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 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.

Cite

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.

2.1.1 Impact

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.

2.2.1 eeID

Estonia's eIDAS node access is handled by TARA [8].

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 [9]. 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 [10] 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 [11]. 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 [11].

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. Without a deep understanding of cultural and social intricacies,

By having this access This process is useful, as one service provider would be able to open up the entirety of EU market. The main issue with using eIDAS nodes as an authentication method, is the restricted access to it. In email correspondence I learnt that in Estonia, access to this service is limited to public sector only, with plans to open it up to private sector in 2022.

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-el.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] 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.

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

[10] 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-link.html, 2021. Online; accessed 27-Feb-2022.

[11] 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.

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