of identity. In *The Future of Identity in the Information Society*, Rannenberg, K., Royer, D., & Deuker, A., eds, 391–399. Springer Berlin Heidelberg.

[10] Q3 2010. Industry roundtable: Digital security and id: how far still to go? *SWIFT Dialogue*, Issue 25, pp. 42–46.

[11] Stevens, T., Elliott, J., Hoikkanen, A., Maghiros, I., & Lusoli, W. 2010. The state of the electronic identity market: Technologies, infrastructure, services and policies.

[12] Proskurovska, V. & Pawlik, K. Eu banking sector: Facts and figures. Technical report, European Banking Federation, 2010.

[13] Yin, R. 2003. *Case study research: design and methods*. Applied social research methods series. Sage Publications.

[14] Leedy, P. & Ormrod, J. 2009. *Practical Research: Planning and Design*. Alternative eText Formats Series. Prentice Hall.

[15] Osterwalder, A. *The Business Model Ontology: A Proposition in a Design Science Approach, PhD Thesis*. PhD thesis, University of Lausanne, 2004.

[16] Osterwalder, A. & Pigneur, Y. 2010. *Business model generation: a handbook for visionaries, game changers, and challengers*. Wiley, Hoboken, New Jersey.

[17] Cameron, K. 2005. The laws of identity.

[18] Identity management task force report. Technical report, National Science and Technology Council, Subcommittee on Biometrics and Identity Management, 2008.

[19] 2006. Information technology- security techniques- a framework on identity management, iso/iec j1sc 27, iso/iec wd 24760.

[20] Cameron, K., Posch, R., & Rannenberg, K. 2008. Proposal for a common identity framework: A user-centric identity metasystem.

[21] Chappell, D. Introducing the azure services platform: An early look at windows azure, .net services, sql services, and live services. Technical report, David Chappell And Associates, 2008.

[22] December 15, 2010. Specification of the identity mixer cryptographic library version 2.3.2.

[23] Brands, S. & Paquin, C. March 2010. U-prove cryptographic specification v1.0.

[24] Thompson, G. & Paquin, C. U-prove ctp white paper. Technical report, Microsoft corporation, March 2010.

[25] Paquin, C. March 2010. U-prove technology integration into the identity metasystem v1.0.

[26] Schneier, B. 2008. The psychology of security.

[27] Dhamija, R. & Dusseault, L. 2008. The seven flaws of identity management: Usability and security challenges. *IEEE Security and Privacy*, 6, 24–29.

[28] 2011. National strategy for trusted identities in cyberspace.

[29] U.s. cyberspace policy review.

[30] An open market solution for online identity assurance.

[31] Open identity trust framework (oitf) model.

[32] Commision, E. December 2010. European interoperability framework (eif) for european public services.

[33] Stefanova, K. & Nikolov, R. 2008. Interoperability of cross-border european egovernment services: some design issues. *Serdica Journal of computing*.

[34] Pouloudi, N. & Kalliamvakou, E. 2007. A qualitative evaluation of a cross-border identity management system to support public administration: insights and lessons learned.

[35] Hartmann, D. & Körting, S. Security issues in cross-border electronic authentication. Technical report, European Network and Information Security Agency (ENISA), February 2010.

[36] Posch, R. 2008. A federated identity management architecture for cross-border services in europe. In *In Proceedings of BIOSIG*.

[37] Heppe, J. Stork: D5.8.2 technical design for peps, mw models and interoperability. Technical report, 2010.

[38] Stork: D5.7.2 functional design for peps, mw models and interoperability. Technical report, 2010.

[39] May 16 2011. Electronic banking internet communication standard specification, version 2.5.

[40] Thorvaldsen, G. 2008. Fra folketellinger og kirkebøker til norsk befolkningsregister. *Die Heilkunst (Heilkunst)*, 45, 341–359.

[41] Skattedirektoratet. 2007. For 2007-11-09 nr 1268: Forskrift om folkeregistrering. Hefte 11.

[42] Klingsheim, A. N. & Hole, K. J. 2008. Identity theft: Much too easy? a study of online systems in norway. 192–196. Springer-Verlag, Berlin, Heidelberg.

[43] Rettsavdelingen, S. 2011. *Håndbok i folkeregistrering, versjon 1.7*. Skattedirektoratet Rettsavdelingen.

[44] Skatteetaten. 2010. Rekordhøy bruk av offentlige tjenester på nettet (http://www.skatteetaten.no/no/Artikler/2010/Hva-gjor-folkeregisteret/) (accessed 19.01.2011).

[45] Graux, H., Inte, Florin Inte Majava, J., & Meyvis, E. eid interoperability for pegs: Norway country profile. Technical report, IDABC, European eGovernment Services, July 2009.

[46] DiFi. October 2010. Rekordhøy bruk av offentlige tjenester på nettet (http://difi.no/artikkel/2010/10/rekordhoy-bruk-av-offentlige-tjenester-paa-nettet) (accessed 05.01.2011).

[47] 2010. Hva er bankaxess? (http://www.bankaxess.no/no/hoved/bankaxess/) (accessed 05.01.2011).

[48] 2009. Now norwegians can change bank in just a few seconds (http://www.edb.com/en/Corporate/Current/Topics/Now-Norwegians-can-change-bank-in-just-a-few-seconds/) (accessed 15.02.2011).

[49] Johnsen, B. September 05, 2005. Bankid coi white paper v1.0.

[50] Semming, A. 2010. Bankid - a norwegian eid provided by retail banks. In *Presentation for EPCA workshop*.

[51] 2009. Bankid på mobil (https://www.bankid.no/Dette-er-BankID/BankID-pa-mobil/) (accessed 05.01.2011).

[52] September 2010. Sertifikatpolicy for bankid på mobil - kvalifiserte sertifikater til personkunder, v 1.2.

[53] 2010. Banker som tilbyr bankaxess (http://www.bankaxess.no/no/hoved/bankaxess/banker-som-tilbyr-bankaxess/) (accessed 05.01.2011).

[54] 2011. Her kan du benytte bankid (https://www.bankid.no/Dette-er-BankID/Her-kan-du-benytte-BankID/) (accessed 15.01.2011).

[55] Committee on Authentication Technologies, N. R. C. 2002. *IDs — Not That Easy: Questions About Nationwide Identity Systems*. National Academies Press.

[56] Gjøsteen, K. 2008. Weaknesses in bankid, a pki-substitute deployed by norwegian banks. In *Public Key Infrastructure*, Mjølsnes, S., Mauw, S., & Katsikas, S., eds, volume 5057 of *Lecture Notes in Computer Science*, 196–206. Springer Berlin / Heidelberg.

[57] Espelid, Y., Netland, L., Klingsheim, A., & Hole, K. 2008. A proof of concept attack against norwegian internet banking systems. In *Financial Cryptography and Data Security*, Tsudik, G., ed, volume 5143 of *Lecture Notes in Computer Science*, 197–201. Springer Berlin / Heidelberg.

[58] Østmoe, J. S. 2009. Bankid. *MACAW CARD BULLETIN: NORDIC EDITION*, 16.

[59] October 2009. Overordnede iktarkitekturprinsipper for offentlig sektor, ver. 2.0.

[60] Flash eurobarometer 225: Data protection in the european union - citizens' perceptions. Technical report, The Gallup Organization, 2008.

[61] Hofstede, G. H. & Hofstede, G. 1984. *Culture's consequences: International differences in work-related values*. Sage Publications, Inc.

[62] Aykut, A. 2009. Cross-cultural analysis of european e-government adoption. *World Applied Sciences Journal*, Vol. 7, No. 9, 1124–1130.

[63] Noack, T. & Kubicek, H. 2010. The introduction of online authentication as part of the new electronic national identity card in germany. *Identity in the Information Society*, 3, 87–110.

[64] Aichholzer, G. & Strauß, S. 2010. The austrian case: multi-card concept and the relationship between citizen id and social security cards. *Identity in the Information Society*, 3, 65–85.

[65] Hoff, J. & Hoff, F. 2010. The danish eid case: twenty years of delay. *Identity in the Information Society*, 3, 155–174.

[66] Grönlund, k. 2010. Electronic identity management in sweden: governance of a market approach. *Identity in the Information Society*, 3, 195–211.

[67] Hamann, U. 2010. Germany on the road to electronic proof of identity. In *ISSE 2010 Securing Electronic Business Processes*, Pohlmann, N., Reimer, H., & Schneider, W., eds, 1–9. Vieweg+Teubner.

[68] Margraf, M. 2010. The new german id card. In *ISSE 2010 Securing Electronic Business Processes*, Pohlmann, N., Reimer, H., & Schneider, W., eds, 367–373. Vieweg+Teubner.

[69] Arendt, D. & Braun, W. 2010. Ausweisapp and the eid service/server - online identification finally more secure. In *ISSE 2010 Securing Electronic Business Processes*, Pohlmann, N., Reimer, H., & Schneider, W., eds, 374–383. Vieweg+Teubner.

[70] Appelgren, M. Swedish bankid a commercial national eid, information security solutions europe. 2010.

[71] Kubicek, H. & Noack, T. 2010. Different countries-different paths extended comparison of the introduction of eids in eight european countries. *Identity in the Information Society*, 3, 235–245.

[72] Kubicek, H. & Noack, T. 2010. The path dependency of national electronic identities. *Identity in the Information Society*, 3, 111–153. 10.1007/s12394-010-0050-2.

[73] March 2011. The nilson report, issue 968.

[74] VISA. March 2011. Visa corporate fact sheet.

[75] Europe, V. December 31 2010. Visa europe annual report.

[76] 2010. "2010 form 10-k visa inc.", united states securities and exchange commission.

[77] VISA. *Rules for Visa Merchants: Card Acceptance and Chargeback Management Guidelines*. VISA, 2006.

[78] VISA. *Interchange: What it is. How it works. And why it is fundamental to the Visa payments system*. VISA, 2008.

[79] Stearns, D. 2011. *Electronic Value Exchange: Origins of the VISA Electronic Payment System*. Springer London.

[80] Hock, D. 2005. *One From Many: VISA and the Rise of Chaordic Organizations*. Berrett-Koehler Publishers, Inc.

[81] VISA. Visa advanced authorization (http://www.advancedauthorization.com/index.html) (accessed 15.05.2011).

[82] VISA. *VisaNet: The technology behind Visa digital currency*. VISA, 2010.

[83] Stearns, D. 2006. In plastic we trust: Dependability and the visa payment system.

[84] Paulson, L. 2002. Verifying the set protocol: Overview.

[85] VISA. December 2006. Verified by visa: System overview external version 1.0.2.

[86] VISA. *Visa Public Key Infrastructure: Certificate Policy (CP)*. VISA, February 2011.

[87] VISA. *Visa International Operating Regulations*. VISA, 2011.

[88] VISA. *Visa International Operating Regulations - Core Principles*. VISA, 2010.

[89] 2000. 2000/520/ec: Commission decision of 26 july 2000 pursuant to directive 95/46/ec of the european parliament and of the council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the us department of commerce (notified under document number c(2000) 2441) (text with eea relevance.).

[90] SWIFT. Swift annual review 2010. Electronicaly.

[91] SWIFT. *SWIFT By-laws*. SWIFT, June 2009.

[92] SWIFT. *General Terms and Conditions*. SWIFT, January 2010.

[93] SWIFT. *User and shareholder eligibility criteria*. SWIFT, September 2009.

[94] Scott, S. V. & Zachariadis, M. 2010. A historical analysis of core financial services infrastructure: society for worldwide interbank financial telecommunications (swift).

[95] SWIFT. *3SKey Service Description*. SWIFT, September 2010.

[96] SWIFT. *3SKey Fact Sheet*. SWIFT, 2010.

[97] Pkcs#7 v1.6: Cryptographic message syntax standard. Technical report, RSA Laboratories, 1997.

[98] SWIFT. *3SKey Portal Online Help*. SWIFT, September 2010.

[99] IdenTrust. Identrust: Trust network certificates, 2010.

[100] IdenTrust. The identrust rule set: Providing secure identities while protecting privacy, 2007.

[101] IdenTrust. Identrust trust prime: Electronic bank account and signatory management, 2010.

[102] IdenTrust. The identtrust trust prime. video demonstration (http://identrust.com/demos/video/trustprime_video.html) (accessed 15.05.2011).

[103] IdentTrust. *IdenTrust Compliant Certification Guide For Technology Providers, Version 3.1*. IdentTrust, April 2004.

[104] IdenTrust. Identrust trust infrastructure: A foundation of trust for business applications, 2010.

[105] Stabell, C. B. & Øystein D. Fjeldstad. 1998. Configuring value for competitive advantage: on chains, shops, and networks. *Strategic Management Journal*, 19, 413–437.

[106] Porter, M. E. 1985. *Competitive advantage: Creating and sustaining superior performance*. Free Press, New York and London.

[107] Biem, A. & Caswell, N. January 22 2008. A value network model for strategic analysis. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences*. IBM T. J. Watson Research Center.

[108] LI, F., TIAN, C., CAO, R., & JIANG, S. 2008. Value network model for service ecosystem in business environment.

[109] Blau, B., Kramer, J., Conte, T., & van Dinther, C. 2010. Service value networks.

[110] Woiceshyn, J. & Falkenberg, L. 2008. Value-creation in knowledge based firms: Aligning problems and resources.

[111] Eisenmann, T., Parker, G., & Van Alstyne, M. W. October 2006. Strategies for two-sided markets. *Harvard Business Review*.

[112] Evans, D. S. Fall 2003. Managing the maze of multisided markets. *Strategy+Business*, issue 32.

[113] Rochet, J.-C. & Tiroley, J. 2004. Two-sided markets: An overview.

[114] Rochet, J.-C. & Tiroley, J. December 13 2002. Platform competition in two-sided markets.

[115] Basel committee on banking supervision "management and supervision of cross-border electronic banking activities". Technical report, Bank for International Settlements, July 2003.

[116] *FFIEC Authentication in an Internet Banking Environment*, 2001.

[117] Koble, S. & Böhme, R. 2006. Economics of identity management: A supply-side perspective. 3856, 259–272.

[118] Spiekermann, S. 2003. Die konsumenten der anonymität - wer nutzt anonymisierungsdienste? *Datenschutz und Datensicherheit*, 27(3).

[119] Camenisch, J. & Van Herreweghen, E. 2002. Design and implementation of the idemix anonymous credential system.

[120] Akerlof, G. 1970. The market for lemons: Quality uncertainty and the market mechanism.