TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Getter Õunapuu

# DIFFERENCES IN CROSS BORDER COMPLIANCE FOR PROVIDING TRUST SERVICES FOR NATIONAL ELECTRONIC IDENTITY MEANS

Master's thesis
Program HAJM08/21, specialization in Law and Technology

Supervisor: Thomas Hoffmann, Dr. jur., LL. M.

Tallinn 2024

I hereby declare that I have compiled the thesis independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously presented for grading.

The document length is 17,070 words from the introduction to the end of the conclusion.

Getter Õunapuu, 01.05.2024
(signature, date)
Student code: 220746HAJM
Student e-mail address: getter.ounapuu@gmail.com

Supervisor: Thomas Hoffmann, Dr. jur., LL. M:
The paper conforms to requirements in force

……..
(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

……
(name, signature, date)

# TABLE OF CONTENTS

# ABSTRACT

Today, qualified electronic signatures have the same legal effect as handwritten signatures across the EU according to the eIDAS Regulation. Only a Qualified Trust Service Provider (QTSP) can issue qualified certificates for qualified electronic signatures. While the requirements are heavily regulated, Member States providing their citizens and residents with eIDs, which also allow the providing of qualified electronic signatures, have addressed this requirement differently by either procuring a private Qualified Trust Service Provider (QTSP) to provide the services, or they have set up a government controlled and operated QTSP, and varying degrees in between. The current work, aims to determine the differences of operating a government QTSP vs a private QTSP in the context of Estonian practice by comparing the similarities and differences in fulfilling requirements and to provide usable recommendations to fill gaps in existing legislation.

Through empirical research and qualitative analysis, followed by a theoretical analysis of academic literature, three different QTSP models from Estonia, Latvia, and Belgium are identified and compared. The varying models are: using a private QTSP to provide services for the government, government owned and controlled QTSP, and hybrid where the government owns and controls the QTSP but a private company provides day-to-day operations. Based on the work, the Estonian government is recommended to look further into switching to a hybrid QTSP model and concrete proposals are made to amend local and EU legislation in light of shortcomings in relation to the eIDAS Regulation and upcoming changes from a new version of the Regulation.

Keywords: Qualified Trust Service Provider, national eID, eIDAS, government vs. private

# INTRODUCTION

The term e-government can be explained as using technology to increase efficiency in government services and to deliver government services and/or information to the public and stakeholders.[1] On the other hand, e-governance is the use of information and communications technology (ICT) in a manner that results in "material change in structures, stakeholders, data, processes or norms" of governance, aims to engage citizens, and does not merely replace already existing services of traditional government with electronic solutions.[2] Estonia is often referred to as an e-government and e-governance success story, with electronic identity (eID) solutions that are widely adopted by Estonian citizens, residents in Estonia, as well as by e-residents.[3] Estonian eIDs in the form of ID-cards can be traced back to 2002 and already then the eID documents could be used for authentication and electronic signatures, but they were only just starting to gain use among the citizens.[4] Twenty years later, the Estonian eID means are viewed by users as beneficial with multiple success factors, including being able to access thousands of online services within Estonia, and for the provided ability to give qualified electronic signatures.[5] Today, qualified electronic signatures have the same legal effect as handwritten signatures across the EU according to EU Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation), and the use of digital signatures in Estonia is seen as "one of the most successful implementations of an electronic signature scheme in Europe".[6] While the eIDAS Regulation, related implementing acts, and European standards all set strict requirements that must be adhered to when it comes to qualified electronic signatures, there is some room for Member States to choose how they fulfil those requirements. For example, for a

[1] Umbach, G. & Tkalec, I. (2022). Evaluating e-governance through e-government: Practices and challenges of assessing the digitalisation of public governmental services. *Evaluation and Program Planning*, 93, Article102118. https://doi.org/10.1016/j.evalprogplan.2022.102118

[2] *Ibid*; Bannister, F. & Connolly, R. (2012). Defining e-Governance. *e-Service Journal*, 8(2), p. 20-21. https://doi.org/10.2979/eservicej.8.2.3; Meijer, A. (2015). E-governance innovation: Barriers and strategies. *Government Information Quarterly*, 32(2), p. 198-206. https://doi.org/10.1016/j.giq.2015.01.001.

[3] Hardy, A. (2023). Digital innovation and shelter theory: exploring Estonia's e-Residency, Data Embassy, and crossborder e-governance initiatives. *Journal of Baltic Studies*, p. 1-18. https://doi.org/10.1080/01629778.2023.2288118. The author explains that the Estonian e-residency program is an example of e-governance, as the e-Resident's digital ID does not replace a service that previously existed without the use of ICT, but instead is a material change in processes and stakeholders all together. E-residency digital identity cards reach a group of people that may not have been reached in the physical world face-to-face and allows them access to different public and private services.

[4] Martens, T. (2010). Electronic identity management in Estonia between market and state governance. *IDIS*, 3, 213-233, p. 214, 216. https://doi.org/10.1007/s12394-010-0044-0.

[5] Pöhn, D., Grabatin, M., & Hommel W. (2021). eID and Self-Sovereign Identity Usage: An Overview. *Electronics*, 10(22), Article2811. https://doi.org/10.3390/electronics10222811.

[6] OJ L 257, 28.8.2014; Mets, T. & Parsovs, A. (2019). Time of Signing the Estonian Digital Signature Scheme. *Digital Evidence and Electronic Signature Law Review*, 16, 40-50, p. 40.

signature to be a qualified electronic signature it must be created by a qualified electronic signature creation device, which meets the criteria of Annex 2 to the eIDAS Regulation, but the device can either be a physical qualified electronic signature creation device (QSCD) or a remote qualified electronic signature creation device (rQSCD).[7] Another requirement for a qualified electronic signature, as defined by article 3 of the eIDAS Regulation, is that the signature is based on a qualified certificate for electronic signatures and a qualified certificate can only be provided by a qualified trust service provider (QTSP). While the strict requirements for QTSPs are the same for all QTSPs, the eIDAS Regulation does not define whether a QTSP ought to be a private company, government owned and operated, or a hybrid of the two, as long as the QTSP is recognized by the Member State. Since the implementation of eIDAS, the Estonian government has used private companies to provide qualified trust services for national eID solutions, which enable users to authenticate and provide qualified electronic signatures. However, some EU Member States have chosen to maintain state control over QTSPs by not outsourcing these services to private entities.[8] In Latvia for example, private QTSPs from other countries can provide limited services within Latvia, but qualified trust services for national eID means which allow giving qualified electronic signatures and the highest level of access with authentication are currently only provided by a state owned and controlled company.[9] Kingdom of Belgium is further an example of a country which has chosen a hybrid approach by creating a government owned and controlled QTSP (called the Kingdom of Belgium – Federal Government QTSP), but private company services are procured to setup the QTSP and to conduct the day-to-day operations.[10]

While the eIDAS Regulation was published in the Official Journal of the European Union nearly ten years ago, different interpretations of the requirements result in issues in interoperability and lack of harmonized fulfilment of the requirements.[11] For instance, according to Article 25 of

[7] See Article 3 of OJ L 257, 28.8.2014, *ibid*; the author explains: an example of a QSCD can be the chip embedded inside a card like an ID-card or for a rQSCD a cell phone application that is downloaded. In case of rQSCD, the signature is formed on behalf of the person giving their signature, but in case of QSCD the person signing is usually performing all the steps of providing the signature with the help of an application.

[8] Cooperation Network, Kirova, M. (2023). *Overview of pre-notified and notified eID schemes under eIDAS*. Retrieved October 14, 2023 from https://ec.europa.eu/digital-building-blocks/wikis/pages/viewpage.action?spaceKey=EIDCOMMUNITY&title=Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS; European Commission. (2023). *EU/EEA Trusted List Browser*. Retrieved September 23, 2023, from https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home.

[9] Compliance Officer of the Latvian State Radio and Television Centre. Author's Microsoft Teams videocall interview. Notes of the interviewer. March 12, 2024;

[10] European Commission (2023), *EU/EAA Trusted List Browser*, *supra nota* 8; Kingdom of Belgium - Federal Government. (2023). *Policies and Practice Statements*. Retrieved October 14, 2023 from https://repository.eidpki.belgium.be/#/policies, see p. 8 of the Belgium Root Certificate Policy v.1.2.

[11] Determann, L. (2021). Electronic Form Over Substance: eSignature Laws Need Upgrades. *Hastings Law Journal*, 72(5), 1385-1452, p. 1407; Entschew, E., et al. (2022). A New eIDAS Beginning for QWACs. *Datenschutz Datensich*,

eIDAS, qualified electronic signatures have the same legal effect as handwritten signatures and Member States shall recognized the qualified electronic signatures given in other Member States. However, this seldom works so seamlessly due to differing opinions of how to technically adhere to the requirements and having different technical means to validate the signature, which results in rejecting signatures from other Member States.[12] With the upcoming revision of eIDAS, commonly referred to as eIDAS 2.0, the requirements and responsibilities of Member States, non-qualified trust services, and QTSPs will increase, but the level of requirements for harmonization is not yet known as the first implementing acts are expected at the end of 2024.[13]

Therefore, the aim of the research is to determine the differences of operating a government QTSP versus a private QTSP in the context of Estonian practice by comparing the similarities and differences in fulfilling requirements and to provide usable recommendations to fill gaps in existing legislation. Three different QTSP models are compared and the comparison can be used by the Estonian government (and by other EU Member States) as a starting point in determining whether they may wish to continue using the existing model of QTSP for national eID means or whether they may wish to switch to a different model of QTSP with less or more control over operations, either in full or in part, going forward in providing national eID means. The first opportunity for such consideration is already now, as all Member States will be required to provide EU Digital Identity Wallets (EUDIW) by as early as the end of 2026 or the beginning of 2027 and that EUDIW will have to include the ability to provide qualified electronic signatures.[14]

The research method used to achieve the aim of the thesis, is primarily empirical research and qualitative analysis, followed by a theoretical analysis of academic literature to evaluate the differences determined in the first phase. The research begins by comparing the EU trusted list, published on the European Commission's eIDAS Dashboard, of notified QTSPs who provide qualified certificates for electronic signatures and by comparing it to the EU Cooperation Network's notified eID schemes which are notified to a Level of Assurance (LoA) high. Then a list is compiled of countries which have notified an eID scheme to a LoA high and whose eID means can also be used to provide qualified electronic signatures. From there on, an evaluation of

46, 217-224, p. 218. https://doi.org/10.1007/s11623-022-1591-x; Kutylowski, M. & Blaśkiewicz, P. (2023). Advanced Electronic Signatures and eIDAS – Analysis of the Concept. *Computer Standards & Interfaces*, 83, Article103644. https://doi.org/10.1016/j.csi.2022.103644;

[12] Determann, *Ibid*., p. 1407; Kutylowski, *Ibid*.

[13] European Parliament (2024). *European Digital Identity Framework*. Retrieved March 24, 2024, from https://www.europarl.europa.eu/doceo/document/TA-9-2024-02-29_EN.html.

[14] European Parliament (2024), *ibid*, article 5a and 5c (6).

whether the trust services provided for those eIDs is from a private company or a government owned and/or operated QTSP. Finally, the list is narrowed to three countries to include three different models of QTSPs and based on the availability of trust service documentation in English (with a final selection: Estonia, Latvia, and Belgium). Next, the service documentation is reviewed for all three QTSPs to determine similarities and differences in how the different models of QTSPs fulfil requirements from the eIDAS Regulation when providing eID means to the general public. For some aspects, the determined similarities and differences were further clarified through an expert interview. The models' differences are then discussed based on the theoretical analysis of academic literature. The thesis then provides concrete proposals for reform for which QTSP model to choose in Estonia, suggestions on fixing existing gaps in current legislation on either the local or EU level, discusses the limitations of this research, and makes recommendations for further research.

# 1. THE EIDAS REGULATION AND QUALIFIED TRUST SERVICE PROVIDERS

EU Regulation No 910/2014 on electronic identification, authentication, and trust services, or otherwise known as the eIDAS Regulation, was entered into force in 2014 and was applied in its entirety in July 2016, while still allowing some transitional measures into 2017.[15] The eIDAS Regulation aimed to do a couple of different things; it aimed to create a framework which would allow Europeans to easily access online services of other Member States, and to build an internal market in which all trust services have the same legal status and the same baseline requirements for security.[16] One of the "most significant improvements" that came from the eIDAS Regulation, are qualified electronic signatures, which are legally equivalent to handwritten signatures, but can be given remotely through the services provided by QTSPs.[17] These QTSPs must all adhere to the same requirements set by the eIDAS Regulation, by associated implementing acts, and by EU standards for qualified electronic signatures to be legally accepted as handwritten signatures across the EU. In order to be in compliance with the eIDAS Regulation, these qualified electronic signatures, brought with them a requirement for public sector entities to also accept them in their services.[18] However, how Member States choose to set up their e-governance, e-government, national eID means and whether to implement and notify private and/or government controlled QTSPs is up to each individual Member State.[19] Some countries have chosen to notify eID means which allow both authentication and qualified electronic signatures; yet others have chosen to notify eID means which only allow authentication or allow authentication and advanced electronic signatures; and a few countries have not notified eIDs or are currently in the pre-notification phase.[20] With the upcoming revision of the eIDAS Regulation, commonly referred to as eIDAS 2.0, all Member States will be required to notify at least one EU digital identity wallet (EUDIW) as part of their national electronic identification system and the EUDIW should also allow the

[15] OJ L 257, 28.8.2014, *supra nota* 6.
[16] European Commission. (2023). *eIDAS Regulation*. Retrieved October 14, 2023 from https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation; European Commission. (2017). *Joint Statement by Vice-President Ansip and Commissioner Gabriel welcoming the adoption of the Tallinn Declaration on e-government*. Retrieved October 14, 2023 from https://ec.europa.eu/commission/presscorner/detail/it/STATEMENT_17_3742.
[17] Hölbl, M., et al. (2023). eIDAS Interoperability and Cross-Border Compliance Issues. *Mathematics*, 11(2), Article430. https://doi.org/10.3390/math11020430.
[18] Pelikánová, R. M., et al. (2019). Qualified electronic signature – EIDAS striking Czech public sector bodies. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, 67(6), 1551-1560, p. 1551-1552. https://doi.org/10.11118/actaun201967061551
[19] Author explains: eIDAS article 7 covers options for eID schemes choices, but beyond that eIDAS does not define if a QTSP ought to be government owned/operated or private sector owned/operated.
[20] Cooperation Network, *supra nota* 8.

creation of qualified electronic signatures.[21] Therefore, all Member States will have to consider which QTSP model they will use, when notifying at least one EUDIW.

## 1.1. Requirements in the eIDAS Regulation now and eIDAS 2.0

When it comes to requirements pertaining to QTSPs in the current eIDAS Regulation, the following are selected provisions from the current eIDAS Regulation, which primarily pertain to QTSPs issuing qualified certificates for electronic signatures[22]:

| eIDAS Article | related portion |
|---|---|
| Article 1 – Subject matter | "(b) lays down rules for trust services, in particular for electronic transactions" |
| Article 2 – Scope | 1. "This Regulation applies" …. "and to trust service providers that are established in the Union." |
| Article 3 – Definitions | (15) "'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;"<br>"(16) 'trust service' means an electronic service normally provided for remuneration which consists of:<br>(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or"<br>"(c) the preservation of electronic signatures, seals or certificates related to those services;"<br>"(17) 'qualified trust service' means a trust service that meets the applicable requirements laid down in this Regulation;"<br>"(20) 'qualified trust service provider' means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;" |
| Article 13 – Liability and | Paraphrased: trust service providers are liable for damage caused due to not complying with eIDAS, but are not liable for damages exceeding limitations |

[21] European Parliament (2024), *supra nota* 13, article 5a, recital (19).
[22] OJ L 257, 28.8.2014, *supra nota* 6.

| | |
|---|---|
| burden of proof | that they have duly informed their customers of, reference made to apply in accordance with national liability rules. |
| Article 15 – Accessibility | "Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities." |
| Article 16 – Penalties | "Member States shall lay down the rules on penalties applicable to infringements of this Regulation. The penalties provided for shall be effective, proportionate and dissuasive." |
| Article 17 – Supervisory Body | Summarized: Supervisory Body roles such as ex ante and ex post supervisory activities of trust service providers, granting or removing QTSP status, reporting security breaches, cooperating with other supervisory bodies, etc. |
| Article 19 – Security requirements for trust service providers | Summarized: non-qualified trust service providers and QTSPs "shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide", while continuously ensuring security is in accordance with degree of risk, reporting "any breaches of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein" within 24 hours of becoming aware of it, rules related to who and when to notify, etc. |
| Article 20 – Supervision of qualified trust service providers | Summarized: 1. Requirement for conformity assessment audits at least once every two years and submission of audit report to Supervisory Body, 2. Supervisory Body may additionally audit the QTSP at any time at QTSPs expense, 3. Supervisory Body may require remediation when QTSP fails to fulfil eIDAS requirements, Supervisory Body may withdraw qualified status in case of non-compliance, etc. |
| Article 21 – Initiation of a qualified trust service | Summarized: steps a QTSP is required to follow to first begin their operations, such as submitting an application to offer trust services to the Supervisory Body, submitting a conformity assessment report to the Supervisory Body, the timeline for the QTSP being added to the trusted listed, etc. |
| Article 22, 23 | Summarized: articles pertain to trusted lists and EU trust mark |
| Article 24 – Requirements for qualified | Summarized:<br>1. QTSP in accordance with national law, shall verify "the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued" either themselves "or by relying on a third party |

| | |
|---|---|
| trust service providers | in accordance with national law". Subsections outline the way the identification is required to be performed for subjects of certificates (i.e. specific rules for identifying in-person, remotely, and/or by other means).<br>2. outlines duties and requirements of the QTSP (e.g. such as notification requirements of changes or termination of the QTSP, requirements for staff employed, requirements for liability insurance or financial means, informing anyone wishing to use QTSP services of terms/conditions, requirements to use trustworthy systems, appropriate measures to protect data, record keeping requirements, termination plan requirements, data processing requirements, maintaining a certificate database, etc.)<br>3. and 4. certificate revocation related requirements. |
| Article 28 Qualified certificates for electronic signatures | Summarized: lists requirements for qualified certificates for electronic signatures, including the requirement for the certificates to meet the requirements in Annex I. |
| Article 29-31 | Summarized: requirements for QSCDs, certifying QSCDs, and publication of a list of QSCDs. |

Source: the table was prepared by the author.

eIDAS 2.0 aims to bridge some of the shortfalls of interoperability and bring about improvements to cross-border use of electronic identity means across the EU, bringing a long list of changes to the existing eIDAS Regulation and to trust services.[23] Perhaps the most discussed change will be the new requirement for Member States to provide EU Digital Identity Wallets (EUDIWs) to natural and legal persons, which enable authentication, providing of qualified electronic signatures, and the ability to house different electronic attestation of attributes.[24] Currently there is no requirement for Member States to provide natural persons with the means to create qualified electronic signatures (or to provide it for free), so this will be a significant new change that will

[23] Fernandez, R. (2022). Reflections on the European Digital Identity Project in Light of the Digital Covid Certificate and the Self-Sovereign Identity Movement. *Revista Catalana de Dret Public (Catalan Journal of Public Law)*, 65, 179-193, p. 184.

[24] European Parliament (2024), *supra nota* 13; Fábián, A. & Kollár, G. (2023). Trends in the Digitalisation of Public Administrations - In Light of EU Legislation and Domestic Developments. *Central European Public Administration Review (CEPAR)*, 21(2), p. 126-131. https://doi.org/10.17573/cepar.2023.2.06.

hopefully increase the ability to not only successfully provide qualified electronic signatures but to also validate them across the EU.[25]

Several of the changes with the new eIDAS Regulation are specific to QTSPs or relate to their services provided.[26] The first noticeable change that is specific to QTSPs and qualified electronic signatures is related to article 3 definitions, where rQSCDs are separately defined from QSCDs in point (23a) and a reference is made to QTSPs being the only ones who can manage rQSCDs, rest of the Articles pertaining to QSCDs are also updated to include rQSCDs.[27] Article 3 also defines the EUDIW in point 42 and makes reference to EUDIWs having to include the ability to provide qualified electronic signatures (further described in Article 5c) and thus this is a clear requirement where a QTSP will have to be involved with the EUDIWs.[28] Article 15 will be further specified for QTSPs as it will refer to EU Directive 2019/882 on the accessibility requirements for products and services.[29] Article 16 will bring about a significant change, as so far it was up to Member States to lay down the rules on penalties applicable to infringements against eIDAS, it will now bring the change that Member States shall ensure that those infringements by "qualified and non-qualified trust service providers be subject to administrative fines of a maximum of at least: (a) "EUR 5 000 000 where the trust service provider is a natural person; or (b) where the trust service provider is a legal person, EUR 5 000 000 or 1% of the total worldwide annual turnover of the undertaking to which the trust service provider belonged in the financial year preceding the year in which the infringement occurred, whichever is higher".[30] While 5 000 000 (or potentially higher for legal persons) is the maximum fine, this is potentially a significant change for Member States who so far were able to determine the range of penalties themselves. Articles 17 and 18 will be deleted with the new version of eIDAS and instead Article 20 is expanded to include more on mutual assistance and the Supervisory Body role.[31] More specifically, Article 20 is amended to include a reference to EU Directive 2022/2555 on measures for cybersecurity or otherwise known

[25] *Ibid*.
[26] European Parliament (2024), *supra nota* 13.
[27] *Ibid*. The author explains that many new trust services are defined in article 3, but the primary focus of this research is on the changes specific to QTSPs.
[28] *Ibid*. The author adds that the EUDIW full definition in the text adopted at the first reading is: "'European Digital Identity Wallet' means an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals". The author further explains that QTSPs will also be issuing qualified electronic attestation of attributes as defined by article 3 of the adopted text, but that goes beyond the scope of the topic of this thesis.
[29] *Ibid*; OJ L 151, 7.6.2019.
[30] European Parliament (2024), *supra nota* 13.
[31] *Ibid*.

as NIS2, and adds a requirement to QTSPs to notify the Supervisory Body of a planned conformity assessment audit at least one month ahead and should the Supervisory Body wish to observe, the QTSP shall allow them to be an observer during the conformity assessments.[32] Article 20 further adds more collaboration between different authorities, as the Supervisory Body will also have to withdraw the qualified status of either the QTSP or a specific service provided, if they receive information from the data protection supervisory authority or from the cybersecurity competent authority that the QTSP has failed to fulfil either data protection or cybersecurity requirements.[33] More references overall are made throughout the eIDAS 2.0 text in regard to eIDAS supervisory bodies and cybersecurity competent authorities working closely together.[34] A significant change to article 24 is in the new option to issue qualified certificates on the basis of a notified eID means to a LoA high or on the basis of the EUDIW, without having to combine the identity verification with other or additional methods.[35] The new article 24 also clarifies timelines for notification of changes or termination of activities but does not clarify the type of changes to be notified beyond the current text.[36] Article 24 also refers to the NIS2 Directive and requires different risk management related policies for the QTSP to have.[37] Article 24 further adds a new notification requirement where the QTSP has to notify the Supervisory Body and other relevant competent bodies or individuals of security breaches or disruptions in the provision of services, which have a significant impact on either the service or personal data within 24 hours of the incident occurring, as opposed to within 24 hours of becoming aware of the incident as is the case currently and will continue to be for non-qualified QTSPs.[38]

## 1.2. Implementing acts, guidance documents, and European standards

There are eight different implementing decisions/acts related to the current eIDAS Regulation and four of the eight are related to different requirements for trust services:

[32] *Ibid*; OJ L 333 27.12.2022.
[33] European Parliament (2024), *supra nota* 13.
[34] *Ibid.*
[35] *Ibid.* The author explains that other methods such as physically appearing or on the basis of a different method that has been approved by the Conformity Assessment Body still remain, but the current text in Article 24 of the eIDAS regulation permitted remote identification only if the person was physically present for the identification when they received the remote identification means. While implementing acts may provide more clarification, it appears that needing to see a person physically for every other issuance will no longer be a requirement.
[36] *Ibid.*
[37] *Ibid.*
[38] *Ibid.*

- Commission Implementing Regulation (EU) 2015/806: form requirements for the EU Trust Mark;
- Commission Implementing Decision (EU) 2015/1505: trusted list formats and specifications;
- Commission Implementing Decision (EU) 2015/1506: formats for advanced electronic signatures and seals that public sector bodies must recognize; and
- Commission Implementing Decision (EU)2016/650: security assessment standards for qualified signature and qualified seal devices[39]

As can already be interpreted from the titles of the Implementing Regulation and Implementing Decisions, the acts only specify very specific requirements for QTSPs. For instance, the implementing acts set requirements for the visual EU Trust Mark that is displayed on websites and the requirements for the trusted list formats and specifications, but adds very little in terms of operating QTSPs. Commission Implementing Decision (EU) 2016/650 does describe the security assessment for technical components such as the Qualified Signature Creation Device, but it does not set requirements or further specifications for general conformity assessments that all QTSPs have to go through on a regular basis.[40] These current implementing acts, add very little in terms of requirements on how to operate a QTSP, and therefore more clarity on how QTSPs can fulfil the eIDAS requirements come from standards. The following standards are European Standards (EN) and EN standards are intended to be used to meet a specific need for Europe or when either the European Commission or the European Free Trade Association requests a standard[41]:

- ETSI EN 319 411-2, titled: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 411-1, titled: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 401,[42] titled: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[39] Kirova, M., European Commission. (2016, June 28) eIDAS – Implementing Acts. Retrieved September 23, 2023, from https://ec.europa.eu/futurium/en/content/eidas-implementing-acts.html.
[40] The author explains that Article 20 of the eIDAS Regulation sets requirements for biannual conformity assessments.
[41] Ducato, R. (2023). Why Harmonised Standards Should Be Open. *IIC - International Review of Intellectual Property and Competition Law*, 54, 1173-1178, p. 1174. https://doi.org/10.1007/s40319-023-01372-1.
[42] The author explains that this standard is not always directly listed in the QTSP repository documentation, but ETSI EN 319 411-2 and ETSI EN 319 411-1 refer to adhering to ETSI EN 319 401 requirements throughout and therefore it is not possible to adhere to the first two without also adhering to ETSI EN 319 401.

While the eIDAS Regulation itself or the implementing decisions/regulations do not mention these particular standards, it is necessary to have some form of written requirements to assess conformity to, in order to fulfil requirements for security and to conduct conformity assessments as required by the eIDAS Regulation (articles: 19, 20, 24, 28).[43] Even though there are still some eIDAS Regulation related interoperability issues between Member States, interoperability and trust would likely not exist if it weren't for standards.[44] Standards also help to simplify some of the very complex requirements of the eIDAS Regulation.[45] Countries compared in this research all make a reference to adhering to the previously mentioned ETSI standards in their QTSP documentation in terms of trust service requirements. eIDAS Conformity Assessment Bodies also use standards for the assessments they conduct. For example, the eIDAS certificate on the Estonian QTSP's website mentions the following standards:

- ETSI EN 319 403-1 on the Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers, and
- EN ISO/IEC 17065 for Conformity assessment - Requirements for bodies certifying products, processes, and services.[46]

Despite the eIDAS Regulation not specifically referring to the ETSI EN 319 403 standard in relation to conformity assessments of QTSPs, an implementing act in Estonia does require the aforementioned standard, or its equivalent, to be adhered to for the conformity assessments of QTSPs in Estonia.[47] The QTSP requirements stemming from the aforementioned legislation, implementing acts, and standards can be further interpreted with the help of a number of different guidance documents that have been published by the European Union Agency for Cybersecurity (ENISA).[48] The next section discusses how different Member States have decided to interpret and

[43] Srinivas, J., et al. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92(2019), p. 179. https://doi.org/10.1016/j.future.2018.09.063.
[44] *Ibid*; European Commission. (2024). *European Standards*. Retrieved April 20, 2024, from https://single-market-economy.ec.europa.eu/single-market/european-standards_en.
[45] Srinivas, J., *supra nota* 43.
[46] See certificate under ESTEID section, valid until 2024-05-28, p. 10, from: SK ID Solutions. (2024). *Compliance Audit*. Retrieved March 31, 2024, from https://www.skidsolutions.eu/resources/compliance-audit/.
[47] Usaldusteenuse osutaja ja usaldusteenuse vastavushindamise kord RT I, 28.10.2016, 17.
[48] For example: European Union Agency for Cybersecurity. (2017). *Recommendations for QTSPs based on standards – Technical guidelines on trust services*. European Network and Information Security Agency: EU Publications. https://data.europa.eu/doi/10.2824/721561; European Union Agency for Cybersecurity, Gorniak, S., Nikolouzou, E., Agrafiotis, I. & Bugneac, D. (2021). *Security framework for qualified trust service providers – Technical guidelines of qualified trust service providers*. European Network and Information Security Agency: EU Publications. https://data.europa.eu/doi/10.2824/06258; European Union Agency for Cybersecurity. (2017). *Guidelines on*

implement different eIDAS Regulation requirements by reviewing the Qualified Trust Service Provider's service documentation and outlining the determined differences and similarities.

*initiation of qualified trust services – Technical guidelines on trust services*. European Network and Information Security Agency: EU Publications. https://data.europa.eu/doi/10.2824/238163; etc.

# 2. COMPARISON OF GOVERNMENT, HYBRID, AND PRIVATE QUALIFIED TRUST SERVICE PROVIDER MODELS

This research compares how roles and responsibilities are divided in different countries for different models of QTSPs. To select countries that are most like Estonia with their eID use, the selection was narrowed down to countries who have also successfully notified an eID means to a Level of Assurance (LoA) high[49] on the EU level and whose eID means can also be used to provide qualified electronic signatures or QES. Looking at notified eIDs, combined with reviewing various government and private company websites and their certificate policies (CPs) and/or certificate practice statements (CPS) for references to national eIDs. The list was then further reduced to different types of QTSP models, the timeline to complete this thesis, and based on the availability of information in English and from publicly accessible sources.

Search of the EU trusted list[50], was narrowed to only qualified trust service providers, further narrowed to include only QTSPs that issue qualified certificates for electronic signatures or QES. The search returned 257 results from 29 countries. Then countries which had not notified any eID schemes to LoA high as of the end of October 2023 were removed (for example: Finland, Hungary, Romania, etc.). Next, the countries who have notified to LoA substantial or low only were also removed. At this point, the list was down to 21 countries. Then, the countries who clearly use a private company for national eID means, or do not have a notified QTSP providing QES in their country at all, were removed (for example: Liechtenstein has not notified a QTSP providing QES, and countries such as Austria, Bulgaria, Norway, etc. use a private company for providing QES). Private QTSPs were removed, as the aim is to determine whether Estonia should switch away from a private model to something different. Countries which did notify an eID scheme with LoA high,

[49] The author, as a member of the EU Cooperation Network, explains that some of the Member States have notified a combination of high, substantial and/or low LoA schemes, meaning that at least in one process flow they have an eID that corresponds to LoA high. For example, a country may have an eID scheme that only corresponds to LoA high if the person is identified in person, but a person may also have the choice to apply or renew the eID remotely, in which case the eID scheme corresponds to a LoA substantial or low. There were also countries who have pre-notified to LoA high but these were also excluded as that is the intention of the country but until they have gone through the full peer-review process, there is no guarantee that other Member States or the EU Commission will also consider the scheme to a LoA high; Sharif, A., et al. (2022). The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes. *Applied Sciences*, 12(24), Article12679. https://doi.org/10.3390/app122412679.

[50] European Commission (2023), *EU/EAA Trusted List Browser*, *supra nota 8*.

but whose eID schemes do not mention the ability to use the eID for QES were also removed (for example: Netherlands has notified two eID means for authentication, but there is no mention of QSCD or QES, and Swedish eID schemes and eID websites only mention Advanced Electronic Signatures (AES), but not QES or QSCD). Finally, countries for which the main documentation such as the certificate policy and/or certificate practice statement were unavailable in English, or there was not enough publicly accessible information to compare the different QTSP models in place, were excluded (for example: Spain has a notified government QTSP but the National Police Corps documentation, such as the Certification Policy, is unavailable in English). Several countries have a government owned and/or operated QTSP for their Ministry of Defence, but the QTSP only issues qualified certificates for military personnel and civilian defence personnel, yet not for the public for their eID means. As Estonia uses the same government issued eIDs to natural persons, regardless if someone is in the military or works for a government agency in relation to national defence, those Ministry of Defence government QTSP models were left out of this comparison as well.

Finally, the list was narrowed down to three countries for comparison which met the criteria of providing national eIDs which are notified on the EU level to a level of assurance high, eIDs which are also QSCDs enabling the providing of qualified electronic signatures, countries for which the documentation was easily accessible in English, and which appeared to have a different model of QTSP from one another. The chosen countries were: Belgium, Estonia, and Latvia[51].

## 2.1. Government owned model: Latvia

The Latvian State Radio and Television Centre is a 100% state owned company and according to their website, referencing local legislation, it is prohibited to dispose of their shares.[52] According to the "eID Karte" Trust Service Policy, version 2.4, which is publicly available in the QTSP's repository, the requirements from ETSI EN 319 411-2 and ETSI EN 319 411-1 are adhered to for operating the Trust Services.[53] More specifically, the policy adheres to the QCP-n-qscd and NCP+

[51] The author explains further, that the number of countries was also narrowed to three, to remain within the time and length parameters of this thesis.

[52] Latvia State Radio and Television Center. (2023). *About Us*. Retrieved October 14, 2023, from https://www.lvrtc.lv/en/about-us/; Also confirmed by: Compliance Officer of the Latvian State Radio and Television Centre, *supra nota* 9.

[53] ePraksts. (2023). *Service policies*. Retrieved October 14, 2023, from https://www.eparaksts.lv/en/about_us/repository/Politikas.

policies as defined in the two ETSI standards.[54] The author for both the policy document such as the "eID Karte" Trust Service Policy, as well as for the more general Trust Service Provider Practice Statement is the LVRTC themselves, but all significant changes to the document have to be approved by the Board of the State joint stock company.[55] In terms of roles, according to the Trust Service Provider Practice Statement, the QTSP may delegate some duties to external legal persons in the role of Registration Authority and independent contractors/consultants may become trusted persons for very specific obligations as specified in a contract.[56] According to the "eID Karte" Trust Service Policy, the Office of Citizenship and Migration Affairs performs the Registration Authority role for the eID cards (including all the identification processes for certificate issuance/revocation/renewal) and uses the technical infrastructure administered by the Ministry of the Interior of the Republic of Latvia for provision of services.[57] As confirmed by the Compliance Officer of the LVRTC, no other Registration Authorities are used for the qualified trust services for the eID cards but they do also outsource to one courier service.[58] The eIDAS Supervisory Body role is held by the Supervisory Committee of Digital Security and it consists of "State Secretaries from the Defence, Transport, Justice, Interior and Environment Protection and Regional Development ministries, Director of the Data State Inspectorate, Director of the "Information Technology Security Incident Response Institution" at the Institute of Mathematics and Computer Science of the University of Latvia and Director of the committee's secretariat. The committee's sessions are closed from public."[59] To fulfil eIDAS Article 24 requirement to either have insurance or sufficient funds for liability of damages, the LVRTC holds approximately three different policies (one for identification services, one for signature services, and one for cases of employee fault).[60] The LVRTC is the only registered company in the QTSP list for Latvia and it is a state-owned company, but they have two distinctly separated parts, where one part provides government qualified trust services and the other part provides commercial or private trust services.[61] For governmental services, the LVRTC holds a state level agreement and receives

[54] *Ibid*. The author explains that ETSI EN 319 411-1 V1.4.1, p. 15 defines NCP+ as the Extended Normalized Certificate Policy „for use where a secure cryptographic device (signing or decrypting) is considered necessary" and ETSI EN 319 411-2 V2.5.1, p. 10 defines QCP-n-qscd as the „Policy for EU Qualified Certificate issued to a natural person where the private key and the related certificate reside on a QSCD".
[55] ePraksts. (2023). *Service policies, supra nota* 53, p. 6; ePraksts. (2023). *Service Practice Statement*. Retrieved October 14, 2023, from https://www.eparaksts.lv/en/about_us/repository/service_practice_statements.
[56] ePraksts. (2023). *Service Practice Statement, Ibid*, p. 55.
[57] ePraksts. (2023). *Service policies, supra nota* 53, p. 5.
[58] Compliance Officer of the Latvian State Radio and Television Centre, *supra nota* 9.
[59] Ministry of Defence Republic of Latvia. *Supervisory Committee of Digital* Security. Retrieved October 14, 2023, from https://www.mod.gov.lv/en/nozares-politika/cybersecurity/supervisory-committee-digital-security; also confirmed by: Compliance Officer of the Latvian State Radio and Television Centre, *ibid*.
[60] Compliance Officer of the Latvian State Radio and Television Centre, *supra nota* 9.
[61] Compliance Officer of the Latvian State Radio and Television Centre, *ibid*.

payment solely for managing that part of the service and for commercial services, LVRTC receives revenue from commercial customers.[62] The LVRTC Compliance Officer further clarified that LVRTC is a state owned company and controlled by the state, but it is operated by the LVRTC.[63]

## 2.2. Government controlled but private company operated hybrid model: Belgium

The Kingdom of Belgium QTSP is an example of a model where the government is the QTSP, controls and owns the QTSP, but procures a private company, Zetes SA, to host and operate the certification authority and time stamp units and they additionally fulfil roles such as personalizing the eID cards and ensuring secure transport of those cards.[64] According to the Certificate Policy (and Certification Practice Statement) for the Citizen CA and Foreign CA, the federal government is the QTSP and it is represented by the Federal Service Policy and Support – BOSA and Federal Public Service Home Affairs – BIK-GCI.[65] According to the overall QTSP's Trust Service Practice Statement, there is a Policy Management Authority (PMA) which consists of representatives of the Private Key Infrastructure (PKI) operator from the private company Zetes SA, as well as representatives from two government agencies – the Federal Public Service Policy and Support (BOSA) and the Federal Public Service Home Affairs.[66] The PMA manages documentation such as the certificate policies and certification practice statements, ensures auditing processes for proper implementation, participates in highly sensitive PKI operations, and conducts risk management.[67] While day-to-day operations and disaster preparedness are done by the procured private company, the PMA has authority over any third-party archive information retrieval and takes charge in case a disaster or critical key compromise actually occurs, assesses the disaster and gives further guidance on operations.[68] When the QTSP goes through eIDAS conformity assessments and non-conformities are determined, then too the PMA determines how to remedy the finding and in what timeline (in line with the conformity assessment body's required timeline).[69] To fulfil eIDAS Article 24 requirement to either have insurance or sufficient funds for

[62] *Ibid.*
[63] *Ibid.*
[64] Kingdom of Belgium - Federal Government, *supra nota* 10, p. 8 of the Belgium Root Certificate Policy v.1.2.
[65] *Ibid*, p. 10-11 of the Citizen & Foreigner CA Certificate Policy v.1.3.1.
[66] *Ibid*, p. 7 of the Citizen & Foreigner CA Certificate Policy v.1.3.1.; *Ibid*, p. 6-7 of the Trust Service Practice Statement v.1.1.
[67] *Ibid*, p. 6-7 of the Trust Service Practice Statement v.1.1.
[68] *Ibid*, p. 18-19 of the Trust Service Practice Statement v.1.1.
[69] *Ibid*, p. 32 of the Belgium Root Certificate Policy v.1.2.

liability of damages, the QTSP documentation simply states that as the QTSP "as part of the Belgian government maintains adequate resources and coverage to meet its obligations regarding the provision and use of its certification services".[70] In terms of documentation and similarly to the Latvian LVRTC, Belgium's QTSP also adheres to the same ETSI standards and the same NCP+ and QCP-n-qscd policies are used.[71] In terms of Registration Authorities, within Belgium both the national government and municipalities are in the Registration Authority role for both initial identification and registering of subjects as well as for revocation of certificates.[72] Abroad, Belgian consulates assume the same role.[73]

## 2.3. Private Qualified Trust Service Provider: Estonia

When reviewing the service documentation for Estonian national eID documents in card format, the general documentation format and requirements adhered to are similar to LVRTC and the Kingdom of Belgium QTSP's documentation. For instance, the same ETSI standards and the same policies for NCP+ and QCP-n-qscd are used, which can be expected as the eID documents for all three countries have the same general functions.[74] However, some differences do arise. For instance, the Estonian Certificate Policy (CP) for card format documents such as the national identity card is administered and enforced by the Estonian Police and Border Guard Board (PBGB), yet all amendments are also approved by the eID Department of the Information System Authority (RIA) and this document is published on the id.ee website which is administered by RIA[75]. The corresponding Certification Practice Statement (CPS), that conforms to the requirements of the certificate policy, is published in a different location, and can instead be found on the private company, SK ID Solutions, QTSP's website.[76] In other words, the PBGB (public sector) sets the requirements, the requirements are confirmed by RIA (also a public sector entity) and SK ID Solutions AS describes how the requirements are adhered to (private sector). Another

[70] *Ibid*, p. 33.
[71] Kingdom of Belgium - Federal Government, *supra nota* 10, p. 7 of the Citizen & Foreigner CA Certificate Policy v.1.3.1.
[72] *Ibid*, p. 13-14.
[73] *Ibid*.
[74] Police and Border Guard Board. (2023). *Police and Border Guard Board - Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card*, Version 2.0, 1-41, p. 10, 14, 38. Retrieved August 17, 2023 from https://www.id.ee/artikkel/id-kaardi-digi-id-elamisloakaardi-ja-diplomaadikaardi-sertifitseerimispoliitika/.
[75] *Ibid*. p. 15.
[76] SK ID Solutions AS. (2023). *SK ID Solutions AS – ESTEID2018 Certification Practice Statement*, Version 6.0, p. 1-47. Retrieved August 18, 2023 from https://www.skidsolutions.eu/resources/certification-practice-statement/.

noticeable difference is that the Estonian CP and CPS lists a lot more involved parties than the government QTSP models described in the previous sections, the listed parties are:

- Issuing authority of identity documents – PBGB (public sector) and the Ministry of Foreign Affairs (latter for diplomatic identity cards only) (public sector)
- Owner of the CP document and Policy Administrator: PBGB (public sector)
- Owner of the CPS document: SK ID Solutions AS and enforced by their CEO (private sector)
- Certification Authority and QTSP: SK ID Solutions AS (private sector - subcontractor of the card manufacturer)
- Registration Authorities: PBGB (public sector), Ministry of Foreign Affairs (public sector), external service providers (PBGB's contractors - private sector),
- Other Participants:
    - Card Manufacturer: Idemia (private company, contractor of the PBGB)
    - Personalizing documents: Idemia (private sector) and PBGB (public sector)
    - Minor IT support function: IT and development centre of the Ministry of the Interior (SMIT) (public sector)[77]

When it comes to liability, the private QTSP also holds an insurance policy, similarly to the LVRTC.[78] The role of eIDAS Supervisory Body in Estonia is assigned to RIA, and RIA's eID Department also holds the role of confirming changes to the CP.[79]

## 2.4. Analysis of the reviewed models

Three possible models that were identified in the analysis were: government owned and controlled QTSP (government), a government owned and controlled QTSP while a private company's services are procured to setup the QTSP and conduct the day-to-day operations (hybrid), and a private QTSP providing the service for the government but in their own name (private). Estonia uses the private QTSP model, Belgium uses the hybrid QTSP model, and Latvia uses the government owned and controlled QTSP model. The next subsections discuss the similarities and

[77] Police and Border Guard Board, *supra nota* 74, p. 10-13; SK ID Solutions AS, *supra nota* 76, p. 5-11.
[78] SK ID Solutions AS. (2024). *Insurance*. Retrieved March 31, 2024, from https://www.skidsolutions.eu/resources/insurance-policy/.
[79] Police and Border Guard Board, *supra nota* 74, p. 15; See §22 of the E-identimise ja e-tehingute usaldusteenuste seadus (lühend – EUTS). RT I, 03.03.2023, 3.

differences in the reviewed documentation, in QTSP roles, critical infrastructure status, and the presence of Conformity Assessment Bodies (CABs).

### 2.4.1. Similarities and differences in documentation

All three models use the Extended Normalized Certificate Policy (NCP+) and the QCP-n-qscd policy corresponding to qualified certificates issued to natural persons, which reside on a qualified signature creation device (QSCD). This is not surprising, as the initial review of the notified eID schemes all indicated that the three Member States all issued card based eID means, where the card is a QSCD and as Estonia currently only issues eID means to natural persons, that was also the focus in reviewing Belgium's and Latvia's documentation. In terms of service polices and practice statements for the end-user certificates, Latvia's LVRTC and the Kingdom of Belgium's QTSP combine the certificate policy (CP) and certification practice statement (CPS) into one document, as the author for both documents is the same. In case of Estonia, the two documents are separate as the government sets the requirements in the CP and the private company describes their adherence to the requirements in the CPS. The trust services documentation was accessible on one website for the Kingdom of Belgium QTSP and on one website for the LVRTC QTSP, yet for the Estonian procured private QTSP, the documentation was in two different locations (CP and Terms and Conditions for Use of Certificates on a government website and rest on the private QTSP website), which makes it more difficult to locate and in case of the CP and CPS two different documents have to be read together in order to assemble the full picture of the service provided to end users.[80]

### 2.4.2. Similarities and differences in roles

Similarities and differences also arose in the division of roles for the models reviewed. In terms of roles for approving documentation, regardless of the role a private company may hold for the QTSP, for all models the final approval of service documentation is done under the government control. For Estonia, the Police and Border Guard Board approves the CPSs that are produced by the private QTSP and the Police and Border Guard produces and manages the CP and the CP is also approved by the eID Department of the Information System Authority. For the Latvian LVRTC, significant changes to policy documentation have to be approved by the Board of the

[80] The author explains that while it is possible that there are other websites (in English and/or in local languages) that also publish the same or additional information as on the Belgium QTSP's and LVRTC's websites that the author was unable to locate, nonetheless, those looking for service-related information would benefit from having a more centralized website or at least a centralized website that links to other websites for service information.

State joint stock company and for Belgium the documentation is approved by a separate Policy Management Authority consisting of both the private company representatives as well as representatives from the Federal Government.

Another example is that all three QTSPs use RAs or registration authorities and all three use government agencies to fulfil those RA duties (e.g. Police and Border Guard Board, Office of Citizenship and Migration Affairs, Ministry of Foreign Affairs). However, Estonia additionally also uses external service providers or private companies to fulfil some of the RA duties. Which may make the public-private partnerships more complex to manage. All three countries have also approached the eIDAS Supervisory Body role differently. In case of Estonia, the role is within the Information System Authority (RIA), which is an implementing authority under the supervision of the Ministry of Economic Affairs and Communications. RIA is also the eID competence centre in Estonia. In Belgium, the Supervisory Body role is directly with the Ministry of Economy (not an implementing authority). Latvia differs even more from the other two, as the Supervisory Body role is not with one entity. Instead in Latvia, the Supervisory Body is a whole committee consisting of state secretaries from multiple ministries and directors of multiple public institutions. The latter would appear to be a great choice for eIDAS 2.0, as many different ministries and agencies will also be involved with electronic attestation of attributes for the EUDIW.

### 2.4.3. Critical entity status and vital services

Estonia is the example of the model where the government procures a private company to provide qualified trust services for the national eID means, and so far, this is the only model the Estonian government has used since the implementation of the eIDAS Regulation. In this model today, there is only one QTSP as the backbone for all Estonian national eID means used by end-users.[81] The Return of the Coppersmith Attack, or otherwise known as the ROCA crisis, that happened in Estonia (where ~800,000 eID documents were impacted) in 2017, showed how much Estonia relies on the existing public key infrastructure and how significant of an impact a vulnerability in the chip of eID cards can have.[82] Similarly, if anything happened to disrupt the qualified trust services

[81] European Commission (2023), *EU/EAA Trusted List Browser*, *supra nota 8*. The author explains that as of October 5, 2023, there are two notified QTSPs on the EU Trusted List for Estonia, however, only one of them, SK ID Solutions AS, provides qualified certificates for electronic signatures (the other, GuardTime OÜ, only provides qualified timestamp services).

[82] Lips, S., et al. (2023). Management of National eID Infrastructure as a State-Critical Asset and Public-private Partnership: Learning from the Case of Estonia. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-022-10363-5; Skierka, I. (2023). When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis. *Government Information Quarterly*, 40, Article101781. https://doi.org/10.1016/j.giq.2022.101781.

for those eID documents, the impact on the Estonian e-government would be drastic. For example, bank transfers (paying online for purchases, bill pay, or simply transferring money) over a set minimum amount in Estonia require using a qualified electronic signature, and at the time of entering the PIN code corresponding to one's signature, a real-time Online Certificate Status Protocol (OCSP) query is done to verify if the certificate for providing qualified electronic signatures is valid or revoked. If for some reason, the QTSP was suddenly no longer capable of providing qualified trust services, then the OCSP requests would also not work as only a QTSP can provide the service. In Estonia, authenticating into government service websites and many private service websites is also done by using an eID and the certificates for authentication and electronic signatures are handled as a pair without being able to have only one or the other certificate.[83] Signing into government service websites to access health related data, to register a place of residence, to vote, or authenticating into private websites, such as accessing the power company's self-service, all also require authenticating with a national or private eID means with qualified certificates, which are also checked for validity with the OCSP query.[84] A study on the Nordic-Baltic Trust Services, ordered by the Norwegian Digitalisation Agency, pointed out that models vary between northern countries in terms of qualified trust services, but Estonia is one of those countries that places security over the comfort of use, which makes sense as eID means are so widely used for a large number of government and private services in Estonia.[85] Therefore, it may not come as a surprise that as of 2018, OCSP services provided by a QTSP for authentication and digital signatures for national eID documents are considered a vital service within the meaning of the Emergency Act in Estonia.[86]

Services provided by the Latvian State Radio and Television Centre are also considered part of the critical infrastructure under Latvian legislation.[87] On the EU level, article 19 of the eIDAS Regulation requires QTSPs to enact strict measures to prevent and minimize the impact of security incidents but does not define QTSPs or the services they provide as vital or critical services.[88] However, that is about to change as according to EU Directive 2022/2555 "on measures for a high common level of cybersecurity across the Union" (NIS2) and Directive 2022/2557 "on the

[83] Police and Border Guard Board, *supra nota* 74, p. 10.
[84] *Ibid*.
[85] P. 7 of: Hinsberg *et al.*, (2020). *Study on Nordic-Baltic Trust Services*. Retrieved January, 23, 2024, from: https://www.digdir.no/internasjonalt-samarbeid/study-nordic-baltic-trust-services/2058.
[86] EUTS, *supra nota* 79, §36; Elutähtsa teenuse kirjeldus ja toimepidevuse nõuded elektroonilise isikutuvastamise ja digitaalse allkirjastamise tagamisel RT I, 15.01.2019, 11; Hädaolukorra seadus (lühend – HOS). RT I, 06.07.2023, 33.
[87] Compliance Officer of the Latvian State Radio and Television Centre, *supra nota* 9.
[88] OJ L 257, 28.8.2014, *supra nota* 6.

resilience of critical entities," all trust service providers (both QTSPs and non-qualified trust service providers) providing one or more trust service, as defined by eIDAS, will have to be identified by Member States as critical entities by July of 2026.[89] In other words, while today in Estonia a specific service provided by a QTSP is defined as a vital service, going forward the entities providing trust services will themselves be defined as critical entities or vital service providers across the EU. Directive 2022/2557 will have to be transposed into national laws by October 17, 2024 and is accordingly planned to be transposed in Estonia with the Crisis Preparedness Act (which will most likely replace the current Emergency Act).[90]

### 2.4.4. Insurance or funds requirement

Another difference determined was in relation to eIDAS Regulation Article 24 requirement for liability insurance or enough financial means. In the service documentation reviewed, the Kingdom of Belgium QTSP or hybrid model stated that the Belgian government maintains sufficient resources for liability related obligations. While the state owned Latvian LVRTC QTSP holds around three different insurance policies and the private QTSP used by the Estonian government publishes one insurance certificate on their website.

### 2.4.5. Conformity Assessment Bodies in Member States

All QTSPs must go through regular conformity assessments to keep their qualified status. According to the EU Trusted List, none of the three countries (Estonia, Latvia, Belgium) have a Conformity Assessment Body (CAB) listed nor any corresponding National Accreditation Bodies listed.[91] In fact, only ten countries in the EU have eIDAS National Accreditation Bodies, meaning only those countries have Conformity Assessment Bodies notified.[92] There are a total of 29 CABs notified, for a total of 257 QTSPs issuing qualified certificates for electronic signatures notified, meaning that around 257 QTSPs are all going through an annual eIDAS conformity assessment for providing qualified certificates for electronic signatures.[93] The ratio of CABs to QTSPs may

[89] OJ L 333 27.12.2022; OJ L 257, 28.8.2014; *ibid*.
[90] Raig, T. (2024, March 13). *Sajad ettevõtted määratakse elutähtsa teenuse osutajaks. Nõuded käivad ettevõtetele üle jõu.* Delfi ärileht. Retrieved March 15, 2024, from https://arileht.delfi.ee/artikkel/120277567/sajad-ettevotted-maaratakse-elutahtsa-teenuse-osutajaks-nouded-kaivad-ettevotetele-ule-jou.
[91] European Commission (2023), *EU/EAA Trusted List Browser*, *supra nota* 8.
[92] European Commission. (2023). *National Accreditation Bodies and Conformity Assessments Bodies for QTSP/QTS*. Retrieved September 23, 2023, from https://eidas.ec.europa.eu/efda/browse/notification/cab-nab.
[93] The author explains that while the eIDAS Regulation Article 20 requires an audit every 24 months, a surveillance audit is performed during the between years of a certification audit resulting essentially in a conformity assessment audit every year; See p. 22 of: ETSI. (2020). *ETSI EN 319 403-1 V2.3.1 (2020-06) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers*. Retrieved January 5, 2024, from: https://www.etsi.org/.

appear unrealistic and would indicate that there might be an issue in finding enough auditors from CABs; however, this does not pose a difficulty for the LVRTC according to their Compliance Officer, as they do regular procurements for CABs and when they do, they reach out to all the CABs listed on the EU Trusted List and typically receive around three offers.[94] When inquired about the frequency of changing CABs, the Compliance Officer shared that it is restricted by local legislation that no agreement should exceed five years and therefore they have had CABs from different countries regularly.[95] The COVID-19 pandemic posed difficulties for Member States to use CAB's services as movement across borders was restricted and the second phase of eIDAS conformity assessments is an on-site conformity assessment.[96] However, it is unclear from the reviewed documentation whether Estonia or Belgium face any difficulties from not having NABs or CABs listed on the EU trusted list when borders are open and movement of CABs is not restricted.

As the requirements from the eIDAS Regulation, implementing acts, and associated standards are all the same for all three models (regardless if the QTSP is a private company, government owned and controlled company, or the government themselves is a QTSP), the comparison did not reveal drastic differences, but it did reveal some. The differences are primarily in how the QTSP is financed and how roles and responsibilities are divided. For instance, a government QTSP may render more control as the operations are kept under the same roof and not in an external private company, but on the other hand it may create more difficulty in establishing clear separation of the Supervisory Body and the QTSP, which are necessary elements in creating trust between Member States when accepting qualified trust services across borders. In the next sections, specific recommendations are made for choosing a QTSP model, and recommendations are made for eIDAS Regulation related changes in the Estonian legislation for shortcomings now and for eIDAS 2.0.

[94] Compliance Officer of the Latvian State Radio and Television Centre, *supra nota 9*.
[95] *Ibid*; The author explains that the eIDAS Regulation does not set a rotation requirement for lead auditors.
[96] Koch, C., et al. (2022). Impact of the COVID-19 pandemic on accredited conformity assessment bodies: insights from a multinational study. *Accreditation and Quality Assurance*, 27, p. 275-288. https://doi.org/10.1007/s00769-022-01514-x; Mirtsch, M., et al. (2023). Quality assurance in supply chains during the COVID-19 pandemic: empirical evidence on organisational resilience of conformity assessment bodies. *Total Quality Management & Business Excellence*, 34(5-6), p. 615-636. https://doi.org/10.1080/14783363.2022.2078189; ETSI EN 403-1, supra nota 93, p. 19.

# 3. RECOMMENDATIONS

In this section specific recommendations are made for what to consider when choosing a QTSP model and what model Estonia may wish to consider. Some roles to consider due to eIDAS 2.0 are also discussed and recommendations to publicly communicate those roles are made. Shortcomings in existing legislation for Latvia, the EU in general, and Estonia in relation to the current eIDAS Regulation are described and recommendations for changes are made.

## 3.1. Public, private, or hybrid Qualified Trust Service Provider for Estonia

Today, the Estonian government has chosen to trust such services to a private company, but availability, quality of service providers, and cybersecurity threat levels may influence what options are available for the government in the future. For instance, regarding availability, in early 2023, the Estonian Police and Border Guard Board published a procurement for certification and qualified trusted services for eID documents, and while the Procurement Register's page for requesting to participate indicates there were four candidates, the tenderers page shows that only one of those four tenderers submitted an offer.[97] While there may be numerous reasons for why there was no additional interest in the procurement, it does illustrate the risk of not having any offers made during procurements for qualified trust services. In terms of cybersecurity, The EU, and large nations outside the EU such as the US and the UK have made public statements regarding the importance of the government and the private sector working together for cybersecurity, but as the comparison showed, the way different Member States have handled this technology sector, varies.[98]

When the Estonian government determines whether to outsource all or some of (qualified) trust services, then they also need to consider the increase in cyberattacks, including the geographical location of Estonia and the current effect of the Russian invasion of Ukraine. While cyberattacks can occur anywhere in the world, recent history has shown a general increase in cyberattacks, as

[97] State Shared Service Centre. (2023). *Sertifitseerimisteenuse ja kvalifitseeritud usaldusteenuse osutamine*. Procurement Register. Retrieved February 12, 2024, from https://riigihanked.riik.ee/rhr-web/#/procurement/5104440/tenders.

[98] Pattison, J. (2020). From defence to offence: The ethics of private cybersecurity. *European Journal of International Security*, 5(2), 233-254, p. 237. https://doi.org/10.1017/eis.2020.6.

well as higher levels of Russian cyberattacks towards countries neighbouring them.[99] This creates a couple of different and conflicting challenges for the Estonian government. On one hand, if the government chose to proceed with a full (or hybrid) government QTSP in the future, then they have to find ways to overcome the challenge of finding enough knowledgeable and competent personnel who wish to work for a government QTSP rather than for private IT companies, as there is large shortage of cybersecurity professionals and generally government agencies cannot compete with large corporations for salaries.[100] On the other hand, when choosing to procure the service entirely or partially from the private sector, then "the higher the number of actors and the more conflicting their goals" can result in a different set of challenges due to a complex partnership for the government to manage.[101] Based on the comparison of documentation for the three different models, the private model in Estonia did reveal a large number of different public and private sector parties involved in providing trust services, and for such a partnership to be successful the government has to continuously have the necessary capacity to manage such partnerships in terms of trust, leadership, personnel, and experience.[102] As such, Estonia may wish to consider a hybrid QTSP model in the future, similar to the Kingdom of Belgium. On one hand, a hybrid model would give Estonia direct control over the QTSP operations and would simplify the current public-private partnership model consisting of numerous public and private entities that are currently involved with the overall QTSP services. A hybrid model would also be more achievable than a full government model, as finding a large number of cybersecurity professionals with QTSP experience, and who wish to work for a government QTSP may prove to be too much of a challenge when just starting out with a government QTSP. With a hybrid model, the government would need to have enough experts in leadership roles, but could procure an experienced QTSP to provide the day-to-day services.

---

[99] Guchua, A. & Zedelashvili, T. (2023). Challenges arising from cyber security in the dimension of modern global security (on the example of the Russian-Ukraine war). *Eastern Review*, 11(2), 79-88, p. 82. https://doi.org/10.18778/1427-9657.11.18; Wilett, M. (2022). The Cyber Dimension of the Russia-Ukraine War. *Survival*, 64(5), 8-11. https://doi.org/10.1080/00396338.2022.2126193; Wirtz, B. W. & Weyerer, J. C. (2017). Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats. *International Journal of Public Administration*, 40(13), p. 1085. https://doi.org/10.1080/01900692.2016.1242614.

[100] Blažič, B. J. (2021). Changing the landscape of cybersecurity education in the EU: Will the new approach procedure the required cybersecurity skills?. *Education and Information Technologies*, 27(3), p. 3012. https://doi.org/10.1007/s10639-021-10704-y; Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security*, 2013(7), 5-10. https://doi.org/10.1016/S1361-3723(13)70062-9; Kouttis, S. (2016). *Improving security knowledge, skills and safety*, 2016(4), p. 13. https://doi.org/10.1016/S1361-3723(16)30037-9.

[101] Van Gestel, K., et al. (2012). How Governance of Complex PPPS Affects Performance. *Public Administration Quarterly*, 36(2), p. 146.

[102] *Ibid*. p. 141-180.

## 3.2. Recommendations for the new version of the eIDAS Regulation

With the upcoming changes from eIDAS 2.0, depending on the role that RIA is assigned in Estonia, there may also be a need to reassign the Supervisory Body role. According to RIA's website, RIA "develops the vision and strategy for the field of eID"[103] and they are managing "the development of the Estonian digital wallet"[104], therefore as the competent authority in this field, it is likely that they may be the best suited organization to fulfil one of the many new trusted roles eIDAS 2.0 brings. Chapter 1 of EUTS defines the Information Security Authority (RIA) as the competent authority and then uses the term "competent authority" throughout when referring to RIA, including in the role of the Supervisory Body in terms of eIDAS.[105] If this is the case, then there are a couple of different ways the Estonian government could change the role and EUTS legislation to ensure that the Supervisory Body does not supervise themselves (clear separation of QTSP from the Supervisory Body):

- the department or unit that is currently exercising supervision could be separated from the rest of RIA as an independent organization, which does not answer to the same leadership as the eIDAS competence centre[106];
- a new panel of representatives from different authorities could make up the Supervisory Body, similarly to Latvia. In Estonia, this could for example consist of representatives from different ministries who are currently related to fulfilling the requirements from eIDAS and perhaps also from the ministries who will be related through eIDAS 2.0 or more specifically the EUDIW for electronic attestation of attributes (e.g. Ministry of Economic Affairs: as the Trasport Administration falls within their jurisdiction (future electronic driver licenses) and RIA also falls into their administrative area, Ministry of Interior as the Estonian Police and Border Guard Board (primary issuer of identity documents) falls into their administrative area[107], the Ministry of Education (for future attributes such as academic qualifications), etc.); or

[103] Republic of Estonia Information System Authority. (2024). *eID competence centre*. Retrieved March 13, 2024, from https://www.ria.ee/en/state-information-system/electronic-identity-eid-and-trust-services/eid-competence-centre.
[104] Republic of Estonia Information System Authority. (2024). *Digital wallet, or the European Union Digital Identity application (EUDI Wallet)*. Retrieved March 13, 2024, from https://www.ria.ee/en/state-information-system/electronic-identity-eid-and-trust-services/eudi-wallet
[105] EUTS, *supra nota* 79.
[106] Republic of Estonia Information System Authority. (2024). *Supervision*. Retrieved February 11, 2024, from https://www.ria.ee/en/cyber-security/administrative-and-national-supervision/supervision.
[107] See §15 (4) of Isikut tõendavate dokumentide seadus (lühend - ITDS). RT I, 06.07.2023, 35.

- similarly to the Kingdom of Belgium, another option is to assign the eIDAS Supervisory Body role to the ministry most closely responsible for roles coming from the eIDAS Regulation (i.e. Ministry of Economic Affairs and Communications).

As the EUDIW will involve more agencies for the different electronic attestation of attributes (e.g. mobile driver's license, university degrees, prescription medication, travel document, and/or digital EURO), it is the author's recommendation for Estonia to consider the same approach that Latvia has taken with involving representatives from a range of ministries and public agencies in forming a Supervisory Body. Regardless of the decision on whether to change the Supervisory Body role in Estonia or not, eIDAS 2.0 will bring many new roles that need to be fulfilled and are likely to be defined in EUTS, and as such, the entity (or entities) assigned in the supervisory role would need to be clearly stated as opposed to referred to as the competent authority throughout.[108] For instance, the following are decisions Estonia (and Member States in general) will have to make:

- who will be responsible for establishing and maintaining a list of registered relying parties for the EUDIW;
- who will be responsible for the issuance of the EUDIW;
- who is the authoritative source of the person identification data for the EUDIW (data source with a specific data controller and/or processor);
- who will ensure the person identifying data is issued to the correct EUDIW;
- who is the Supervisory Body for QTSP, non-qualified trust service providers, EUDIW issuers, register etc. – this may be one Supervisory Body (such as the current one), or multiple Supervisory Bodies, as there is a long list of new non-qualified trust services defined in article 3;
- who will be responsible for notifying and updating the EUDIW scheme on the EU level;
- who will be responsible for the technical EUDIW (i.e. will it be developed by a government IT house, will it be procured from a private company, some form of public and private partnership etc.);
- will there be a national accreditation body for the EUDIW (currently Estonia does not have eIDAS related National Accreditation Bodies);

[108] European Parliament (2024), *supra nota* 13.

- will there be a Conformity Assessment Body in Estonia or will there be a contract with a Conformity Assessment Body from another country (currently Estonia does not have any conformity assessment bodies for QTSPs);
- will there be a designated body for certifying rQSCDs, QSCDs and/or EUDIW (currently Estonia does not have such bodies designated); etc.[109]

While not all of these roles would have to be written into law, they do all have to be decided upon, and adding the ongoing roles such as issuers of EUDIW, person identifying data, Supervisory Body, register maintainer, etc. to EUTS would bring more clarity into roles and transparency to Estonia's e-governance. For some of the roles, it may not be necessary to write them into law but in the interest of transparency they should be communicated in a way that is publicly accessible.[110] Transparency or sharing easily accessible information about the Estonian roles in relation to the eIDAS Regulation could also have a positive effect of bringing new interested private companies to the Estonian market for one or multiple aforementioned roles or technology.

eIDAS 2.0 also brings about an interesting change of Member States having to define administrative fines of a maximum of at least 5 000 000 euros in case the (Q)TSP infringes against the requirements stemming from the eIDAS Regulation.[111] This creates for an interesting dilemma if Estonia were to choose a government owned and/or controlled QTSP model, where if the QTSP is a part of the government (i.e. like is the case with the Kingdom of Belgium QTSP), then in case of infringements one government agency would be in a role to fine another government agency, where potentially in a very simplified way funds are simply moved from one part of the government's wallet to another. Similarly, if proceeding towards a government QTSP model, the

[109] *Ibid*; European Commission. (2023). *Designated Bodies for SSCD and QSCD*. Retrieved September 23, 2023, from https://eidas.ec.europa.eu/efda/browse/notification/designated-bodies; European Commission. (2023). *National Accreditation Bodies and Conformity Assessments Bodies for QTSP/QTS*, *supra nota* 92.

[110] Alcaraz-Quiles, F. J., et al. (2014). Factors influencing the transparency of sustainability information in regional governments: an empirical study. *Journal of Cleaner Production*, 82(2014), p. 179-191. https://doi.org/10.1016/j.jclepro.2014.06.086; Lopez-Lopez, V., et al. (2018). E-Government, Transparency & Reputation: An Empirical Study of Spanish Local Government. *Information Systems Management*, 35(4), p. 276-293. https://doi.org/10.1080/10580530.2018.1503792.
The author further explains that recently it has been on the news in Estonia that 800,000 euros were spent on a e-state application called mRiik and that the first version of the application has been scrapped and depending on who is being interviewed, the money was wasted or the money was a so-called learning experience. At the same time, it is on the news that budget cuts are necessary across the board. Therefore, as public communication regarding the EUDIW will be made shortly after, it is especially important to remain transparent in this project, to maintain the public's trust in a similar project. An example of such a news article: Pott, T. (2024, February 13). *Minister: €800,000 spent on mRiik e-state app not wasted*. Err.ee. Retrieved April 27, 2024, from https://news.err.ee/1609252110/minister-800-000-spent-on-mriik-e-state-app-not-wasted.

[111] European Parliament (2024), *supra nota* 13, article 16.

Estonian government would also have to decide whether to simply have necessary funding set aside or to have one or multiple insurance policies similarly to Latvia's LVRTC model.

As Member States will have to revise local legislation to accommodate the new eIDAS Regulation anyway, it is a good time to also eliminate existing shortcomings in local legislation. The next section describes current shortcomings in local legislation in relation to the eIDAS Regulation in force for Latvia, the EU in general, and in more detail in the Estonian legislation. Following the shortcomings are recommendations to reduce or eliminate the (potential) shortcomings.

## 3.3. Recommendations for improvements in legislation

While the eIDAS Regulation is a directly binding legislative act, it is up to Member States to decide, and where necessary, define how the requirements from the eIDAS Regulation are adhered to on the national level. When EU regulations leave room for Member States to decide how requirements from a regulation are adhered to, there may be many benefits to this such as technology neutrality, learning from other Member States of their solutions and innovation, and so forth. However, this can also lead to lack of clarity in local legislation and different interpretations between Member States.[112]

### 3.3.1. Shortcomings and recommendations for Latvian and EU legislation

Some shortcomings in existing legislation (both on the EU level and Member State level) have arisen in the course of actual implementation of the eIDAS Regulation. For instance, in an interview with the LVRTC, their Compliance Officer pointed out a shortcoming in the current legislation where eIDAS and the local Latvian legislation currently do not clarify enough: eIDAS requires notifying the Supervisory Body of incidents, but does not clearly identify what type of incidents to notify.[113] When reviewing the eIDAS Regulation, article 19, clause 2 states that "Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the Supervisory Body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant

[112] Baratta, R. (2015). Complexity of EU Law in Domestic Implementing Process. *The Theory and Practice of Legislation*, 2(3), p. 293-308. https://doi.org/10.5235/12050-8840.2.3.293.
[113] Compliance Officer of the Latvian State Radio and Television Centre, *supra nota 9*.

impact on the trust service provided or on the personal data maintained therein".[114] Clause two continues on, but does not define what constitutes a significant impact on the trust service provided. Currently, the LVRTC notifies of all incidents, with the main ones being if any of the services do not comply with an agreed SLA (for example a system is down for more minutes than permitted), but they run into situations where the requirement is unclear in terms of significant impact.[115] The Compliance Officer further explained through the following example: if for example there is a Russian DDOS attack which overloads some servers resulting in partial availability and impacting some individuals, who may have to try several times and then the system works, just not on the first try, then it is unclear whether such a situation constitutes significant impact.[116] Another example to illustrate this issue presented by the LVRTC Compliance Officer was, that it is clearly a significant incident if current users can't provide e-signatures with their eID, but unclear if it's a significant incident if only onboarding is affected.[117] The LVRTC has asked for further clarification from their Supervisory Body on this subject.[118] Once LVRTC does receive clarification from the Supervisory Body, adding such clarification also to either local legislation or making it accessible for all QTSPs in Latvia would reduce uncertainty and would lead to the same level of incident notifications across the board.[119]

In addition to the LVRTC, Trust Service Providers across the EU have demonstrated a lack of clear clarity on the type and significance of incidents to report according to the key takeaways of ENISA's Trust Services Security Incidents 2019 annual analysis report.[120] The report reiterates that according to the eIDAS Regulation, QTSPs are required to notify their Supervisory Bodies about security breaches that have a significant impact, then the Supervisory Bodies are to give an overview of the incidents to ENISA if there is a cross-border impact, and ENISA compiles an annual report such as this one. As most of the incidents that ended up in ENISA's report were minor, the lack of clarity on the severity of incidents to report appears to be unclear to more Member States than just Latvia. Whenever there is unclarity in interpreting a regulation on the EU

[114] OJ L 257, 28.8.2014, *supra nota* 6.
[115] Compliance Officer of the Latvian State Radio and Television Centre, *supra nota 9*.
[116] *Ibid*.
[117] *Ibid*.
[118] *Ibid*.
[119] Compliance Officer of the Latvian State Radio and Television Centre, *supra nota 9*. The author explains that in the interview with the Compliance Officer, the Officer pointed out that while the LVRTC is the only QTSP on national QTSP list, the Estonian QTSP SK ID Solutions AS is also active in Latvia with their private SmartID product, thus such clarification would also be beneficial for other QTSPs who are offering services within Latvia.
[120] European Union Agency for Cybersecurity. (2020) *Trust services security incident 2019 – Annual analysis report*. Retrieved September 23, 2023 from https://data.europa.eu/doi/10.2824/047833.

level, Member States can turn to the European Commission for an interpretation.[121] If Member States do not seek out an interpretation from the Commission and due to varying interpretations implement the law differently, they run the risk of infringement proceeding against them.[122] Therefore, the author recommends that if the Latvian Supervisory Body is unable to clarify the question for the LVRTC, then they ought to seek an interpretation from the European Commission. The author further recommends bringing more clarity to Member States on what constitutes a significant incident on the EU level when implementing acts are reworked or new ones published for eIDAS 2.0.

### 3.3.2. Shortcomings in the Estonian legislation

Before offering further recommendations for improvements specific to the Estonian legislation, the related legislation and identified shortcomings are described, followed then by recommendations for each identified shortcoming. The main legislation in Estonia that corresponds to the eIDAS Regulation, is the Electronic Identification and Trust Services for Electronic Transaction Act (EUTS); and according to Chapter 1, it "regulates electronic identification and trust services for electronic transactions, and organisation of state supervision to the extent that these are not regulated" by eIDAS.[123] In relation to QTSPs, EUTS assigns multiple competent authority roles to RIA (e.g. §3 assigns the role of maintaining a trusted list, multiple paragraphs in Chapter 2 refer to RIA as the authority to apply authorization to for providing trust services, §22 assigns the role of Supervisory Body, and so forth).[124] Chapter 2 further clarifies eIDAS requirements for QTSPs, (e.g. what sum the QTSP has to have in terms of insurance or security in case of compensation for damages on line with Article 13 of eIDAS, how many years records must be maintained for, etc.).[125] EUTS also covers procedures for revocation or suspension of certificates in Chapter 2, but in some instances refers to the Identity Documents Act.[126] For example, Chapter 3 of the Identity Documents Act describes the requirements for who issues certificates for national identity documents, which functions of the issuance may be delegated to another party, and the circumstances and authority for either the authentication or the electronic signature certificates.[127] For the suspension of the certificate enabling digital identification and the

[121] Baratta, R., *supra nota* 112.
[122] *Ibid*.
[123] EUTS, *supra nota* 79, §1(1).
[124] *Ibid*.
[125] *Ibid*.
[126] *Ibid*; ITDS, *supra nota* 107.
[127] *Ibid.*

certificate enabling the providing of electronic signatures, the Identity Documents Act refers back to EUTS.[128]

In other words, EUTS sets additional requirements and clarifies certain requirements from the eIDAS Regulation for the QTSPs (regardless of if they are providing commercial services or services for the public sector), yet the certificates that are issued to national identity documents are primarily regulated by the Identity Documents Act. Therefore, both EUTS and the Identity Documents Act apply to certificates for digital identification and for providing electronic signatures for national eID means, yet for certificates for private eID means, only EUTS applies. While it may be reasonable to keep requirements for national eID documents separately from private eIDs, having some requirements for national eID documents in one act and some in another can cause some confusion (for national eID documents, the revocation requirements for certificates are described in one act but suspension related requirements are described in another act). Having eIDAS requirements spread over different national acts for the same type of documents (national eID means) is the first identified shortcoming of the current national legislation.

The second shortcoming of EUTS that was identified through this research, was that EUTS copies some parts of eIDAS directly, without providing any additional guidance. Similarly to the Latvian LVRTC, when reviewing EUTS in Estonia, it does not further clarify the reporting requirement for incidents, but simply refers to the eIDAS requirement in Chapter 2.[129] When further reviewing ETSI standards, ETSI EN 319 401 also includes the same general wording "significant impact on the trust service provided and on the personal data maintained" in clause 7.9, but does not provide further clarification, nor do ETSI EN 319 411-1 or ETSI EN 319 411-2.[130] Similarly, no guidance is provided on notifying of changes to trust services, which is also vaguely stated by the eIDAS Regulation, Article 24, clause 2 as "any changes in the provision of its qualified trust services".[131]

The third potential shortcoming of EUTS is that it does not currently define or clarify all eIDAS roles on the national level. For example, §3, section 3 of EUTS states that the minister in charge

[128] *Ibid*.
[129] EUTS, *supra nota* 79, §4.
[130] See p. 18 of: ETSI. (2021). *ETSI EN 319 401 V2.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*. Retrieved January 6, 2024, from: https://www.etsi.org/; see p. 40 of: ETSI. (2023). *ETSI EN 319 411-1 V1.4.1 (2023-10) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*. Retrieved January 6, 2024, from: https://www.etsi.org/.
[131] OJ L 257, 28.8.2014, *supra nota* 6.

of the policy sector may set "requirements and procedure for establishing, maintaining and updating of a trust infrastructure", yet when clicking on the hyperlink within the text, no implementing act has been published.[132] Based on the explanatory note to EUTS in the first reading in 2016, the purpose of this section is to give RIA the right to organize the trust infrastructure in Estonia in case of situations where a QTSP may stop its activities suddenly.[133] That right corresponds directly to eIDAS Regulation Article 17, section 5, which states that Member States may set a requirement for their national Supervisory Body to establish and maintain a trust infrastructure.[134] This same right is also given to RIA in RIA's statute §8 section 3.[135] As there is no implementing act from the Ministry of Economic Affairs and Communications, and some of the procurements for trust services for national eID means are organized by the Police and Border Guard Board, this right lacks clarity on what the process would be in such an emergency situation. While as a Member State, Estonia did decide to give this optional right from eIDAS to the Estonian Supervisory Body, it has not provided any further clarification or actual direction through implementing acts to fulfil this right.

### 3.3.3. Recommendations to eliminate shortcomings in the Estonian legislation

Regarding the first shortcoming, there will always be some cross reference between legislative acts, but in the interest of clarity, qualified certificate related requirements for national eID documents could all be within the Identity Documents Act. This could be done by adding suspension related requirements to the Identity Documents Act for national eID documents and leaving the suspension related requirements for private eIDs in EUTS. Clearly stating in both legislations what type of eID means the requirements apply to, would further eliminate confusion. This minor change in the Identity Documents Act and in EUTS would increase in clarity of requirements for public vs private eID means that contain certificates for authentication and for providing qualified electronic signatures.

EUTS or an additional implementing act to EUTS is one potential place further guidance could be given on notifying of incidents and notifying of any changes in the trust services provided. While a non-legislative other public document may also fulfil this function, there does not appear to be such a guide or document currently published on the Estonian Information System Authority's

[132] EUTS, *supra nota* 79.
[133] Riigikogu. (2016). *E-identimise ja e-tehingute usaldusteenuste seadus 237 SE*. Retrieved April 18, 2024, from https://www.riigikogu.ee/tegevus/eelnoud/eelnou/323afaca-cb96-4118-a675-2a2db388141e.
[134] OJ L 257, 28.8.2014, *supra nota* 6.
[135] Riigi Infosüsteemi Ameti põhimäärus. RT I, 03.10.2023, 3.

(RIA's) website.[136] Clarifying such requirements publicly would reduce the second shortcoming, increase transparency, and would also benefit any new QTSPs and corresponding Conformity Assessment Bodies entering the Estonian market. Providing clarification on what constitutes significant incidents and changes that require notification to the Supervisory Body would aid in reducing the second shortcoming.

On the third potential shortcoming, it may be of benefit to the Estonian government to rereview whether it is necessary to add an implementing act in case the Estonian Supervisory Body does have to take over and/or maintain trust services in an emergency where a QTSP suddenly stops providing services. Alternatively, such a review may also determine that it is no longer necessary to define this in EUTS or through an implementing act to EUTS, as in 2018 a part of the QTSP's services were defined as critical services, and as such, emergency plans may already exist due to requirements in the Emergency Law and the taking over of Directive 2022/2557 on the resilience of critical entities.

### 3.3.4. Additional recommendations for Estonia

Another change for Estonia to consider is whether to define a requirement in national legislation to rotate either lead auditors or CABs after a set period of time, similarly to Latvia. As the eIDAS Regulation does not set a requirement for rotating lead auditor for the eIDAS conformity assessments, then this could be defined in an implementing act of EUTS which outlines the procedural requirements for conformity assessments of trust services and trust service providers.[137] Rotating lead auditors is standard practice in finance and other technology audit areas to prevent the auditor from auditing their own work and from becoming too close to the auditee.[138] However, further review of QTSPs and CABs would need to be done to determine if there is more benefit or harm from such a requirement. On one hand preventing an auditor from auditing their own work is a benefit, further review of whether such a requirement with the low number of CABs compared to the number of QTSPs would cause a hardship in finding available CABs to perform the assessments. As the comparison of the three models indicated, there is also currently no NAB or

[136] The author explains that as RIA is both the Supervisory Body and the eID competence centre of Estonia, it is unlikely such information would be published on a different government entity's website in Estonia.
[137] *Supra* nota 47.
[138] Dordzhieva, A. (2022). Disciplining Role of Auditor Tenure and Mandatory Auditor Rotation. *The Accounting* Review, 97(2), p. 161-182. https://doi.org/10.2308/TAR-2018-0277; article 17 of: Regulation (EU) No 537/2014 of the European Parliament and of the Council of 16 April 2014 on specific requirements regarding statutory audit of public-interest entities and repealing Commission Decision 2005/909/EC Text with EEA relevance, OJ L 158, 27.5.2014.

CAB for eIDAS in Estonia. Academic literature reviewed indicated that closing of borders during the COVID-19 pandemic, caused hardships for CABs as their movement was restricted. Estonia may benefit from encouraging existing technology audit firms to gain the necessary competence to conduct eIDAS conformity assessments and to notify a CAB in Estonia. It would not only benefit Estonia in terms of having a CAB close by but would also aid other Member States in adding more CABs to the overall EU list.

Another aspect that stood out during the comparison of the three models, was that Estonia has QTSP service documentation spread over two different websites. Having one central website that links to all locations of public service documentation, especially with a new procurement in progress and potentially new partner(s) for qualified trust services, would increase in ease of access and the expectation of online transparency by members of the public and private companies entering the Estonian digital ecosystem.[139] As the id.ee website currently seems to combine a wide range of end-user information, this would be a potential location to make accessing such information easier.[140] In the next section, the limitations of this thesis are discussed and a proposal for further research is made.

[139] Jaeger, P. T. & Bertot, J. C. (2010). Transparency and technological change: Ensuring equal and sustained public access to government information. *Government Information Quarterly*, 27(4), 371-376. https://doi.org/10.1016/j.giq.2010.05.003.

[140] Information System Authority. (2024). *ID*. Retrieved January 10, 2024, from https://www.id.ee/en/. The author explains that the website has some certificate policies and terms for using certificates, but it does not have a clear link to the QTSP's general practice statement, the certificate practice statements, conformity assessment related information, etc. that is posted directly on the QTSPs website.

# 4. LIMITATIONS AND PROPOSAL FOR FURTHER RESEARCH

The Estonian government could benefit from a further review of service documentation and from interviews with representatives from more countries, in order to shape the model that would best work for the Estonian e-government. There are limitations to this research, since the research analysed publicly available sources and only received information through interviewing, that may be publicly shared. If the interviews are conducted by Estonian government representatives, then there may also be the possibility that Member States who have strong relationships with Estonia are willing to share non-public information that may be of use (e.g., lessons learned, handling of crises situations or similar). Based on the review of the EU trusted list, the following countries appear to have some form of a government QTSP (list is not exhaustive as some countries have national QTSPs for a narrow function, such as for employees of a particular agency or similar)[141]:

- Denmark, QTSP Den Danske Stat: The Danish Digital Agency provides qualified certificates for natural persons, that can be used for electronic signatures to be used with the state's signing service.[142] While their eID means is notified to a LoA substantial, they do operate a qualified trust service. According to their website, they do not however currently provide certificates for smart cards for private company use.[143]
- Greece, QTSP Hellenic Public Administration Certification Authority: While Greece has not notified an eID means[144], they do have a government QTSP that providers authentication and electronic signature certificates for natural persons.[145]
- Spain, QTSP Dirección General de la Policía: A review of the Spanish National Police website indicates that they issue national ID cards which allow both authentication and electronic signatures.[146] Neither the website of the National Police nor documentation such as the Certificate Policy are available in English, but they have notified an eID scheme to a LoA high.[147]

[141] European Commission (2023), *EU/EAA Trusted List Browser*, *supra nota 8*.
[142] Den Danske Stat – Tillidstjenester. (2023). *Den Danske Stat Tillidstjenester (CA1)*. Retrieved October 15, 2023, from https://www.ca1.gov.dk/.
[143] Cooperation Network, *supra nota* 8.
[144] *Ibid*.
[145] Ministry of Digital Governance. (2023). *govgr*. Retrieved October 15, 2023, from https://aped.gov.gr/.
[146] Cuerpo Nacional De Policia. *DNI y Pasaporte*. Retrieved October 15, 2023, from https://www.dnielectronico.es/PortalDNIe/.
[147] Cooperation Network, *supra nota* 8.

- Finland, QTSP Digital and Population Data Services Agency: While Finland has not notified any of their eID means[148], they do have a national QTSP who provides certificates for authentication and for qualified electronic signatures.[149]

While the identification and issuance processes would vary for very specific government QTSPs, such as ones for the employees of a Ministry or Defence, from those for the general public, there may be still valuable lessons to learn from how the QTSP was established, what kind of technology is used, and how conformity assessments are carried out by conformity assessment bodies (e.g., do the conformity assessment body auditors have to obtain clearance for state secrets or similar).

- Some other countries to consider interviewing:
    - Netherlands: has multiple government QTSPs such as the Ministerie van Defensie (Ministry of Defence) and the Ministerie van Infrastructuur en Waterstaat (Ministry of Infrastructure and Water Management), who have government QTSPs, but do not offer certificates to the eIDs of the general public.[150]
    - Slovakia: Similarly to Netherlands, Slovakia has multiple government QTSPs for narrow and specific purposes such as the National Security Authority, The Ministry of Defence Slovak Republic, and the National Agency for Network and Electronic Services.[151]

[148] *Ibid*.
[149] Digital and Population Data Services Agency. (2023). *Qualified certificate*. Retrieved October 14, 2023, from https://dvv.fi/en/qualified-certificate.
[150] Ministerie van Defensie. *Certification Practice Statements*. Retrieved October 14, 2023, from https://cps.ca.pkidefensie.nl/cps-en.jsp.html; Ministry of Infrastructure and Water Management. (2024). *Trust Service Provider – TSP*. Retrieved March 24, 2024, from https://bct.tsp.minienw.nl/index_en.html.
[151] European Commission. (2023). *eIDAS Dashboard - Trust service providers results(9)*. Retrieved October 14, 2023, from https://eidas.ec.europa.eu/efda/tl-browser/#/screen/search/type/3?searchCriteria=eyJjb3VudHJpZXMiOlsiU0siXSwicVNlcnZpY2VUeXBlcyI6WyJRQ2VydEVTaWciXX0%3D

# CONCLUSION

While it has been approximately ten years since the eIDAS Regulation was entered into force and approximately seven years since it fully applied, there are still remaining gaps in regulation which may be interpreted differently across Member States and could therefore be clarified either in local legislation or through implementing acts that will be applied either six months or a year after the new version of the eIDAS Regulation is entered into force. The eIDAS Regulation is a directly binding legal act for all Member States with the goal of building trust and improved digital interoperability. Unfortunately, not all goals of interoperability and mutual acceptance were achieved with the first and current version of the eIDAS Regulation. For instance, Member States are required to accept qualified electronic signatures from other Member States, but as there are different technical formats for signatures, Member States may be unable to validate the signature and then the reality may be that the signature is denied. The eIDAS Regulation does impose strict requirements for implementation, yet as some requirements are left open and other requirements leave room for interpretation, there is still a long way to go to achieve one single digital market. Another example of those requirements up to interpretation, is how Member States choose to notify and operate a QTSP, as the regulation does not define whether the QTSP ought to be a private company or a government owned and operated QTSP for national eID means. The aim of the research was to determine the differences of operating a government QTSP vs a private QTSP in the context of Estonian practice by comparing the similarities and differences in fulfilling requirements and to provide usable recommendations to fill gaps in existing legislation.

Comparing QTSPs from different countries revealed at least three different models to explore further: a government owned and controlled company as a QTSP (government model), a government controlled QTSP for which a private company provides day-to-day services for regular operations (hybrid model), and a private company providing qualified trust services to the government through a procurement (private model). The government model identified and used in the comparison, is the state-owned Latvian company LVRTC. The Kingdom of Belgium QTSP was identified as using the hybrid model and Estonia uses the private QTSP model. The comparison revealed both similarities and differences in interpreting the complex requirements of the eIDAS Regulation, and based on the research conducted, such a comparison has not previously been done in terms of the countries chosen and the documentation compared. Regarding the similarities and differences, all three models use the same standards and policies for services provided and for formatting their service documentation, but whether policy and practice statement

documentation are separate or combined varied. Roles for approving the service documentation also vary between the countries. Furthermore, the comparison showed differences in how Registration Authority roles have been delegated and each country has chosen to notify a different Supervisory Body role from the others, but the baseline requirements for each role are the same. Estonia also revealed a more complex public-private partnership model than the government-controlled models and there were also differences in how each country has satisfied Article 24 requirements for insurance or sufficient funds. Today, there are also some differences in how QTSPs are defined as critical entities or vital service providers, but due to EU Directive 2022/2557 all QTSPs, as defined by the eIDAS Regulation, will have to be defined as critical entities going forward.

The reviewed similarities and differences lead to a proposal for Estonia to pursue a hybrid QTSP model in the future, in order to gain more control over vital service operations, while considering the additional (cyber)security risks brought form the geographical location. The hybrid model would also make it easier to manage the risk of not finding enough qualified employees in a niche field, in comparison to the government model, and would allow to set up the new model with the help of an already experienced private QTSP. Being in direct control of the QTSP would aid in simplifying the already complex public-private partnerships to provide QTSP services (e.g. from government Registration Authorities such as the police or consulates abroad, to using supermarkets in a limited Registration Authority role to issue electronic identity documents). As the eIDAS Regulation is about to be changed to what is commonly called eIDAS 2.0, it is currently the appropriate time to consider the best model of a QTSP for national eID means, as eIDAS 2.0 requires all Member States to provide an EUDIW to natural and legal persons by the end of 2026 or beginning of 2027. As the EUDIW is required at a minimum to allow authentication and providing of qualified electronic signatures, then a QTSP is needed to provide qualified certificates and to manage a remote QSCD or rQSCD. The renewed regulation also defines many more trust services and complex new roles which need to all work together to ensure a functioning EUDIW, which can lead to Member States to look at their existing QTSP models and to consider new models in light of new requirements. Member States will need to consider how to define all the different new roles as well, and in case of Estonia, some of those roles can be defined in the EUTS legislation and others on a publicly accessible website. Either way, all roles should be defined in the interest of transparency to end-users, as well as to new companies wishing to enter the Estonian market to provide such services. Smaller countries such as Estonia, where competence in this field is within the same organization as the eIDAS Supervisory Body role, may need to consider

separating those roles to ensure continued impartiality and the three proposed options (separating the existing Supervisory Body to an independent organization, moving the role to the Ministry of Economic Affairs and Communications, or best fitted option for eIDAS 2.0: forming a panel of representatives similar to the Latvian model) are a usable starting point to analyze the best possible solution.

The comparison of models also revealed a number of existing shortcomings in current legislation both on the EU level as well as in Estonia in relation to the eIDAS Regulation. One area of contributions offered within the thesis are concrete proposals to eliminate those shortcomings. For instance, the eIDAS Regulation requires QTSPs to notify significant incidents, but there is unclarity between Member States on what constitutes a significant incident. This ambiguity could be either clarified on the local level (i.e. in Estonia in EUTS or on the public website operated by the authority that includes the Supervisory Body) or more clarity can be provided with implementing acts of eIDAS 2.0. Clarity for this requirement is especially important, as the timeframe for QTSPs to notify significant incidents is reduced by eIDAS 2.0 from having 24 hours from becoming aware of an incident to 24 hours from the incident occurring.

Review of Estonian legislation also revealed multiple other shortcomings. For example, there is cross reference between two different local legislations for the same type of electronic identity document, that could be simplified as proposed within the work. Certain assigned roles in the existing Estonian legislation also lack clarity and should therefore be reviewed and updated. The Estonian government will have to update local legislation such as EUTS to accommodate changes from eIDAS 2.0 once it is published within the next few months, so this will also be an opportunity to eliminate current shortcomings during the same updates. Other proposals are also made to the Estonian government in light of the results of the thesis. For instance, to move away from the current practice of publishing qualified trust service related information on multiple websites and moving them all to one repository for transparency and ease of access. Some fields also require the rotation of lead auditors (e.g. finance audits, other technology audits) to prevent the auditor from auditing their own work. Similarly to Latvia, Estonia could also consider imposing a requirement for eIDAS lead auditors to rotate after a set number of years. This would however require a deeper analysis, as there are limited number of eIDAS Conformity Assessment Bodies across the EU, and such a requirement could cause some difficulty in the availability of the lead auditors.

While this research provides insight into different models and is a functional starting point in determining the best possible QTSP model for Estonia, it is based only on publicly available information. Estonia (or other Member States) would benefit from a more in-depth review of information that other Member States are willing to share between government representatives and that is not accessible publicly to go into more depth on the challenges and benefits of changing to a different QTSP model. In addition to the three models compared, six additional countries are proposed for the Estonian government to contact for a more in-depth review of other possible hybrid and/or government models.

# LIST OF REFERENCES

## Scientific articles


1. Alcaraz-Quiles, F. J., Navarro-Galera, A. & Ortiz-Rodríguez, D. (2014). Factors influencing the transparency of sustainability information in regional governments: an empirical study. *Journal of Cleaner Production*, 82(2014), 179-191. https://doi.org/10.1016/j.jclepro.2014.06.086.

2. Bannister, F. & Connolly, R. (2012). Defining e-Governance. *e-Service Journal*, 8(2), 3-25. https://doi.org/10.2979/eservicej.8.2.3.

3. Baratta, R. (2015). Complexity of EU Law in Domestic Implementing Process. *The Theory and Practice of Legislation*, 2(3), 293-308. https://doi.org/10.5235/12050-8840.2.3.293.

4. Blažič, B. J. (2021). Changing the landscape of cybersecurity education in the EU: Will the new approach procedure the required cybersecurity skills?. *Education and Information Technologies*, 27(3), 3011-3036. https://doi.org/10.1007/s10639-021-10704-y.

5. Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security*, 2013(7), 5-10. https://doi.org/10.1016/S1361-3723(13)70062-9;

6. Determann, L. (2021). Electronic Form Over Substance: eSignature Laws Need Upgrades. *Hastings Law Journal*, 72(5), 1385-1452.

7. Dordzhieva, A. (2022). Disciplining Role of Auditor Tenure and Mandatory Auditor Rotation. *The Accounting Review*, 97(2), 161-182. https://doi.org/10.2308/TAR-2018-0277.

8. Ducato, R. (2023). Why Harmonised Standards Should Be Open. *IIC - International Review of Intellectual Property and Competition Law*, 54, 1173-1178. https://doi.org/10.1007/s40319-023-01372-1.

9. Entschew, E., Hall, K., Bailey, C., & Nguyen, K. (2022). A New eIDAS Beginning for QWACs. *Datenschutz Datensicherheit - DuD*, 46, 217–224. https://doi.org/10.1007/s11623-022-1591-x.

10. Fábián, A. & Kollár, G. (2023). Trends in the Digitalisation of Public Administrations - In Light of EU Legislation and Domestic Developments. Central European Public Administration Review (CEPAR), 21(2), 119-140. https://doi.org/10.17573/cepar.2023.2.06.

11. Fernandez, R. (2022). Reflections on the European Digital Identity Project in Light of the Digital Covid Certificate and the Self-Sovereign Identity Movement. *Revista Catalana de Dret Public (Catalan Journal of Public Law)*, 65, 179-193.

12. Guchua, A. & Zedelashvili, T. (2023). Challenges arising from cyber security in the dimension of modern global security (on the example of the Russian-Ukraine war). *Eastern Review*, 11(2), 79-88. https://doi.org/10.18778/1427-9657.11.18.

13. Hardy, A. (2023). Digital innovation and shelter theory: exploring Estonia's e-Residency, Data Embassy, and crossborder e-governance initiatives. *Journal of Baltic Studies*, 1-18. https://doi.org/10.1080/01629778.2023.2288118.

14. Hölbl, M., Kežmah, B. & Kompara, M. (2023). eIDAS Interoperability and Cross-Border Compliance Issues. *Mathematics*, 11(2), Article430. https://doi.org/10.3390/math11020430.

15. Jaeger, P. T. & Bertot, J. C. (2010). Transparency and technological change: Ensuring equal and sustained public access to government information. *Government Information Quarterly*, 27(4), 371-376. https://doi.org/10.1016/j.giq.2010.05.003.

16. Koch, C., Ashari, P. A., Mirtsch, M., Blind, K. & Castka, P. (2022). Impact of the COVID-19 pandemic on accredited conformity assessment bodies: insights from a multinational study. *Accreditation and Quality Assurance*, 27, 275-288. https://doi.org/10.1007/s00769-022-01514-x.

17. Kouttis, S. (2016). Improving security knowledge, skills and safety. *Computer Fraud & Security*, 2016(4), 12-14. https://doi.org/10.1016/S1361-3723(16)30037-9.

18. Kutylowski, M. & Blaśkiewicz, P. (2023). Advanced Electronic Signatures and eIDAS – Analysis of the Concept. *Computer Standards & Interfaces*, 83, Article103644. https://doi.org/10.1016/j.csi.2022.103644.

19. Lips, S., Tsap, V., Bharosa, N., Krimmer, R., Tammet, T. & Draheim, D. (2023). Management of National eID Infrastructure as a State-Critical Asset and Public-private Partnership: Learning from the Case of Estonia. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-022-10363-5.

20. López-López, V., Iglesias-Antelo, S., Vázquez-Sanmartín, A., Connolly, R. & Bannister, F. (2018). E-Government, Transparency & Reputation: An Empirical Study of Spanish Local Government. *Information Systems Management*, 35(4), 276-293. https://doi.org/10.1080/10580530.2018.1503792.

21. Martens, T. (2010). Electronic identity management in Estonia between market and state governance. *IDIS*, 3, 213-233. https://doi.org/10.1007/s12394-010-0044-0.

22. Meijer, A. (2015). E-governance innovation: Barriers and strategies. *Government Information Quarterly*, 32(2), 198-206. https://doi.org/10.1016/j.giq.2015.01.001.

23. Mets, T. & Parsovs, A. (2019). Time of Signing the Estonian Digital Signature Scheme. *Digital Evidence and Electronic Signature Law Review*, 16, 40-50.

24. Mirtsch, M., Koch, C., Ashari, P. A., Blind, K. & Castka, P. (2023). Quality assurance in supply chains during the COVID-19 pandemic: empirical evidence on organisational resilience of conformity assessment bodies. *Total Quality Management & Business Excellence*, 34(5-6), 615-636. https://doi.org/10.1080/14783363.2022.2078189

25. Pattison, J. (2020). From defence to offence: The ethics of private cybersecurity. *European Journal of International Security*, 5(2), 233-254. https://doi.org/10.1017/eis.2020.6.

26. Pelikánová, R. M., Cvik, E. D., & MacGregor, R. (2019). Qualified electronic signature – EIDAS striking Czech public sector bodies. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis*, 67(6), 1551-1560. https://doi.org/10.11118/actaun201967061551

27. Pöhn, D., Grabatin, M., & Hommel W. (2021). eID and Self-Sovereign Identity Usage: An Overview. *Electronics*, 10(22), Article2811. https://doi.org/10.3390/electronics10222811.

28. Sharif, A., Ranzi, M., Carbone, R., Sciarretta, G., Marino, F. A. & Ranise, S. (2022). The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes. *Applied Sciences*, 12(24), Article12679. https://doi.org/10.3390/app122412679.

29. Skierka, I. (2023). When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis. *Government Information Quarterly*, 40, Article101781. https://doi.org/10.1016/j.giq.2022.101781.

30. Srinivas, J., Das, A. K. & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92(2019), 178-188. https://doi.org/10.1016/j.future.2018.09.063.

31. Umbach, G. & Tkalec, I. (2022). Evaluating e-governance through e-government: Practices and challenges of assessing the digitalisation of public governmental services. *Evaluation and Program Planning*, 93, Article102118. https://doi.org/10.1016/j.evalprogplan.2022.102118.

32. Van Gestel, K., Voets, J. & Verhoest, K. (2012). How Governance of Complex PPPS Affects Performance. *Public Administration Quarterly*, 36(2), 140-188.

33. Wilett, M. (2022). The Cyber Dimension of the Russia-Ukraine War. *Survival*, 64(5), 7-26. https://doi.org/10.1080/00396338.2022.2126193.

34. Wirtz, B. W. & Weyerer, J. C. (2017). Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats. *International Journal of Public Administration*, 40(13), 1085-1100. https://doi.org/10.1080/01900692.2016.1242614.

**Estonian Legislation**

1. E-identimise ja e-tehingute usaldusteenuste seadus (lühend – EUTS). RT I, 03.03.2023, 3.

   In English: Electronic Identification and Trust Services for Electronic Transactions Act. RT I, translation published 06.03.2023.

2. Elutähtsa teenuse kirjeldus ja toimepidevuse nõuded elektroonilise isikutuvastamise ja digitaalse allkirjastamise tagamisel. RT I, 15.01.2019, 11.

In English: The description and requirements for ensuring the continuity of digital identification and digital signing as a vital service, translation published 10.10.2019.

3. Hädaolukorra seadus (lühend – HOS). RT I, 06.07.2023, 33.

   In English: Emergency Act, translation published 08.01.2024.

4. Isikut tõendavate dokumentide seadus (lühend - ITDS). RT I, 06.07.2023, 35.

   In English: Identity Documents Act, translation published 16.01.2024.

5. Riigi Infosüsteemi Ameti põhimäärus. RT I, 03.10.2023, 3.

6. Usaldusteenuse osutaja ja usaldusteenuse vastavushindamise kord RT I, 28.10.2016, 17.

**EU legislation**

1. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333 27.12.2022, p. 80-152.

2. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance), OJ L 333, 27.12.2022, p. 164-198

3. Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance), OJ L 151, 7.6.2019, p. 70-115.

4. Regulation (EU) No 537/2014 of the European Parliament and of the Council of 16 April 2014 on specific requirements regarding statutory audit of public-interest entities and repealing Commission Decision 2005/909/EC Text with EEA relevance, OJ L 158, 27.5.2014, p. 77-112.

5. 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, OJ L 257, 28.8.2014, p. 73-114.

6. European Parliament. (2024). *European Digital Identity Framework*. Retrieved March 24, 2024. Retrieved from: https://www.europarl.europa.eu/doceo/document/TA-9-2024-02-29_EN.html.

**Other sources**

1. Cooperation Network, Kirova, M. (2023). *Overview of pre-notified and notified eID schemes under eIDAS*. Retrieved October 14, 2023, from https://ec.europa.eu/digital-building-

blocks/wikis/pages/viewpage.action?spaceKey=EIDCOMMUNITY&title=Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS;

2. Compliance Officer of the Latvian State Radio and Television Centre. Author's Microsoft Teams videocall interview. Notes of the interviewer. March 12, 2024.

3. Cuerpo Nacional De Policia. *DNI y Pasaporte*. Retrieved October 15, 2023, from https://www.dnielectronico.es/PortalDNIe/

4. Den Danske Stat – Tillidstjenester. (2023). *Den Danske Stat Tillidstjenester (CA1)*. Retrieved October 15, 2023, from https://www.ca1.gov.dk/.

5. Digital and Population Data Services Agency. (2023). *Qualified certificate*. Retrieved October 14, 2023, from https://dvv.fi/en/qualified-certificate.

6. ePraksts. (2023). *Service policies*. Retrieved October 14, 2023, from https://www.eparaksts.lv/en/about_us/repository/Politikas.

7. ePraksts. (2023). *Service Practice Statement*. Retrieved October 14, 2023, from https://www.eparaksts.lv/en/about_us/repository/service_practice_statements.

8. ETSI. (2021). *ETSI EN 319 401 V2.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*. Retrieved January 6, 2024, from: https://www.etsi.org/.

9. ETSI. (2020). *ETSI EN 319 403-1 V2.3.1 (2020-06) Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers*. Retrieved January 5, 2024, from: https://www.etsi.org/.

10. ETSI. (2023). *ETSI EN 319 411-1 V1.4.1 (2023-10) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.* Retrieved January 6, 2024, from: https://www.etsi.org/.

11. ETSI. (2023). *ETSI EN 319 411-2 V2.5.1 (2023-10) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*. Retrieved January 6, 2024, from: https://www.etsi.org/.

12. European Commission. (2023*). Designated Bodies for SSCD and QSCD*. Retrieved September 23, 2023, from https://eidas.ec.europa.eu/efda/browse/notification/designated-bodies.

13. European Commission. (2023). *eIDAS Dashboard - Trust service providers results(9)*. Retrieved October 14, 2023, from https://eidas.ec.europa.eu/efda/tl-browser/#/screen/search/type/3?searchCriteria=eyJjb3VudHJpZXMiOlsiU0siXSwicVNlcnZpY2VUeXBlcyI6WyJRQ2VydEVTaWciXX0%3D

14. European Commission. (2023). *eIDAS Regulation*. Retrieved October 14, 2023 from https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.

15. European Commission. (2023*). EU/EEA Trusted List Browser*. Retrieved September 23, 2023, from https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home.

16. European Commission. (2024). *European Standards*. Retrieved April 20, 2024, from https://single-market-economy.ec.europa.eu/single-market/european-standards_en.

17. European Commission. (2017). *Joint Statement by Vice-President Ansip and Commissioner Gabriel welcoming the adoption of the Tallinn Declaration on e-government*. Retrieved October 14, 2023 from https://ec.europa.eu/commission/presscorner/detail/it/STATEMENT_17_3742.

18. European Commission. (2023). *National Accreditation Bodies and Conformity Assessments Bodies for QTSP/QTS*. Retrieved September 23, 2023, from https://eidas.ec.europa.eu/efda/browse/notification/cab-nab.

19. European Union Agency for Cybersecurity. (2017). *Guidelines on initiation of qualified trust services – Technical guidelines on trust services*. European Network and Information Security Agency: EU Publications. https://data.europa.eu/doi/10.2824/238163.

20. European Union Agency for Cybersecurity. (2017). *Recommendations for QTSPs based on standards – Technical guidelines on trust services*. European Network and Information Security Agency: EU Publications. https://data.europa.eu/doi/10.2824/721561.

21. European Union Agency for Cybersecurity, Gorniak, S., Nikolouzou, E., Agrafiotis, I. & Bugneac, D. (2021). *Security framework for qualified trust service providers – Technical guidelines of qualified trust service providers*. European Network and Information Security Agency: EU Publications. https://data.europa.eu/doi/10.2824/06258.

22. European Union Agency for Cybersecurity. (2020) *Trust services security incident 2019 – Annual analysis report*. Retrieved September 23, 2023 from https://data.europa.eu/doi/10.2824/047833.

23. Hinsberg *et al*., (2020). *Study on Nordic-Baltic Trust Services*. Retrieved January, 23, 2024, from: https://www.digdir.no/internasjonalt-samarbeid/study-nordic-baltic-trust-services/2058.

24. Information System Authority. (2024). *ID*. Retrieved January 10, 2024, from https://www.id.ee/en/.

25. Kingdom of Belgium - Federal Government. (2023). *Policies and Practice Statements*. Retrieved October 14, 2023 from https://repository.eidpki.belgium.be/#/policies.

26. Kriova, M., European Commission. (2016, June 28) eIDAS – Implementing Acts. Retrieved September 23, 2023, from https://ec.europa.eu/futurium/en/content/eidas-implementing-acts.html.

27. Latvia State Radio and Television Center. (2023). *About Us*. Retrieved October 14, 2023, from https://www.lvrtc.lv/en/about-us/.

28. Ministerie van Defensie. *Certification Practice Statements*. Retrieved October 14, 2023, from https://cps.ca.pkidefensie.nl/cps-en.jsp.html.

29. Ministry of Defence Republic of Latvia. *Supervisory Committee of Digital* Security. Retrieved October 14, 2023, from https://www.mod.gov.lv/en/nozares-politika/cybersecurity/supervisory-committee-digital-security.

30. Ministry of Digital Governance. (2023). *govgr*. Retrieved October 15, 2023, from https://aped.gov.gr/.

31. Ministry of Infrastructure and Water Management. (2024). *Trust Service Provider – TSP*. Retrieved March 24, 2024, from https://bct.tsp.minienw.nl/index_en.html.

32. Police and Border Guard Board. (2023). *Police and Border Guard Board, Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card,* Version 2.0. Retrieved August 17, 2023 from https://www.id.ee/artikkel/id-kaardi-digi-id-elamisloakaardi-ja-diplomaadikaardi-sertifitseerimispoliitika/.

33. Pott, T. (2024, February 13). *Minister: €800,000 spent on mRiik e-state app not wasted*. Err.ee. Retrieved April 27, 2024, from https://news.err.ee/1609252110/minister-800-000-spent-on-mriik-e-state-app-not-wasted.

34. Raig, T. (2024, March 13). *Sajad ettevõtted määratakse elutähtsa teenuse osutajaks. Nõuded käivad ettevõtetele üle jõu.* Delfi ärileht. Retrieved March 15, 2024, from https://arileht.delfi.ee/artikkel/120277567/sajad-ettevotted-maaratakse-elutahtsa-teenuse-osutajaks-nouded-kaivad-ettevotetele-ule-jou.

35. Republic of Estonia Information System Authority. (2024). *Digital wallet, or the European Union Digital Identity application (EUDI Wallet)*. Retrieved March 13, 2024, from https://www.ria.ee/en/state-information-system/electronic-identity-eid-and-trust-services/eudi-wallet.

36. Republic of Estonia Information System Authority. (2024). *eID competence centre*. Retrieved March 13, 2024, from https://www.ria.ee/en/state-information-system/electronic-identity-eid-and-trust-services/eid-competence-centre.

37. Republic of Estonia Information System Authority. (2024). *Supervision*. Retrieved February 11, 2024, from https://www.ria.ee/en/cyber-security/administrative-and-national-supervision/supervision.

38. Riigikogu. (2016). *E-identimise ja e-tehingute usaldusteenuste seadus 237 SE*. Retrieved April 18, 2024, from https://www.riigikogu.ee/tegevus/eelnoud/eelnou/323afaca-cb96-4118-a675-2a2db388141e.

39. SK ID Solutions. (2024). *Compliance Audit*. Retrieved March 31, 2024, from https://www.skidsolutions.eu/resources/compliance-audit/.

40. SK ID Solutions AS. (2023). *SK ID Solutions AS - ESTEID2018 Certification Practice Statement*, Version 6.0. Retrieved August 18, 2023 from https://www.skidsolutions.eu/resources/certification-practice-statement/.

41. SK ID Solutions AS. (2024). *Insurance*. Retrieved March 31, 2024, from https://www.skidsolutions.eu/resources/insurance-policy/.

42. State Shared Service Centre. (2023). *Sertifitseerimisteenuse ja kvalifitseeritud usaldusteenuse osutamine*. Procurement Register. Retrieved February 12, 2024, from https://riigihanked.riik.ee/rhr-web/#/procurement/5104440/tenders.

# APPENDICES

## Appendix 1. Non-exclusive licence

**A non-exclusive licence for reproduction and publication of a graduation thesis[152]**

I, Getter Õunapuu,

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "Differences in Cross Border Compliance for Providing Trust Services for National Electronic Identity Means",

supervised by Thomas Hoffmann,

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

---

01.05.2024

[152] *The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period*