UNIVERSITY OF TARTU
Faculty of Science and Technology
Institute of Computer Science
Computer Science Curriculum

Gediminas Milašius

Exploring integration complexity of different multi-national eID authentication solutions in the EU private sector

Master's Thesis (24 ECTS)

Supervisor(s): Axel Rose, MSc
May Flower, PhD

Tartu 2022

Exploring integration complexity of different multi-national eID authentication solutions in the EU private sector

Abstract:
Many interpreting program languages are dynamically typed, such as Visual Basic or Python. As a result, it is easy to write programs that crash due to mismatches of provided and expected data types. One possible solution to this problem is automatic type derivation during compilation. In this work, we consider study how to detect type errors in the WHITESPACE language by using fourth order logic formulae as annotations. The main result of this thesis is a new triple-exponential type inference algorithm for the fourth order logic formulae. This is a significant advancement as the question whether there exists such an algorithm was an open question. All previous attempts to solve the problem lead lead to logical inconsistencies or required tedious user interaction in terms of interpretative dance. Although the resulting algorithm is slightly inefficient, it can be used to detect obscure programming bugs in the WHITESPACE language. The latter significantly improves productivity. Our practical experiments showed that productivity is comparable to average Java programmer. From a theoretical viewpoint, the result is only a small advancement in rigorous treatment of higher order logic formulae. The results obtained by us do not generalise to formulae with the fifth or higher order.

Keywords:

List of keywords

CERCS:
CERCS code and name: `https://www.etis.ee/Portal/Classifiers/Details/d3717f7b-bec8-4cd9-8ea4-c89cd56ca46e`

Tüübituletus neljandat järku loogikavalemitele

Lühikokkuvõte:

One or two sentences providing a basic introduction to the field, comprehensible to a scientist in any discipline.

Two to three sentences of more detailed background, comprehensible to scientists in related disciplines.

One sentence clearly stating the general problem being addressed by this particular study.

One sentence summarising the main result (with the words “here we show´´ or their equivalent).

Two or three sentences explaining what the main result reveals in direct comparison to what was thought to be the case previously, or how the main result adds to previous knowledge.

One or two sentences to put the results into a more general context.

Two or three sentences to provide a broader perspective, readily comprehensible to a scientist in any discipline, may be included in the first paragraph if the editor considers that the accessibility of the paper is significantly enhanced by their inclusion.

Võtmesõnad:

List of keywords

CERCS:

CERCS kood ja nimetus: `https://www.etis.ee/Portal/Classifiers/Details/d3717f7b-bec8-4cd9-8ea4-c89cd56ca46e`

Contents

Unsolved issues

1 Introduction

1.1 Motivation

With the emergence of COVID-19, work from home has rapidly grown in popularity. It has been especially noticeable in the IT industry. This phenomenon has led some businesses to transition to operate fully remote [1], allowing for potential customers, clients, and employees to operate with the companies' IT systems from all around the globe.

Identity verification is a significant roadblock when establishing a remote work policy. In some managerial businesses, such as logistics, it is essential to assure the authenticity of persons signing in to perform their duties. Traditionally, as work was always on-premises, it was easy to verify the identity with the help of an ID Card or equivalent and physical verification. With the constraints of operations being fully remote, companies can no longer perform such a check.

Establishing identity online for potential employees and clients is not the only use case for digital identity. Organizations such as the British Council employ privacy undermining practices. They require their customers to submit a photocopy of their identity document for verification purposes [2]. This process is a significant privacy concern since anyone could replicate the uploaded document. Having no agency over their documents is of great concern for the end-users, and they would be reluctant to use the company services. Replacing the document upload with a digital signature check is a more secure and trustworthy way of performing business.

After the EU introduced the eIDAS regulation, an alternative method for identity verification became available. All EU member states are mandated to implement an eID solution in their country and recognize other countries' eID solutions [3]. Each eID solution comes with an identity certificate and means to prove it by signing a challenge via public-key cryptography. Because of this regulation, it is now possible to obtain a persons' legal identity with trustworthy means.

Particular risks exist that businesses must be aware of before integrating an eID authentication service. There are no comprehensive resources outlining the obstacles and costs of implementing eID authentication in the private sector. Lack of information makes it difficult to assess risks and estimate the resources required [?]. Unknown Cite risks are an excellent deterrent for innovation and make companies reluctant to use new technologies. Proper research into this subject may lead companies to take risks associated with implementation and kickstart the mainstream adoption of eIDs in the private sector.

1.2 Research Problem

The main goal of the thesis is to investigate if the advantages provided by eIDs are sufficient to warrant adoption in the free market and to shine a light on the costs associated with implementation. From this goal, the extracted research question is as follows:

What is the best eID authentication option available for an Estonian EU targeting enterprise for use in their Web-based Single Sign-On (SSO)?

Maybe it would be good to change to "is the market ready"

The research question can be refined further into additional sub-questions:

- What advantages do eIDs provide?
- What technological risks companies must address to implement the solution?
- What privacy considerations must companies take when processing user data?
- What are the categories of eID authentication solutions?

QESD vs. middleware

- What are the different eID authentication options available to Estonia's private sector?
  - What risks the eID provider transfers?
  - What is the market reach (in countries) of a given solution?
  - Where are the weak points in the protocol used? How should a company assess them?

1.3 Scope and goal

In the thesis, there will be some assumptions in place about the company wishing to implement eID authentication:

- Company in question already uses an HTTP-based SSO (in the cloud or on-premises);
- Company is willing to spend money for operational costs;

1.4 Contribution

The thesis aims to fill the research gap for the use of eID in the private sector. There is some research about connecting eIDAS nodes, but the focus was to connect eIDAS nodes of other countries and not connect customers to the eIDAS infrastructure.

* The two researches done about the private sector focused on only the eIDAS implementation. * Development cost analysis is ignored. * No instructions as to how

to properly connect to eIDAS node for businesses. * No research has been done on the development costs on any of the Estonia's eID authentication methods.

This thesis aims to fill the gaps by providing implementation instructions and comparison of 4 eID providers: Estonian ID-card, Smart-ID, Dokobit, and eeID.

Structure of work The document will consist of the following main chapters:

ISO standard to pick trust level for if companies even need it

What are different options in eIDAS, e.g. what is a QESSD

What are the differences between primary services and middlemen, advantages disadvantages

What are the weakpoints in the company structrue

What is the research model?

Findings about ID Card, Dokobit, and eeID

Non web-based SSO?

Ponder about the advantages of middleware pseudominization? Say instead of personal code you get some arbitrary ID that matters only in the system

2 Background

2.1 eID

In Estonia, digital identity has been around for over 20 years [4]. The Estonian government has loaded all identity cards issued with certificates enabling cardholders to identify themselves digitally. Compare the speed of adoption to Romania, where the first easy access to eIDs came in the form of new chip ID cards in August of 2021 [5].

Estonia's early adoption of eID, the political focus on digital government, has led to over 89% of internet users accessing the e-government, landing it the first place in the EU [6]. The 20 years of easy access to an eID has led to a stark difference to Romania, where only 16% of internet users access the government services online.

Depending on the country a company would like to access the market, eID sign-in may confuse the potential clients. Early adopters must be aware of the widespread adoption of the eID infrastructure.

In different countries, the eID solution may vary wildly. There can also be more than one eID solution in a singular county.

2.2 eIDAS

The eIDAS regulation [3] provided the groundwork for recognizing the signatures issued by other EU countries by imposing strict liability and mutual-recognition requirements. The regulation introduced the concept of a Trust Service Provider (TSP), which allowed relying parties to have a trust anchor. Each member state maintains a list of TSPs, where each TSP is certified to perform specific tasks, such as timestamping or issuing signing certificates. The regulation also requires member states to establish eID systems, if they haven't already, and make them able to be integrated into a federal system.

The regulation was the basis for creating the eIDAS node network [7]. These nodes connect across country borders, allowing users to authenticate with the eID of their home (eID issuer) country in the host (current residence) country. The eIDAS authentication protocol redirects the authentication requests to the appropriate country, federating the identification process. For the institutions trying to target the EU market, this provides a significant advantage since access to one node would mean access to all nodes in the EU.

The main issue private companies will encounter is the highly restricted access to any nodes. The eIDAS network is only concerned about connecting countries. To allow access to the web would be up for the member state to decide.

2.3 eID widespread adoption

2.3.1 eID adoption in Estonia and Lithuania

On the surface, Estonia and Lithuania have the exact eID solutions - Bank Link, ID card, Mobile-ID, and Smart-ID. However, even with the same infrastructure, we see many inconsistencies even in the case of just these two countries.

Consider Lithuania. It is possible to connect from a centralized website `https://epaslaugos.lt` to access the public sector services [8]. Here it is possible to sign in via bank link, ID card, and Mobile-ID. Smart-ID is not part of the list. Although most banks support sign-in via three major eID providers, including Smart-ID, some listed banks like PaySera provide significant security concerns. With that bank, it is possible to access the e-government services with only email, password, and a 2FA code sent to the registered person's phone number . For this reason, Estonia's Information System Authority has taken steps to deprecate bank link [9] from use in TARA. In Estonia, all three major authentication options, ID card, Mobile-ID, and Smart-ID, are available to access the e-government.

source: I did it myself 02-27

2.3.2 eIDAS notifications in Estonia and Lithuania

For countries to communicate through the eIDAS node network, countries must notify the European Commission about what eID authentication methods they could provide [3]. Other countries can then use these methods to authenticate foreign citizens into their public services.

In the case of Estonia, the country has notified the European Commission about its Smart card and Mobile-ID authentication methods [10]. Smart-ID is not a permitted method of authentication in the context of eIDAS. In Lithuania's case, only the Smart card solution is allowed - no mobile sign-in methods have been notified [10].

Estonia and Lithuania have shown a gap between what countries consider to be a secure and trusted source of eID and what they are willing to be held liable for in the context of eIDAS.

2.4 eID providers in Estonia

Applied Cyber Security Group of the University of Tartu maintains a list of e-services [11] that uses at least one eID authentication method in Estonia. The following authentication methods were listed: Bank Link, ID-card, Mobile-ID, Smart-ID, TARA, and HarID.

2.4.1 Bank link

Banks have initially created this authentication method to provide close integration with e-commerce providers to receive risk-free payments [12]. Over time it saw an additional use case - secure and trustworthy authentication method for the public and private services [13]. Over time researchers found that the protocol used was extremely insecure [14]. From March of 2021, RIA has disabled the use of bank link to access public services [9], which accounted for only 1 percent of all authentications.

Due to the lack of security auditing required to satisfy eIDAS, poor market reach, and no support from the government, this authentication method will not be discussed in the scope of this thesis.

2.4.2 ID-card

Id cards are the most popular way to access their eID in Estonia, primarily due to the legal requirement of having one. Chapter 2 of the Identity Documents Act [4] requires all EU, not only Estonian, citizens residing in Estonia to hold an ID card, with which they could access public services online. Interestingly, this requirement caused the government to issue more ID cards than there are people in Estonia [15, 16].

There are no variable costs to allow a person to log in to websites with their ID card. For this authentication method, no per-transaction fees exist, as the certificate validity service (OCSP) [17] can be queried for free.

An end user's computer can extract an authentication certificate from their ID card with the help of special software distributed by the government [15]. This certificate, once on the computer, can be sent to the private company's authorization server with Client Certificate TLS option [18] natively or with the use of specialized helper library [19], using standard REST calls.

Qualified trust service provider for Qualified Certificates for e-signatures installs the certificates in ID-cards [20], which ensures a high degree of certainty about the identity of person authenticating.

Why does this matter?

A significant advantage of using a decentralized eID infrastructure, such as the ID-card authentication, is that there are no middlemen in the process, allowing companies to skip going into expensive contracts with an eID service provider.

2.4.3 Mobile-ID

Five years after SK ID Solutions introduced ID cards for use in Estonia, they have developed a mobile phone-friendly way to access the users' eID for use in Estonia and Lithuania [21]. SK achieved it by extending the functionality of SIM cards to make them mimic the functionality of ID cards.

The price of using Mobile-ID for the service provider varies based on usage, starting from 10 euro per month (10ct per request) to costing over 5 000 euro, where the effective cost is under 1ct for request [22]. For the end-user, mobile operators can charge an additional fee for the use of this service [23].

Accepting Mobile-ID would allow companies to access the markets of two countries: Estonia, and Lithuania, as the technical implementation is identical.

Qualified trust service provider for Qualified Certificates for e-signatures installs the certificates in a particular variety of SIM cards, capable of supporting Mobile-ID [20], which ensures a high degree of certainty about the identity of person authenticating.

Explain why companies should not consider this protocol in the protocol choice section.

2.4.4 Smart-ID

Smart-ID is the latest and fastest-growing way of accessing citizens' eID, working in all 3 of the Baltic States [24]. The protocol utilizes mobile phones as authentication, similar to Mobile-ID. Unlike Mobile-ID, it does not require specialized external hardware [25]. The authentication process is handled by combining the eID server and the end user's smartphone. Despite that, it still passed the eIDAS compliance audit for the requirement of ensuring signature private key is "with a high level of confidence under sole control" of its owner [26]. After passing the audit, Smart-ID was recognized as a QSCD, allowing it to create QES in 2018 [27].

The price of using Smart-ID for service providers, much like Mobile-ID, varies based on usage, starting from 50 euros per month (10ct per request) to over 20 000 euros, where the effective cost is under 1ct for request, based on the total amount of transactions performed within a month [28]. For users, unlike Mobile-ID [23], there are no telecommunication operators involved, and there are no costs associated with using Smart-ID.

Implementation of Smart-ID would allow users to access the markets of three countries: Estonia, Latvia, and Lithuania.

Qualified trust service provider for Qualified Certificates for e-signatures users their data centers to hold part of the private key and certificate used to authenticate users [20], which ensures a high degree of certainty about the identity of person authenticating.

2.4.5 TARA

TARA is Estonia's primary gateway for authentication to public services [29]. TARA provides the ability for users to sign in with any of the three primary eID methods of Estonia and with the eID schemes of other EU member states. The ability to authenticate with the systems of other countries is of particular interest, as it also doubles up as the official eIDAS node of Estonia [29].

Estonian Information System Authority intends to limit the use of TARA to public services only [30].

Technical implementation for the consumer, unlike Mobile-ID and Smart-ID, will be much easier to implement, as it uses the well-adopted protocol of OpenID Connect

[31, 32].

It is worth mentioning while the underlying authentication methods have received proper eIDAS auditing and are backed by a qualified trust service, this and all of the following authentication methods have not been audited in compliance with eIDAS.

Unlike the eID providers backed by a Trust Service Provider, TARA acts as only an authentication service. It would not be able to provide means of signing documents [31]. If the business is considering expanding to allow for online digital signing, an infrastructure like TARA will unlikely be a great choice.

2.4.6 eeID

Estonian Internet Foundation created eeID service for the exclusive purpose of bringing eID authentication to the private sector [33]. It is a clone of TARA without it being Estonia's gateway for the eIDAS node network. The similarities mean that all points outlined to TARA apply to this service too.

The service is new, does not have pricing tiers, and currently asks for 9ct per successful authentication request [34].

The vision of the said service is to allow users to access the markets of all EU countries. Currently, there are only fourteen countries with notified eID authentication methods [10]: Estonia, Germany, Italy, Spain, Belgium, Luxembourg, Croatia, Portugal, Latvia, Lithuania, Netherlands, Czech Republic, Slovakia, and Denmark.

Does it work? Have to wait as much as I can

2.4.7 HarID

Estonian Ministry of Education and Research created this service for the youth of Estonia to access different educational institutions across Estonia [35]. ID cards are only legally required to be held by citizens over the age of 15 [4], so everyone under would have been unable to access their school system. HarID accepts TARA authentication methods with the addition of username & password. This authentication method is held exclusively for the education sector and will be skipped over in this thesis.

2.4.8 Dokobit

In the initial list of services using eID in Estonia [11], one service stands out - Dokobit [36]. They provide services comparable to eeID in that they aggregate different eID methods of Estonia (ID-card, Mobile-ID, and Smart-ID) and other countries. The primary difference between the authentication providers is the multi-national implementation goal - Dokobit relies on integrating each country's system individually. In contrast, eeID depends on using the framework of the eIDAS infrastructure [33].

Pricing for Dokobit varies drastically, and the provided prices for the Baltic States [37] start at 50 euros per month (7.1ct per request), going down to 4.2ct per request at

500 euros per month.

Dokobit supports 11 countries: Estonia, Italy, Spain, Belgium, Latvia, Lithuania, Finland, Norway, Iceland, Poland, and Portugal [36].

UAB Dokobit is a trust service provider for Qualified validation of qualified e-signature. It means the service itself does not provide Digital Signature certificates, but eIDAS considers the results of validation of signatures trustworthy [20].

2.5 Authentication and eID and QSCD

Maybe find a better spot for this section

Fact check?

The requirements for Estonian ID cards make a clear distinction between "ADF AWP" and "ADF QSCD" applications. Both software applications are loaded onto the smart card; however, only the QSCD application, guarded by PIN2, can create QES. Implication here is that for authentication with an ID card, a QSCD is not used.

Fundamentally, the only legal guarantees provided by eIDAS require the use of QSCD [3], and for authentication this process, this device is not used [38]. It is up to the relying party to trust the authentication certificate and signature associated with the authentication challenge. This technicality affects business in only the document signing part of the business - using encryption or authentication certificates does not provide the necessary legal guarantees.

Similarly, when using a third-party provider such as TARA (eeID) or Dokobit, the new eID provider acts as a new trust anchor. Companies must consider the risks of using such providers, as adding any middleware increases the attack surface on the company.

2.6 Levels of assurance

Levels of assurance section

2.7 GDPR

When dealing with eID, sensitive personal data processing is required.

GDPR section

2.8 Federated Identity Architecture of the European eID System

The authors of this paper describe the current situation in the identity management landscape [39]. The researchers provide all the necessary background information to understand the implementation details of any eID authentication system design.

Does this belong in related work? This paper is de-facto required background

2.8.1 Authentication methods

The first significant contribution relates to explaining different ways of authenticating persons.

Any authentication method is based on something user knows (password, pin code, answer to security question), is (biometrics - eyes, fingerprints), or has (physical device - key card, USB device) [40]. Any other method would leave the person without agency over the authentication process.

An emphasis is put on the importance of mixing and matching these authentication schemes to increase the system's security.

2.8.2 Authentication Paradigms and Models

The second helpful point of the paper is the description of different identity management paradigms and models [41]. Paradigms refer to the implementation and deployment, whereas models refer to the data storage and roles.

The three main paradigms as network, service, or user-centric. The network-centric approach gathers all identities into one place, usually known as a "Domain Controller." The service-centric method would create a new identity for each service, leading to high duplication. The user-centric paradigm makes the user prove their own identity. Europe's eID solution does not favor any of the paradigms allowing identity providers to innovate [4, 33, 36].

There are also three authentication models: isolated, centralized, and federated. Unlike paradigms, where any of them is fair game, Europe's identity providers can use only the federated one. The isolated model requires all services to hold a copy of every identity in the EU. The centralized model is suitable for having a central place for looking up identity in a country, and it is an excellent solution for high-profile agencies. The federated system has the advantage of scaling well horizontally and not requiring to keep an index of all citizens it would like to serve, which is a tremendous advantage in the world of GDPR.

2.8.3 Authentication protocols and services

Researchers have allocated a good portion of the paper to provide an overview of potential protocols and implementations. The list is massive and in-depth; however, it becomes clear that SAML [42], OAuth2.0 [43], and OpenID Connect [32] protocols are by far the most popular protocols to choose for implementation. The engineers behind the eIDAS network implementation decided to settle on the SAML protocol.

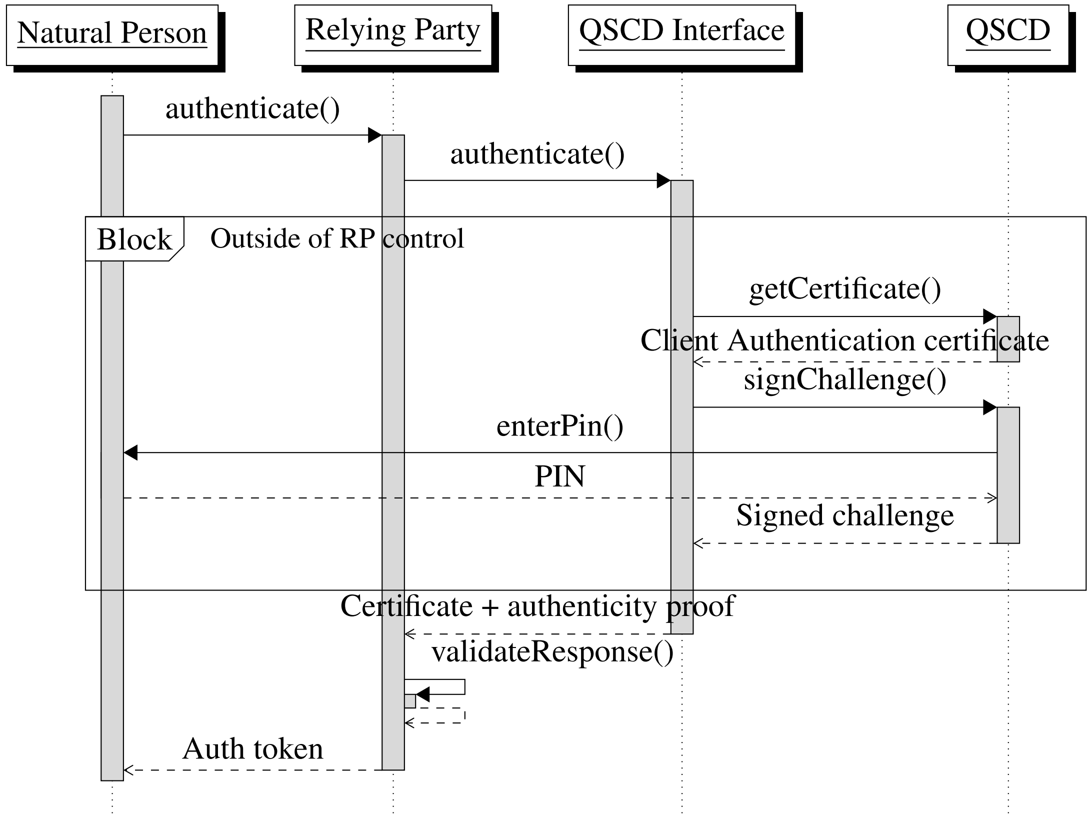

Figure 1. High-level sequence diagram of a eID authentication flow

2.9 Threats

There has to be a source with the extensive list, all protocols I checked look basically the same, but I can't seem to find a post saying yes, you need to do this.

In the sequence diagram (see figure 1), we see a high-level overview of any eID authentication solution. In the authentication protocol, the relying party (company implementing eID sign-in) is entirely dependent on the QSCD interface, which acts as a trust anchor. A communication channel exists between the relying party and the interface. We can categorize the channel type into two groups:

1. trusted, where the sender can reasonably guarantee that adversaries are unable to change the data in transit (Smart-ID, TARA, Dokobit);

2. untrusted, where there is a possibility for data to be tampered with in transit (Web eID).

Trusted communications generally operate using an encrypted backchannel, where untrusted ones require the client to send data from the QSCD interface. Because the client sends the data, this becomes an untrusted channel, and the relying party must perform additional certificate verification.

Failure to encrypt and establish the authenticity of the interface in a trusted backchannel or not validating data in a untrusted channel allows adversaries to perform man-in-the-middle attacks.

Limitations: For the scope of the thesis, only two security aspects will be analyzed: the network communication between the natural person and the interface and the certificate authenticity guarantees. Security analysis of QSCD and its communications with the interface will not be analyzed.

Further research? Limitations: proper analysis of what companies would like to see in a solution for easier bullet points

3 Related Work

3.1 National e-ID card schemes: A European overview

In 2008, researcher Siddhartha Arora investigated different uses of eID in Europe [44].

The published technical report leads us to believe that at the time, the eID technology was still in its infancy, and the concept of eID was tied to it being linked to a physical ID card.

Paper references that eID cards offer three forms of information security functionality: identification, authentication, and signature (see table 1).

Table 1. Forms of information security functionality provided by eID [44, 45]

Identification (I)	A can prove to B that he is A, but someone else can not prove to B that he is A.
Authentication (A)	A can prove to B that he is A, but B can not prove to someone else that he is A.
Signature (S)	A can prove to B that he is A, but B can not prove to himself that he is A.

The idea of splitting functionality into identification, authentication, and signature can be verified today in Estonian [38], and Lithuanian [46] ID cards. In these cards, there are two certificates — one for client authentication and the second for digital signature.

These authentication and identification certificates are not encrypted, and can anyone with the correct tools can read them from the ID card. Signed documents also have a copy of the certificate attached. These certificates identify a person, but due to ease of replication, the recipient should not trust the sender's certificate because there are no guarantees that the certificate belongs to the sender.

The authentication and signing certificates require their respective keys to perform asymmetric cryptographic operations. In theory, it is possible to sign documents with the authentication certificate; however, the verification software will reject such signatures because the certificate's purposes would not include digital signature.

Maybe move this out?

The paper mentions Austria wants to have multiple sources of eID, not limit themselves only to one card. Many countries followed suit, and in Estonia, there are three primary sources of eID. In France, a source of eID doesn't even come from an ID card [47].

The paper's conclusion emphasizes the importance of the eID itself, not ID cards. The EU took this path when implementing the legislation for eIDAS, which allowed easier integration of infrastructure member states already had in place.

3.2 The Austrian eID ecosystem in the public cloud: How to obtain privacy while preserving practicality

This paper explores what information the Austrian government stores on the issued identity documents and what operations the documents can perform [48]. Researchers identified four types of functionality: identification and authentication of Austrian citizens, qualified electronic signature creation, encryption and decryption, data storage. This functionality matches Estonia's ID card.

Paper presented an interesting issue - Austria does not allow a person identifying code (CRR number) to be "used directly in e-Government applications due to legal data protection restrictions." Austria has created SourcePIN, where it is possible to create different ones for each service trying to access it [48, 49].

The paper's main contribution to this thesis is to remind that even though technological barriers are crumbling, there might still be legal obstacles to overcome. Austria is currently not part of the eIDAS node network, and it would be an excellent opportunity for further research to investigate what information Austria's eIDAS node provides.

The big concern of the study is that everything goes through one single source of trust, which does not scale well. If many people wanted to use the system, it would quickly become a bottleneck. Moving many essential components to the public cloud can alleviate the problem.

3.3 Secure cross-cloud single sign-on (SSO) using eIDs

The idea behind this paper seems to be very close to what I am trying to do. Researchers explore the possibility of users using an SSO system to log in via their eID instead of the traditional username/password authentication method [50]. As means of doing so, they explore the capabilities of the STORK framework and other frameworks seen in previous references. The STORK framework is the predecessor to eIDAS [51].

The idea of the STORK framework is that any EU citizen should be able to use their eID issued by their home country to authenticate with services in other countries. An example of an activity would be opening a bank with an Italian ID card. The paper suggests extending the framework to support federation so private business identity providers can use the security options provided by eIDs and not store weak passwords.

The paper shows a proof of concept prototype usage for bringing STORK to support SSO. Emphasis was given on the backward compatibility, not to require any breaking changes to an existing STORK protocol.

Researchers found that one SAML protocol, however similar they may be, is not compatible with one another. The consumer company wishing to implement the proposed protocol will have to make an adapter to implement different ID providers, such as STORK and Google. Ultimately it is an acceptable compromise.

3.4 Electronic identity verification: personal data protection challenges and risks

The thesis outlines the conflicting requirements of eIDAS or any other eID law with GDPR [52]. In the first part, the author presents the history and fundamentals of data protection in the EU. A significant portion of the thesis was allocated to describe the eIDAS law and how it affects privacy.

The second part of the thesis performs a couple of case studies.

The first case study is about Smart-ID.

Try to even talk about this trainwreck of a thesis with misleading sources?

3.5 EID @ Cloud: integración de la identificación electrónica en plataformas europeas en la nube de acuerdo con el reglamento eIDAS.

This paper talks about integrating a new eIDAS node with the private sector in mind [53]. The eID@Cloud research initiative has proven it possible to allow private citizens to integrate this system to authenticate persons. Potential does not mean ready and outlines some issues that need addressing.

Even though the eIDAS node infrastructure brings apparent benefits to the citizens, the public, private entities, and the service vendors, there are still caveats that slow the final integration of the EU digital identity platform. The project eiD@cloud shines light upon these barriers:

1. There are still some differences between the national schemes and the integrations of said national schemes in a unique and interoperable net that must be the eIDAS in the context of the EU.

2. The deployment of each eIDAS node of each member state happens at different speeds, creating mistakes and a lack of availability to complete the eIDAS project.

The interoperability testing consisted of accessing each partner's cloud platforms to verify the identities that belonged to the citizens of the other partners' countries. Norway's eIDAS node did not work with other countries' eID - the protocol executes correctly, but the user incorrectly received an error message asking for Norway identification. It shows that some parts of the system were not stable at the research time, but the whole infrastructure continued to run.

The eID@Cloud was a great project testing the implementation and readiness for public and private sectors, which provided excellent feedback for the EU Commission. The most important finding is that it would be possible for private entities to connect to the mesh.

3.6 LEPS - Leveraging eID in the private sector

This final research [54] was performed at a similar time to the eID@cloud [53], but in different countries. LEPS researchers have implemented an eIDAS node for private customers. However, they also provided market analysis.

The market analysis targeted four main categories of e-service providers:

1. Organizations that need or want to migrate from the existing identity and access management (IAM) solution. This could apply to organizations that have scaled out their internal or tailor-made IAM solutions or organizations that already use partially external or third-party e-identification or authentication services but are looking for a higher level of assurance (LoA).

2. Organizations that use low assurance third-party eID providers such as a social login want to elevate the overall level of security and decrease identity theft and fraud by integrating eIDAS eID services.

3. Organizations that are already acting or could be acting as eID brokers.

4. Organizations that want to open new service delivery channels through mobile phone and are interested in mobile ID solutions that work across borders.

In the case of the thesis, the targeted e-service providers are of the first category - organizations wishing to improve IAM solutions to include a higher level of assurance.

The researchers recommend using an approach like LEPS to integrate eID authentication rather than creating an eIDAS node. The primary reason for avoiding node creation would be the cost-effectiveness of implementation, as these adopters "are unlikely to have the know-how, resources, and capacity to implement eIDAS connectivity." "Many organizations do not have resources for eID service implementation and operation internally was already exploited by social networks." The targeted benefit is the "easy way to integrate highly scalable, yet low assurance, eID services."

4 Research

4.1 General security requirements

4.1.1 User ID tracking

4.1.2 User storage

focus on GDPR

4.2 Case study: Dokobit

4.3 Case study: eeID

4.4 Case study: Web eID

4.5 Case Study: Web eID

4.5.1 About

Released in the Summer of 2021 [19] and having undergone significant changes in January of 2022, this eID framework allows users to authenticate and sign documents using their smart cards.

Functionally this framework is split into three parts: custom software the user needs to install, a javascript library that acts as a data intermediary, and the certificate validation library on the back-end.

The software users need to install is similar to the one various countries' governments issue. The significant difference in this scenario is that the software supports more than one countries' eID solutions. The solution currently supports smart cards of Estonia, Latvia, Lithuania, and Finland [19].

4.5.2 Data Flow

Figure 2 displays the high-level overview of the complete flow of data within the Web eID framework. A detailed explanation of the steps can be found on the technical specification page [55]. Companies implementing the framework should only consider the browser and server application (steps 1-3 and 13-17).

4.5.3 Security Analysis

Researcher Arnis Paršovs published a security analysis of the protocol v1 in October of 2021 [56]. Developers behind the Web eID framework acknowledged the weaknesses and addressed them in v2 [55], which will be used in the scope of the thesis. At the time of writing, independent researchers and auditors have not yet performed security analysis for this version.

Actors The actors in the figure 1 assume the roles of: QSCD Interface - web-eid.js [57], web-eid-app [58]; QSCD - Smart cards of Estonia, Latvia, Lithuania, and Finland [19]. This interface is a separate application from the official id.ee software Estonian citizens use to sign and verify documents. However, "in the future, the final version of Web eID will be added into the ID-software installation package, available for the users the website on www.id.ee" [19]. Owners of other countries' smart cards would still have to download the special software.

Threat protection The framework uses an unsecure channel for communications, so special measures are required to be taken. Unlike in Dokobit and eeID, the risk of impersonation is not transfered to the eID service provider so the countermeasures must be performed by the relying party.

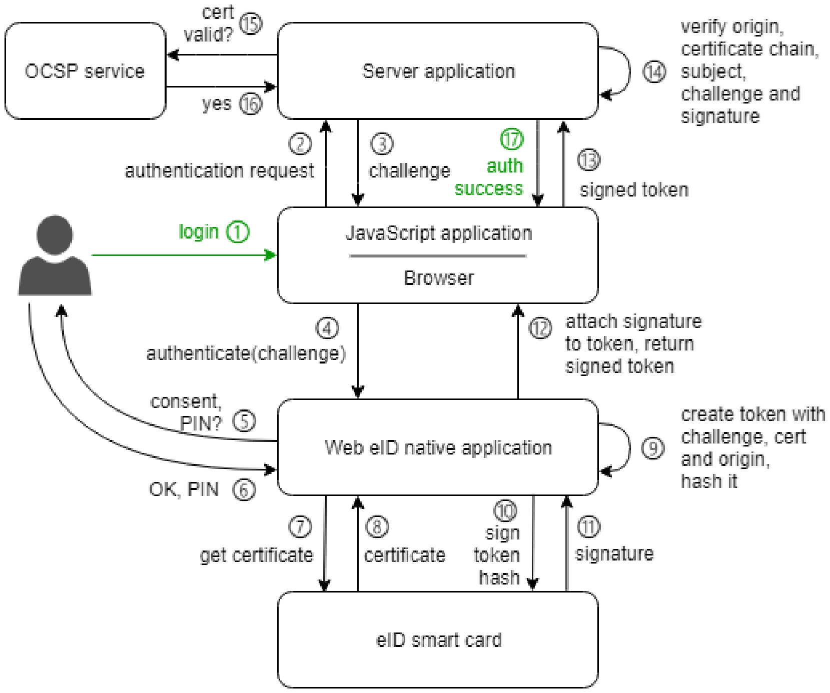

Figure 2. Web eID Authentication flow [55]

Discussion: suggest how the certificates are way too challenging to obtain for a casual company and may lead to additional vulnerabilities

Discussion: phishing attacks if company establishes policy to add certificates if they cannot sign in with their card

4.5.4 Trust Anchor

Unlike Dokobit and eeID, Web eID does not provide any guarantees about the trustworthiness of a certificate. It goes so far in the protocol to remind developers by sending the certificate in a field called "unverifiedCertificate" [59] because the application transfers the certificate from an untrusted source.

The relying party must verify the certificate and challenge themselves by checking the origin, certificate expiry, trust chain, OCSP responses, and the challenge. This validation structure makes the trust anchor technological and highly depends on the implementation correctness by the developers.

Discuss how we can never trust developers without proper supervision

More information can be found in the implementation section.

4.5.5 Pricing

This service is free of charge for the uses of authentication.

4.5.6 Maturity of the solution

4.5.7 Implementation

For each protocol implementation step, developers will have to fulfill certain guarantees before the system goes into production.

Steps 1-3 Building the challenge nonce. The goal of these steps is to create the challenge the user will have to sign with their private key. There are a couple of requirements the developers have to provide:

1. Generated challenge nonce must be between 32 and 96 bytes (inclusive) in length [60];
2. "It must be guaranteed that the authentication token is received from the same browser to which the corresponding challenge nonce was issued" [59]. The framework creators recommend attaching it to the user session.
3. "Cache must be used for protection against replay attacks by guaranteeing that each authentication token can be used exactly once" [59]. The developers must create temporary storage for challenge nonces or any other means to revoke already used nonces.
4. "Cookie-based authentication must be protected against cross-site request forgery (CSRF) attacks and extra measures must be taken to secure the cookies by serving them only over HTTPS and setting the HttpOnly, Secure and SameSite attributes" [59].

In the implementation example, these measures were addressed:

1. A 64 byte cryptographically secure randomly generated nonce is created (see listing 1).
2. Challenge nonce is set in the user's session, which adversaries cannot tamper.
3. The generated nonce is stored into local memory cache for later use.
4. A input field is rendered on the page with a unique CSRF validation token, which prevents cross-site request forgery attacks (see listing 2).

```
private TimeSpan ChallengeLifetime { get; } = TimeSpan.FromMinutes(5)
    ;

private readonly IMemoryCache _cache; // Injected

[HttpGet("challenge")]
public IActionResult GetChallenge()
{
    var nonce = RandomNumberGenerator.GetBytes(64);

    _cache.Set(Convert.ToBase64String(nonce), true, ChallengeLifetime
        );
    HttpContext.Session.Set("eid.challenge", nonce);

    return Ok(new { nonce });
}
```

Listing 1. Web eID Challenge Endpoint

```
@inject Microsoft.AspNetCore.Antiforgery.IAntiforgery _csrf
@{ var csrfToken = _csrf.GetAndStoreTokens(HttpContext); }

<!   Button used to sign in   >
<a role="button" class="btn btn secondary" id="webeid auth button">
    Web eID</a>

<input id="csrfToken" type="hidden" value="@csrfToken.RequestToken"/>

<script>
    ...

    const authTokenResponse = await fetch("/signin id/login", {
        method: "POST",
        headers: {
            "Content Type": "application/json",
            "RequestVerificationToken": document.getElementById("
                csrfToken").value
        },
        body: JSON.stringify(...)
    });

    ...
</script>
```

Listing 2. Web eID UI excerpt

Steps 13-17 After the user signs the nonce challenge and sends their certificate, the server must verify its authenticity. There are a couple of steps developers must take before allowing the user to sign in.

1. Verify the CSRF token from earlier steps [59].
2. Verify the challenge nonce came from the original user and has not expired, was not consumed.
3. Verify the certificate validity and check if nonce was signed by the associated private key (see below).
4. Issue an authentication token with the fields from the certificate's subject.

In the implementation example, these measures were addressed:

1. The back end endpoint for login is decorated with ValidateAntiForgeryToken Attribute. This attribute instructs the ASP.NET API to ignore requests not containing a CSRF token [61]. A JavaScript application can then access the protected endpoints by providing RequestVerificationToken header (see listing 2).
2. The application tries to extract the challenge nonce from the browsing session. The process would succeed if the session cookie were not modified. After the extraction, the application checks the nonce cache to verify if the challenge is still active. Cache hit means the nonce has not expired, and a previous request has not consumed it already. Remove the challenge nonce from all stores.
3. The API calls a standalone validation service to verify the nonce and certificate (see below).
4. Application populates the ASP.NET identity management system with the fields from the certificate: serial number, given name, surname, country. An identity session cookie is sent to the client.

```
[HttpPost("login")]
[ValidateAntiForgeryToken]
public async Task<IActionResult> Login([FromBody]
    WebIdAuthTokenResponse token)
{
    // Obtain the challenge from session
    if (!HttpContext.Session.TryGetValue(ChallengeNonceKey, out var
        nonce) && nonce == null)
        return Unauthorized();

    // Check if token was not used before or expired
    var challenge = Convert.ToBase64String(nonce);
    if (!_cache.TryGetValue(challenge, out _))
        return Unauthorized();
```

```
        _cache.Remove(challenge);
        HttpContext.Session.Remove(ChallengeNonceKey);

        // Validate the certificate and signed challenge
        var validationResult = await _webEidValidationService.GetResult(
            new WebEidValidationRequest(token, nonce));
        if (!validationResult.Success)
             return Forbid();

        // Certificate is valid. Sign in the user

        await HttpContext.SignInAsync(BuildUser(new X509Certificate2(
            Convert.FromBase64String(token.UnverifiedCertificate)).Subject
            ));

        return Ok();
}
```

Listing 3. Web eID Login Endpoint

Certificate and nonce verification This step is the most complicated in the entire validation process. To prevent any issues with incorrect implementation, the framework maintainers recommend using their library for validation [59]. Libraries can come with security vulnerabilities, and developers rarely update the used version; however, it is still more favorable to creating vulnerabilities from misconfiguration [62].

The eu.webeid.security Java package performs most of the certificate validation (expiry, purpose, policy, OCSP nonce) [59]. Still, the developer will have to configure revocation and host validation. Configuration is handled by providing a set of trusted CA certificates for trust chain verification and the hostname for challenge nonces.

This library does favor EE cards a lot more, even having hardcoded some Mobile ID policies. Not sure if it is worth mentioning.

Because the library performs most of the heavy lifting, the developer can easily configure the validation service (see listing 4).

```
public class AuthTokenValidatorService {

    @Bean
    public AuthTokenValidator validator() {
        try {
            return new AuthTokenValidatorBuilder()
                .withSiteOrigin(URI.create(System.getenv("ORIGIN_URL")))
                .withTrustedCertificateAuthorities(
                    loadTrustedCACertificatesFromCerFiles())
                .build();
        } catch (JceException e) {
            throw new RuntimeException("Error building the Web eID auth
                token validator.", e);
```

```
    }
  }

  private X509Certificate[] loadTrustedCACertificatesFromCerFiles() {
    List<X509Certificate> caCertificates = new ArrayList<>();

    try {
      CertificateFactory certFactory = CertificateFactory.getInstance
          ("X.509");

      File[] files = new File("/certs").listFiles((f, n)  > n.
          endsWith(".cer"));
      if (files != null) {
        for (File file : files) {
          try (InputStream stream = new FileInputStream(file)) {
            X509Certificate caCertificate = (X509Certificate)
                certFactory.generateCertificate(stream);
            caCertificates.add(caCertificate);
          }
        }
      }
    } catch (CertificateException | IOException e) {
      throw new RuntimeException("Error initializing trusted CA
          certificates.", e);
    }

    return caCertificates.toArray(new X509Certificate[0]);
  }
}
```

Listing 4. Web eID Login Endpoint

From the listing 4 we see that the developer needs to provide the origin URL in the form of an environment variable and to populate the folder /certs with trusted CA certificates.

Developers can obtain the origin URL by checking the window.origin of the page containing the sign-in button.

For the CA certificate set, the developers or maintainers can get an up-to-date list of trusted certificates at the EU Trust Services Dashboard [20]. The issue with this list is that it contains all trust certificates for various scopes. In our case, we should limit the search to the extent of QCert for ESig. In the case of Estonia and Lithuania, only three entities are certified to issue certificates for QSCD (see figure 3). It is in stark contrast to Spain's 31 [20]. It is possible to further narrow down to only certificate generation services for qualified certificates (CA/QC).

In the case of Estonia's single TSP, we can see that only 3 CA are currently operational (see figure 4). Unfortunately, there is no standardized way of narrowing down which

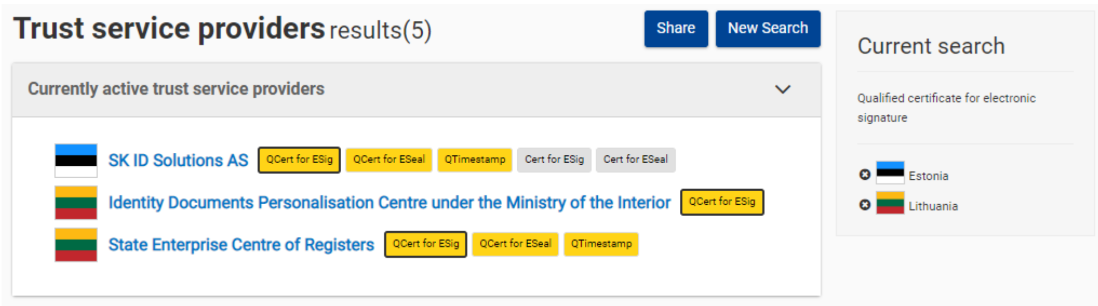

Figure 3. List of EU Trust service providers of Estonia and Lithuania capable of creating qualified certificates for e-signatures

certificates could be used for authentication any further.

An alternative way to obtain certificates would be to go to the government authority of each country responsible for the distribution of certificates. This action requires prior knowledge of who is responsible for issuing certificates and their purposes.

In Lithuania's case, it is the Ministry of the Interior [63] who issue two certificates (A and B) every couple of years. As of early 2022, four certificates are active, and all will be added to the trusted CA list.

In Estonia's case, SK ID Solutions manages the CA certificates [64]. Of the three certificates found on the EU Trust Services Dashboard, only two are relevant to us, the 2015 and 2018 ones, as the 2016 one has its purpose for use in Smart-ID, which the Web eID framework does not support.

The final list of certificates to support Lithuania and Estonia include four certificates from Lithuania's Ministry of the Interior and two certificates issued by SK ID Solutions for a total of six. It is essential to keep track of these certificates as each one of them acts as a point of compromise and must be monitored in the event they are revoked for security [65] or other issues.

Exposing the service With the certificate validation service configured, it is now required to link it to the Web API. If the company orients around using microservices, this service can be just that. All that the validation service requires is to expose an endpoint that accepts a nonce and a token from the javascript library and returns a validation result.

Companies must take proper measures to protect such service from adversaries as it acts as a fundamental trust anchor. Developers should take steps outlined in assume breach .

citation missing

Related research about legal persons documents?

High-level overview of the system

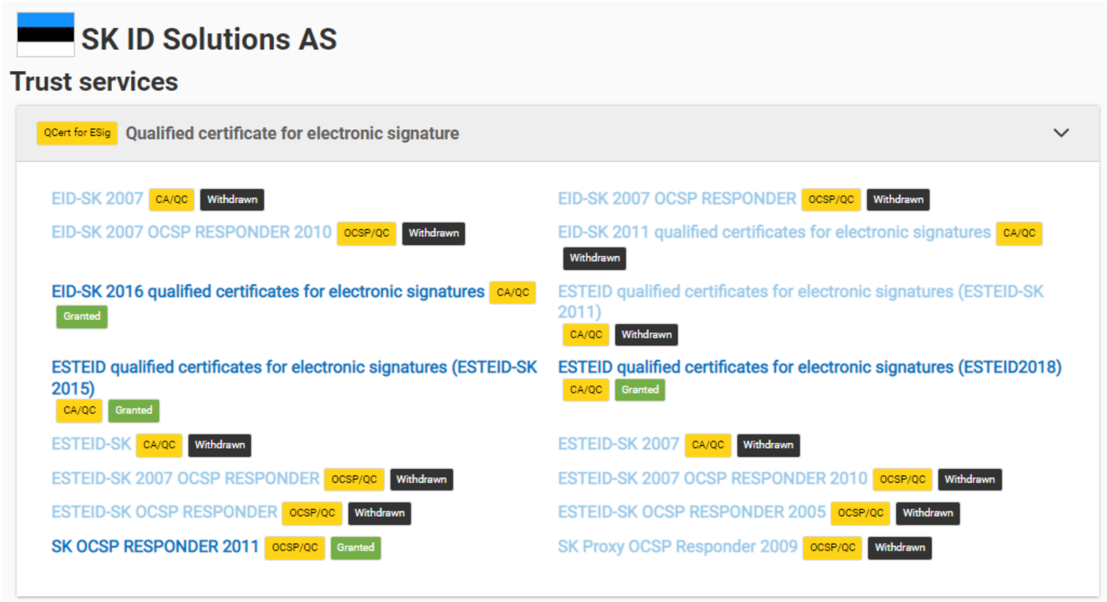

Figure 4. List of certificates issued to SK ID Solutions AS for the purposes of Qualified certificate for electronic signature

Points of compromise?

Complete alternative, using your own issued certificates?

5 Discussion

Talk about which of the 3 case studies would work best in a company in early 2022

Should notify how eeID and Web eID are really in their infancy and further research should repeat this study in a couple of years

References

[1] Adam Ozimek. The future of remote work. *Available at SSRN 3638597*, 2020.

[2] British Council. IELTS - how to register. https://www.ielts.org/for-test-takers/how-to-register, 2022. Online; accessed 26-Feb-2022.

[3] THE EUROPEAN PARLIAMENT and THE COUNCIL OF THE EUROPEAN UNION. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of the European Union*, L 257/73, 2014.

[4] Riigikogu. Identity documents act. 2021.

[5] Răzvan Dan. Cât plătesc oamenii pentru buletinul cu cip care a început să fie eliberat deja populației. https://stirileprotv.ro/stiri/actualitate/buletinul-cu-cip-eliberat-deja-in-cluj-napoca-oamenii-platesc-70-de-lei-pentru- html, 2021. Online; accessed 27-Feb-2022.

[6] European Comission. Digital economy and society index (desi) 2021. 2021.

[7] Jesus Carretero, Guillermo Izquierdo-Moreno, Mario Vasile-Cabezas, and Javier Garcia-Blas. Federated identity architecture of the european eid system. *IEEE Access*, 6:75302–75326, 2018.

[8] Informacinės visuomenės plėtros komitetas. E-government gateway. https://www.epaslaugos.lt/portal/nlogin, 2022. Online; accessed 27-Feb-2022.

[9] Estonian Information System Authority. As of 1 march, it will no longer be possible to access certain public e-services via a bank link. https://www.ria.ee/en/news/1-march-it-will-no-longer-be-possible-access-certain-public-e-services-bank-lin html, 2021. Online; accessed 27-Feb-2022.

[10] European Comission. Electronic identification schemes notified pursuant to Article 9(1) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. *Official Journal of the European Union*, C 432/7, 2020.

[11] Applied CyberSecurity Group. Estonian e-services using eid. https://acs.cs.ut.ee/services_using_eid, 2021. Online; accessed 21-Nov-2021.

[12] Katri Kerem. *Internet banking in Estonia*, volume 7. PRAXIS, 2003.

[13] AS SEB Pank. Bank link and authentication service. https://www.seb.ee/en/bank-link, 2021. Online; accessed 21-Nov-2021.

[14] Arnis Paršsovs. Security analysis of internet bank authentication protocols and their implementations. Master's thesis, Tallinn University of Technology, 2012.

[15] Estonian Information System Authority. Home - id.ee. https://www.id.ee/en/, 2021. Online; accessed 20-Nov-2021.

[16] Statistics Estonia. Population figure. https://www.stat.ee/en/avasta-statistikat/valdkonnad/rahvastik/population-figure, 2021. Online; accessed 20-Nov-2021.

[17] Stefan Santesson, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Dr. Carlisle Adams. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 6960, June 2013.

[18] Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, August 2018.

[19] Estonian Information System Authority. Web eid. https://www.id.ee/en/article/web-eid/, 2022. Online; accessed 28-Feb-2022.

[20] European Commission. Trust service providers. https://esignature.ec.europa.eu/efda/tl-browser/, 2022. Online; accessed 28-Feb-2022.

[21] SK ID Solutions. History - 2007. https://www.skidsolutions.eu/en/about/history/year-2007/, 2007. Online; accessed 21-Nov-2021.

[22] SK ID Solutions. Price list of Mobile-ID service. https://www.skidsolutions.eu/en/services/pricelist/mobile-id-service, 2021. Online; accessed 21-Nov-2021.

[23] Telia. Mobiil-ID. https://www.telia.ee/era/lisateenused/mobiil-id/, 2022. Online; accessed 28-Feb-2022.

[24] SK ID Solutions. History - 2017. https://www.skidsolutions.eu/en/about/history/year-2017/, 2017. Online; accessed 21-Nov-2021.

[25] SK ID Solutions. Smart-ID documentation. https://github.com/SK-EID/smart-id-documentation, 2021. Online; accessed 10-Feb-2022.

[26] Sylvie Lacroix, Olivier Delos, Evgenia Nikolouzou (ENISA), and Slawomir Gorniak (ENISA). Assessment of Standards related to eIDAS. Technical report, European Union Agency For Network and Information Security, 2018.

[27] SK ID Solutions. Digital signatures with Smart-ID. https://www.smart-id.com/e-service-providers/smart-id-as-a-qscd/, 2018. Online; accessed 28-Feb-2022.

[28] SK ID Solutions. Price list of Smart-ID service. https://www.skidsolutions.eu/en/services/pricelist/smart-id/, 2021. Online; accessed 21-Nov-2021.

[29] Estonian Information System Authority. The information system authority's authentication service TARA. https://www.ria.ee/en/state-information-system/eid/partners.html, 2022. Online; accessed 27-Feb-2022.

[30] Estonian Information System Authority. TARA business description. https://e-gov.github.io/TARA-Doku/Arikirjeldus, 2021. Online; accessed 21-Nov-2021.

[31] Estonian Information System Authority. TARA technical specification. https://e-gov.github.io/TARA-Doku/TechnicalSpecification, 2021. Online; accessed 21-Nov-2021.

[32] Natsuhiko Sakimura, John Bradley, Mike Jones, Breno De Medeiros, and Chuck Mortimore. Openid connect core 1.0. *The OpenID Foundation*, 2014.

[33] Estonian Internet Foundation. eeid service. https://www.internet.ee/eeid-service, 2021. Online; accessed 28-Feb-2022.

[34] Estonian Internet Foundation. Subscription agreement and terms of use of the estonian internet foundation electronic identification service. https://meedia.internet.ee/files/Pricing_eeID.pdf, 2021. Online; accessed 28-Feb-2022.

[35] Estonian Ministry of Education and Research. HarID. https://harid.ee/et/users/sign_in, 2022. Online; accessed 28-Feb-2022.

[36] Dokobit. Electronic signature API solutions. https://www.dokobit.com/solutions, 2022. Online; accessed 28-Feb-2022.

[37] Dokobit. Dokobit authentication solutions pricing. https://www.dokobit.com/docs/pricing/Dokobit-authentication-solutions-pricing.pdf, 2022. Online; accessed 28-Feb-2022.

[38] Estonian Information System Authority. Id-card documentation. https://www.id.ee/en/article/id-card-documentation/, 2021. Online; accessed 01-Mar-2022.

[39] Jesus Carretero, Guillermo Izquierdo-Moreno, Mario Vasile-Cabezas, and Javier Garcia-Blas. Federated identity architecture of the european eid system. *IEEE Access*, 6:75302–75326, 2018.

[40] L. O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040, 2003.

[41] Yuan Cao and Lin Yang. A survey of identity management technology. In *2010 IEEE International Conference on Information Theory and Information Security*, pages 287–293, 2010.

[42] Scott Cantor, Internet2 John Kemp, Nokia Rob Philpott, and E Maler. Assertions and protocols for the oasis security assertion markup language. *OASIS Standard (March 2005)*, pages 1–86, 2005.

[43] Dick Hardt. The OAuth 2.0 Authorization Framework. RFC 6749, October 2012.

[44] Siddhartha Arora. National e-id card schemes: A european overview. *Information Security Technical Report*, 13(2):46–53, 2008.

[45] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In *Conference on the theory and application of cryptographic techniques*, pages 186–194. Springer, 1986.

[46] Lietuvos Respublikos vidaus reikalų ministerija. Sertifikatai įrašyti atk. `https://www.eid.lt/lt/apie-tapatybes-kortele/sertifikatai-ir-ju-valdymas`, 2020. Online; accessed 01-Mar-2022.

[47] The eIDAS Cooperation Network. Opinion no. 3/2021 of the cooperation network on the on the french eid scheme ("franceconnect+/the digital identity la poste"). `https://ec.europa.eu/digital-building-blocks/wikis/pages/viewpage.action?pageId=439222578`, 2021. Online; accessed 01-Mar-2022.

[48] Bernd Zwattendorfer and Daniel Slamanig. The austrian eid ecosystem in the public cloud: How to obtain privacy while preserving practicality. *Journal of Information Security and Applications*, 27-28:35–53, 2016. Special Issues on Security and Privacy in Cloud Computing.

[49] Herbert Leitold. eid and egovernment in austria. Graz University of Technology `https://online.tugraz.at/tug_online/voe_main2.getvolltext?pCurrPk=16600`, 2006. Online; accessed 01-Mar-2022.

[50] Bernd Zwattendorfer and Arne Tauber. Secure cross-cloud single sign-on (sso) using eids. In *2012 International Conference for Internet Technology and Secured Transactions*, pages 150–155, 2012.

[51] Ribeiro C., Leitold H., Esposito S., and Mitzam D. Stork: a real, heterogeneous, large-scale eid management system. *International Journal of Information Security*, 17(5):569 – 585, 2018.

[52] Elvīra Krēķe. Electronic identity verification: personal data protection challenges and risks. Master's thesis, Riga Graduate School of Law, 2020.

[53] Vicente Guerola-Navarro, Raúl Francisco Oltra Badenes, Hermenegildo Gil Gómez, and Doina Stratu-Strelet. Eid@ cloud: integration of electronic identification in european platforms in the cloud in accordance with the eidas regulation. *3C Business, Researchóand critical thinking*, 8(3):64–87, 2019.

[54] Martín J.C., Aranda N.I., Carreras R.C., Pasic A., Baún J.C.P., Ksystra K., Triantafyllou N., Papadakis H., Torroglosa E., and Ortiz J. *LEPS - Leveraging eID in the private sector*. 2019.

[55] Estonian Information System Authority. Web eid: electronic identity cards on the web. `https://github.com/web-eid/web-eid-system-architecture-doc`, 2022. Online; accessed 05-Mar-2022.

[56] Arnis Paršovs. On the format of the authentication proof used by ria's web eid solution. Technical report, University of Tartu, 2021.

[57] Estonian Information System Authority. web-eid.js. `https://github.com/web-eid/web-eid.js`, 2021. Online; accessed 06-Mar-2022.

[58] Estonian Information System Authority. web-eid-app. `https://github.com/web-eid/web-eid-app`, 2021. Online; accessed 05-Mar-2022.

[59] Estonian Information System Authority. web-eid-app - authenticate.cpp. `https://github.com/web-eid/web-eid-authtoken-validation-java`, 2022. Online; accessed 05-Mar-2022.

[60] Estonian Information System Authority. web-eid-app. `https://github.com/web-eid/web-eid-app/blob/8bedc0c57698c729012a0c16f590ce0907d27d20/src/controller/command-handlers/authenticate.cpp#L103`, 2021. Online; accessed 05-Mar-2022.

[61] Fiyaz Hasan, Rick Anderson, and Steve Smith. Prevent cross-site request forgery (xsrf/csrf) attacks in asp.net core. `https://docs.microsoft.com/en-us/aspnet/core/security/anti-request-forgery`, 2022. Online; accessed 05-Mar-2022.

[62] Ying Wang, Bihuan Chen, Kaifeng Huang, Bowen Shi, Congying Xu, Xin Peng, Yijian Wu, and Yang Liu. An empirical study of usages, updates and risks of third-party libraries in java projects. In *2020 IEEE International Conference on Software Maintenance and Evolution (ICSME)*, pages 35–45, 2020.

[63] Asmens dokumentų išrašymo centras. Asmens tapatybės kortelė ir elektroninis parašas. `https://www.nsc.vrm.lt/downloads.htm`, 2021. Online; accessed 05-Mar-2022.

[64] SK ID Solutions. Certificates. `https://www.skidsolutions.eu/en/repository/certs/`, 2022. Online; accessed 05-Mar-2022.

[65] Estonian Information System Authority. Roca vulnerability and eid: Lessons learned. Technical report, Estonian Information System Authority, 2018.

Appendix

I. Glossary

II. Licence

Non-exclusive licence to reproduce thesis and make thesis public

I, **Gediminas Milašius**,
(author's name)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

   reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   Exploring integration complexity of different multi-national eID authentication solutions in the EU private sector,
   (title of thesis)

   supervised by Axel Rose and May Flower.
   (supervisor's name)

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Gediminas Milašius
11.06.2022