**TALLINN UNIVERSITY OF TECHNOLOGY**

**Faculty of Social Sciences**

**Tallinn Law School**

Sandra Särav

# Effectuating the Concept of Borderless Digital Citizen with the Estonian E-Residency

Master's Thesis

Supervisor: Tanel Kerikmäe LL.M, LL.Lic, Ph.D

Tallinn 2015

I hereby declare that I am the sole author
of this Master's Thesis and it has
not been presented to any other
university of examination.

Sandra Särav
" … " ..... 2015

The Master's Thesis meets the established requirements

Supervisor Tanel Kerikmäe

" ..... " ..... 2015

Accepted for examination " ..... " ..... 2015

Board of Examiners of Law Master's Theses

……

# Table of Contents

## Abbreviations

| | |
|---|---|
| **DSM** | Digital Single Market |
| **e-ID** | Electronic Identity |
| **eIDAS** | Electronic Identification and Signature |
| **eIDMS** | Electronic Identity Management System |
| **ICT** | Information and Communications Technology |
| **IDA** | Identity Documents Act |
| **PKI** | Public Key Infrastructure |

# Introduction

Given master's thesis is presented in the form of an academic publication supported by explanatory concept framing the publication. Insofar as the article will not be published by the time of defence, the author presents the committee an official statement from the editor of the book where the article is published in the form of a chapter. As foreseen by the Tallinn University of Technology rules, the student and supervisor are named co-authors of the publication.

## I. Novelty of the chosen topic and basis for selection

Estonian rapid technological developments since restoration of its Independence have attracted attention globally. The uptake of information and communications technologies (ICTs) in establishing a comprehensive e-governance system has induced Estonian people to lead a quasi-digital lifestyle with which they are apparently content. Towards the very end of year 2014, Estonia became the first country in the world to render accessible some of its e-government services to non-Estonians. The programme launched for that purpose is a government-supported concept termed e-residency, which foresees the issuing of e-residencies – the Estonian equivalent to digital identities – to foreign nationals. Based on the pre-existing system of national digital identity cards, the e-residency as a state-proven digital identity dispensed by the government of this tech-savvy European Union Member State is intended to grant its users a secure access to world-leading digital services via a smart identity card, but does not entail citizenship nor even full residency.

The implementation of the notion of e-residency originates from Estonian Development Fund price-winning development idea presented in 2014 by Taavi Kotka, Ruth Annus and Siim Sikkut and aspired to have 10 million Estonians by the year 2025.[1] This concept was subsequently inserted into Digital Strategy 2020 for Estonia, which in turn indicated the issuing of virtual residencies to foreign nationals to serve the purpose of retaining the image of Estonia as a technologically advanced country.[2] Another motive behind issuing the e-residencies for

[1] Information retrieved from the Estonian Development Fund website: http://www.arengufond.ee/2014/06/arenguidee-konkursi-2014-loppurituse-salvestused/

[2] Digital Agenda 2020 for Estonia. Ministry of Economic Affairs and Communications. Available at: https://e-estonia.com/wp-content/uploads/2014/04/Digital-Agenda-2020_Estonia_ENG.pdf, Chapter 5.4.

Estonia pursuant to the same Agenda is to support the Estonian aspiration to become renowned for the e-services.[3] The legislative footing for the e-residency, the Identity Documents Act of Estonia,[4] states as the objective of issuing the e-residencies the promoting of "the development of the Estonian economy, science, education or culture by providing access to e-services with the Estonian digital document."[5] Cumulatively, the e-residency serves a third objective stemming from its official Concept, i.e., contribution to Estonian compatriot policy.[6]

Nowhere else in the world is there such an efficacious implementation of the idea of a borderless digital citizen as there is in Estonia, whose digital services unlocked to foreign nationals (now e-residents), include the possibility to digitally sign documents (legally enforceable in any EU Member State[7]), do online banking, as well as establish and manage a company in Estonia and declare its taxes online. E-residency obtained clearance from the Government at the end of April 2014 and the first e-residency was issued to British journalist Edward Lucas on 1 December 2014. The concept is unique and innovative, matching the criteria of what is internationally and at the European Union level being sought after for the purpose of legitimisation of mutual recognition of electronic identities at international and supranational levels.[8] When becoming aware on opening of the virtual borders of Estonia during the summer 2014, the author of this thesis found a gradually developing research interest in the scope of legal and technical application of the e-residency. The prominence of the topic is manifold. Firstly, by following the scope and progress it can be rightfully stated that although the idea for the need of virtual citizens is not a novel one, there are no comparable programmes whereby a country has opened its public and private sector services to foreign nationals[9]. In fact, lack of

[3] Ibid, p. 3.
[4] Estonian Identity Documents Act. RT I, 23.03.2015, 16, for provisions directly related to e-residency, see Chapter $5^2$ E- resident's Digital Identity Card
[5] Ibid, § $20^5$ (2).
[6] The Concept, p. 6.
[7] Regulation 910/2014, on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) adopted by the co-legislators on 23 July 2014 is a milestone to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities.
[8] An example of the process of digital identity management has been provided by Price, who divides it into four steps: 1. A user presents themselves to a trusted authority. 2. The trusted authority verifies the user's identity. 3. The user is then given an ''identifier''. 4. That ''identifier'' is then presented by the user when they wish to access or use a service post-registration. See Price, G. The benefits and drawbacks of using electronic identities. Information Security Technical Report, 2008, 13, p. 95.
[9] Although identity management with the use of privacy-enhancing tools have been considered to increase the control over "online identities" since 2000s, there has been no globally effective system developed to day. See for instance Hansen, M., Berlich, P., Camenisch, J., Claus, S., Pfitzmann, A., Waidner, M. Privacy-Enhancing Identity Management. Information Security Technical Report, 2004, 9 (1), pp 35-44.

common secure digital identification methods has led some authors write about an era of a "global identity crisis."[10] The significance of e-residency is also notable by considering the fact that the Digital Strategy 2020 of the EU has acknowledged the need for cross-border electronic identification and trust services for the effectuation of the Digital Single Market (DSM).[11]

## II. Methodology and research materials

In order to gain a more organised understanding of the concept of e-residency with regard to its underlying reasons, its status and position in the Estonian regulatory context, qualitative research methods were used for legal assessment. Structured and systematic research into Estonian relevant legislation surrounding the concept was conducted. Insofar as there is no first-hand previous literature on the topic of e-residency due to its novelty, the statuses of more prevalent related concepts common in academic sources, such as "electronic identity", "digital identity management", "electronic identification", "digital person" were analysed. The research process was exploratory and the outcomes do not offer definite solutions to the various discrepancies regarding e-residency, but direct attention to antagonism of e-residency within a rule of law state. The official Concept of e-residency in the form of an Appendix to explanatory memorandum[12] (hereinafter referred to as the Concept or the official Concept) to draft legislation of the Estonian Identity Documents Act[13] provided the necessary insight and scope of application of the idea of e-residency as seen by its drafters and served as the most ample document providing the comprehension of e-residency.

Based on the initial inquiries into the topic and various aspects it embraces, a hypothesis was developed for the research: The Estonian digital identity (e-residency) is not yet sufficiently regulated nor does Estonia have the institutional capacity for the purpose of effectuating the

[10] See Saxby, S. (2014). Electronic identity: The global challenge. Presented at the 8th International Conference on Legal, Security and Privacy issues in IT Law (LSPI) November 11e15, 2013, Tilleke & Gibbins International Ltd., Bangkok, Thailand. *Computer law & Security review*, 30, p. 112.

[11] See for that purpose the European Commission Directorate General for Communications Networks, Content and Technology introduction to eIDAs, available at: http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond. In July 2014, a new regulation was adopted on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) and the related delegated / implementing acts are being developed.

[12] Issuing digital identities to non-residents: creating e-residency. Concept. Appendix to explanatory memorandum to draft legislation of Estonian Identity Documents Act and State Fees Act. Appendix 1." [Mitteresidentidele digitaalse isikutunnistuse väljaandmine: e-residentsuse loomine. Kontseptsioon. Isikut tõendavate dokumentide seaduse ja riigilõivuseaduse muutmise seaduse eelnõu seletuskirja juurde. Lisa 1.] 2014.

[13] Estonia Identity Documents Act, RT I, 23.03.2015, 16.

concept of a borderless digital citizen; however, the existing technical platform has a capability to serve as a key for a supranational identity management system within the meaning of eIDAS regulation at the EU level. At this point, there is no possibility to see how effective, secure or successful the e-residency programme will become due to its relatively short life-span; therefore, in order to confirm or overrule the hypothesis, five research questions were set forth:

a. What is the national objective and what is the legal basis for e-residency in Estonia?
b. Are the various aspects of the concept of e-residency in compliance with national and EU legislation?
c. What is the legal status of an e-resident?
d. What are technical solutions the e-residency is based on?
e. Can e-residency provide means for sought-after cross border safe electronic identification?

## III. Main emphasis and outcomes of the work undertaken

The scope of the chapter outstretched in the successive part of this thesis titled "E-Residency – a Cyberdream Embodied in a Digital Identity Card?" will be published in the Springer-Verlag Heidelberg book *Future of eTechnologies*. This work of the author of given thesis scrutinises the concept of e-residency from various perspectives. The first principal section of the chapter (section 2 – The concept of e-residency outstretched) focuses on explaining the concept, bearing in mind that at the time of writing it, there are no previous English language research outcomes published on the topic. Even though four articles have been published in *Juridica*,[14] they are in Estonian language and only one of them is solely dedicated to e-residency, whereas it is written by one of the authors of the concept itself and thus cannot be regarded to provide entirely impartial overview. Consequently, the first section after the introduction in the publication sheds light on the reciprocal benefits in terms of the e-resident vis-à-vis the Estonian state, and provides an overview of what does the status of an Estonian e-resident entail. The second main part of the publication (section 3 – The Conflicting regulatory framework) focuses on the Estonian national legislation that was amended in order to legitimise the concept of e-residency, as well as discusses the legal certainty for the e-residents within the framework of e-residency;

[14] Alekand, A. Osaühingu osanikeregistri pidamine. Juridica, 2015 (1), pp 10-15; Rosentau, M. *E-tempora, e-mores*. Juridica, 2015 (2), pp 138-153; Tupay, P. K. and Mikiver, M. E-riik ja põhiõigused. Juridica, 2015 (3), pp 163-176; Annus, R. E-residentsus. Juridica 2014 (10), pp 740-750.

additional focus point is on EU principles of data protection. Third section (section 4 – Can e-residency create a global digital citizen?) touches upon the e-residency as a tool for digital identity management.

# E-Residency – a Cyberdream Embodied in a Digital Identity Card?

Sandra Särav and Tanel Kerikmäe

**Abstract** Estonia – the small, yet digitally advanced EU Member State, is the first country to open up its e-services to the world by issuing e-residencies, the Estonian equivalent to digital identity, to non-nationals. The Estonian digital identity or an e-residency grants its holder several rights unbeknownst to, or at least unapplied in majority of the EU Member States and in the world at a larger scale. Being an e-resident of Estonia, one can use the digital services of that country even if there had beforehand been no prior connection to Estonia, provided the potential e-resident shows legitimate interest. The digital services include possibility to digitally sign documents (legally enforceable in any EU Member State), do online banking, encrypt documents, as well as establish and manage a company in Estonia and declare its taxes online via the state-proven digital identity card issued and backed by the Estonian government. Given chapter scrutinises the perception of e-residency and discloses the problematical unbalanced aspects of it, pointing out that although secure from technical point of view, e-residency lies on a defective concept and conflicting Estonian national regulatory framework that does not fully support the integration of the idea.

## 1. Introduction

In October 2014, as a response to Apple's introduction of a possibility to sign PDF-documents using a trackpad, the Prime Minister of the Republic of Estonia, Taavi Rõivas, posted a bold tweet on his Twitter account, stating: "Dear Apple, If you are interested in how files are really signed digitally, contact any Estonian. Best rgds, Taavi."[1] Indeed, the people of Estonia are e-conscious – as of 3 May 2015, 214 363 679 Estonians have active ID Cards, which have been used for electronic authentication as many as 344 654 526 and for signing documents digitally 214 363 679 times.[2] As there are approximately 1 320 000 Estonians, this means that roughly 95% of Estonians really do know how files are signed digitally. Using their ID-cards and e-solutions available, Estonians lead a digital lifestyle - in 2015, 96% of taxpayers declared

[1] Hereinafter web links available at the end of Chapter in the References list.
[2] Statistics from Official ID-card and Mobile-ID portal.

their taxes electronically,[3] 99.6% of the bank transactions are being done online[4] and 33% of eligible voters e-voted during the 2015 national parliamentary elections.[5] The confidence of the citizens appears to be further supported by the fact that Estonia is among the most wired and technologically advanced countries[6] having freedom of speech and expression protected by the Constitution[7] and Internet established as a human right.[8]

Simultaneously listed amid countries with lightest content restrictions, Estonia appears to be in a digital fairy tale – with its numerous e-government services, the country is regarded a "model for free access as a development engine for society."[9] This is supported by facts from the European Digital Agenda country Scoreboards placing Estonia to the forefront in offering and using digital public services,[10] as well as by reputable media issues worldwide declaring Estonia to be "a leader in technology," "a place where cyberdream is already reality," and "a country famed for its digital infrastructure."[11] Other governments yearn for Estonian best practices, too – towards the end of the year 2014, a novel union was formed by representatives of the Republic of Korea, the UK, Estonia, New Zealand and Israel by a mutual agreement to establish a network called D5, comprising of the most digitally advanced governments in the world, with the common goal to share best practices and make the digital governments of the participating states more efficient.[12] Estonian rapid developments with regard to e-solutions and digital infrastructure are undeniably sought-after.[13]

---

[3] In fact, Estonia adopted the system of electronic declarations in 2000; 3% of the people declared their taxes online back then, within 15 years, this number has increased by 94%. Statistics from Estonian Tax and Customs Board Yearbooks.

[4] Estonian Information System Authority.

[5] Statistics about Internet Voting in Estonia from Estonian National Electoral Committee. For more information see, for instance, Madise, Ü. and Vinkel, P. Internet Voting in Estonia: From Constitutional Debate to Evaluation of Experience Over Six Elections. Regulating eTechnologies in the European Union. Normative Realties and Trends. T. Kerikmäe (ed.) Springer, 2014, pp 53-72.

[6] Freedom House Freedom on the Net 2014. Estonia country report.

[7] § 45 of the Constitution of the Republic of Estonia.

[8] Pursuant to §44 of the Constitution, Estonia, everyone is entitled to free access to information disseminated for public use; it is laid down by the Public Information Act, §33, that "Every person shall be afforded the opportunity to have free access to public information through the Internet in public libraries, pursuant to the procedure provided for in the Public Libraries Act."

[9] Freedom House 2014 Freedom of the Net Estonia report.

[10] Digital Agenda for Europe. Progress by country. Estonia Scoreboard.

[11] See for instance, the Economist explains: How did Estonia become a leader in technology? The Economist. 30 July 2013, by A.A.K, describing Estonia as having a "strong tech culture." As well as "Digital identity cards. Estonia takes the plunge." The Economist. 28 June 2014. Furthermore, Elisabeth Braw, "'E-stonia' Attempts to Become the Uber of Economies by Introducing Virtual Residency." 30 October 2014. Newsweek, etc.

[12] "The D5 will provide a focused forum to share best practice, identify how to improve the Participants' digital services, collaborate on common projects and to support and champion our growing digital economies." The D5 Charter.

[13] Another Estonian success story is the Data Exchange Layer X-Road that was launched in 2011 to enable secure Internet-based data exchange between the state's information systems. President Ilves has claimed that the system was adopted merely because Estonia was too *poor* to afford a central server. In 2013, Finland and Estonia signed a MoU on cooperation in the field of ICT, one of the objectives of which was set implementing the source code of

Recently Estonia opened up its digital borders to anyone legitimately interested in the country's e-services – this small, yet tech-savvy European Union Member State has become the first country in the world to have rendered accessible some of its e-government and private sector e-services to non-Estonians in the form of something now known as e-residency – the Estonian equivalent to digital identity. Within first month and a half, 650 applications were filed and 463 e-residencies issued. Majority of applications came from Finland (239), Russia (118), Latvia (39), the United States (36) and the United Kingdom (24); but e-residency had raised fascination across the world – numerous applications were additionally submitted from unanticipated countries, such as Venezuela, Sri Lanka as well as from Mexico.[14]

The intent of this chapter is to familiarise the reader with the innovative concept of e-residency from three different angles. The first viewpoint presented in the second section of given chapter provides an overview of the concept itself, including the technological basis, objectives for Estonia and expectations from the e-resident. The third main division scrutinises the Estonian national regulatory framework with regard to issuing the e-residencies; subdivisions present the clash between e-residency and Estonian legislation and indicate the discrepancies between e-residency and the EU principles of data protection. The fourth section seeks and provides an answer to the question whether the e-residency is the key to sought-after global digital identity management. Therewith, the purpose of the next pages is not to offer solutions to the various problematic aspects of e-residency, but rather to initiate critical discussions and provide food for thought for further analyses.

## 2. The concept of e-residency outstretched

As stated above, Estonian technological advancement has been noted internationally. Estonian citizens and residents are privileged in being able to manage most of their public and private affairs digitally. The plan to share that privilege with the rest of the world was presented in the Estonian Development Fund competition and the price-winning development idea was titled "10 million e-Estonians by 2025."[15] The concept of e-residency was born and thus it had

the X-Road for practical use in Finland as a national data exchange layer. Another interesting fact is that the same MoU was the first international intergovernmental digitally signed agreement.

[14] The Minister of the Interior of the Republic of Estonia, Mr Hanno Pevkur at 05.02.2015 weekly press conference of the Government of the Republic of Estonia. It must be noted that up-to-date statistics on the number of applicants and e-residencies issued is not available to public.

[15] The idea was introduced by Taavi Kotka, Ruth Annus and Siim Sikkut. Estonian Development Fund is a public institution subject to the Parliament investing in innovative companies for the purpose of contributing to Estonian economic development.

to be introduced to the wider public: "E-resident is a foreigner, to whom Estonia has created a digital identity based on identity of the country of citizenship and issued a digital identity card – digital-ID of an e-resident."[16] To give a more tangible framework to the innovative idea, the Digital Agenda 2020 for Estonia designated the opening of Estonian "secure and convenient services" to foreign nationals as one of the priority initiatives of the named strategy.

Impetus for Estonia? – Apparently, the country is aspiring to become as renowned for its e-services as Switzerland is for its banks.[17] Accordingly, the Digital Agenda 2020 for Estonia puts down the intent to retain the image of a tech-savvy country, whereas the concept of e-residency is emphasised as being one of the key factors in achieving that goal.[18] However, issuing digital identities is not only about Estonia's reputation but has a multifaceted effect. In addition to marketing Estonian e-services, the legal foundation for the e-residency – the Identity Documents Act of Estonia – introduces as the objective of the issuing of e-residencies the advancement of Estonian "economy, science, education or culture by providing access to e-services with the Estonian digital document;"[19] and thirdly, as laid down by the Concept, the e-residency programme further ought to contribute to enhancement of the policy of Estonian compatriots programme supporting Estonians and Estonian culture abroad.[20] Here it remains inscrutable whether the incentives are indeed systematically organised layers of a deliberate compound programme, or the concept of e-residency has been "squeezed in" to any more or less agreeable initiative to justify its existence.

### 2.1. Technological basis (PKI)

Due to the fact that Estonia already had a functioning system for digital identity documents, it was not seen as a technological impediment to effectuate a system of secure digital ID-cards

[16] Issuing digital identities to non-residents: creating e-residency. Concept. Appendix to explanatory memorandum to draft legislation of Estonian Identity Documents Act and State Fees Act. Appendix 1." [Mitteresidentidele digitaalse isikutunnistuse väljaandmine: e-residentsuse loomine. Kontseptsioon. Isikut tõendavate dokumentide seaduse ja riigilõivuseaduse muutmise seaduse eelnõu seletuskirja juurde. Lisa 1.] 2014. Available only in Estonian. Hereinafter referred to as the Concept.

[17] Digital Agenda 2020 for Estonia.

[18] The Digital Agenda 2020 has submitted amongst its objectives the maintaining of Estonian image as a technologically advanced country and well-developed information society as well as creating awareness of e-Estonia in the world.

[19] Identity Documents Act of the Republic of Estonia. § $20^5$. E-resident's digital identity card. Hereinafter referred to as IDA.

[20] The supporting of Estonians and the Estonian culture abroad is organised through the national compatriots programme led by the Ministry of Education and Research and implemented in cooperation with the Ministry of Culture and the Ministry of Foreign Affairs.

for e-residents.[21] The idea of prior existing ID-cards itself was first introduced in 1998 and in January 2002, first ID-cards were issued to citizens.[22] The chip embodied in the national ID-cards and now also in the digital ID-cards of e-residents uses a 2048-bit public key encryption (the old versions of the card had a 1024-bit version), which confirms the definite proof of the identification in any electronic environment supporting the Estonian system.[23] Insofar as the e-resident's ID-card functions as an authentication tool similarly to citizens' and residents' ID-card, it is a national state-backed Public Key Infrastructure (PKI), which means that the state undertakes to assure its existence and functioning.

The Public Key Infrastructure (PKI) is the literal key for the secure authentication and digital signing. The key can be referred to as a sophisticated code kept on the electronic chip of the ID-cards (both Estonian national ID-cards and the novel e-residency digital identity cards).[24] This is subsequently comprised of two parts, i.e., two keys: a public encryption key and a private decryption key. To exemplify, the digital signature is created in combination of the two – first, by using the data necessary for giving the signature that is contained in the a secure signature creation device – *the private decryption key;* and second, by using the data that is needed for verification of that signature and uniquely corresponds to the first – *the public encryption key.*[25] There are two certificates[26] within the contact chip or microchip of the card which can be used for authentication and digital signatures respectively, whereas by using the same software that is compatible with Estonian ID-cards.[27] Therewith, the card can be used for digitally signatures and authentications by installing the necessary software and using either an ID-card reader attached via USB to a computer (some have built-in hardware) or a Mobile-ID whereat the users can sign in without a card reader, by only using one's phone. The card works on two-factor authentication – in order to access a digital service or to sign digitally, secure PIN codes previously provided to the e-resident, must be entered.

The other part of that set of two keys is kept in the public part of the chip, which means that the ID-card readers, whether installed in the hardware or separately attachable by a USB cable, access system card readers, web services or any other ID-card based application that can read that information. The certificate that has been place in this part of the key, including the personal

[21] The Concept, supra nota 16.
[22] Chronology of ID-Card from the Official ID-Card and Mobile-ID portal.
[23] Electronic ID-Card information from E-Estonia site.
[24] Public Key Infrastructure. PKI. Estonian Information System Authority.
[25] § 2 (2) of the Estonian Digital Signatures Act.
[26] A certificate is an electronic certification that binds the data necessary for certifying the authenticity of the person and the digital signature with a person and certifies the identity of the person. See more from the ID-card and Mobile-ID Portal "What are certificates."
[27] IDA, Supra nota 19. § $9^4$. Entry of certificates in document.

data, is the electronic proof accessible via the PKI.[28] The secret key of the set is saved in the protected part of the chip and can only be accessed by the PIN-codes which were given to the owner. To illustrate: the public and private key are in mathematical connection but it is not, however, possible to derive the private key on basis of the public key. The information encrypted by the public key can only be unencrypted with the personal secret key which means that the confidential message is only readable by its addressee. Therefore, by authenticating oneself with the ID-card, the web server sends the owner a session key that is being encrypted with that person's public key and can only be encrypted with that specific authentication key (inserting the PIN).[29]

The further, perhaps more easily conceivable security aspect lies in the fact that merely knowing other persons PIN-codes will not suffice to abuse the ID-card – the physical possession of the ID-card is required to authenticate oneself for the purposes of using the e-services. This works vice versa as well – if the physical card gets into wrong hands, the e-services are still not available if the public key infrastructure cannot conform the validity of the certificates. Moreover, the chip on the card has a counter of wrong entries which means that the PIN will be blocked after three erroneous attempts to identify oneself (and it can be unblocked by a PUK-code).[30] The possible attacks on the system can include, for instance, the specifically designed malware which could imitate the utility or plugins in the browser attempting to redirect the users who has authenticated oneself or tries to change the details of a bank transfer. However, both of these presume that it is the computer that is compromised, not the e-ID system.

With a view to future developments and taking into account what Estonia has already achieved at national level, the near future will enable the use of Mobile-IDs[31] outside of Estonia. Once the e-resident exchanges the existing SIM-card with the PKI-capable one (meaning that enabling the use of Mobile-IDs requires a contract with an Estonian mobile network operator), the authentication and verification of digital identities via a mobile phone offers the same potentiality and quality as it is through a computer – only more convenient - the authentication and giving digital signatures will no longer be dependent on having access to a computer alongside with an ID-card reader and the software, it will suffice to have access to a mobile phone (does not necessarily have to be a smartphone) or a tablet. Mobile-IDs provide the same

[28] §5 (1) of the Digital Signatures Act: „ ... a certificate is a document which is issued in order to enable a digital signature or digital seal to be given and verified and in which a public key is uniquely linked to the certificate holder."
[29] ID-Card. Computer protection. Information security signpost. [ID-kaart. Arvutikaitse. Infoturvalisuse teeviit.]
[30] *Ibid*.
[31] About Mobile-ID from the official ID-card and Mobile-ID portal.

access to the services by remembering the PIN codes 1 and 2, and the data exchange takes place over an encrypted connection, which thus ensures the same level of security.[32]

### 2.2. Political aim

An e-resident will receive an identification card which, however, does not have a photo on it, and thus it cannot be used as a travel document, for instance. Accordingly, an e-resident's identity card is first and foremost a digital document[33] embodying a variety of e-services which are opened to the new e-resident in the form of the ID-card bearing a microchip with security certificates similar to national ID-cards.[34] The focus point is that irrespective of the nationality and whatever the digital service, an e-Estonian can authenticate oneself with just a few clicks. Until the first e-residency was issued towards the end of 2014,[35] only citizens of some other EU Member States who operated a digital identification system similar to Estonian were able to authenticate themselves in the same way (access was granted for specific services exclusively, e.g., the e-Business Register) as those owning an Estonian ID-card. However, due to minimal number of such ID-cards and their users in the rest of the EU[36] (Estonia accepts the certificates of Belgium, Finnish, Portuguese and Lithuanian ID-Cards since 2008), as well as considering that there was no effective solution for involving third country nationals, it was perceived that the Estonian economy, culture, education and science could not be advanced sufficiently without foreigners taking up the use of Estonian digital services and hence the e-residence was created as a solution addressing the issue.[37]

This is explicated in the concept of e-residency which marks attracting and involving foreign expertise and investment as the only possibility (if not a prerequisite) for Estonia in today's globalised world where economic, political and cultural development is mostly based on international communication and cooperation.[38] The drafters[39] of the Concept stipulated that

[32] Martens (2013) p. 217.
[33] IDA, supra nota 19, § $20^5$. The Identity Documents Act differentiates between a digital identity card §2 ($1^1$) and a digital document prescribed for digital identification of a person §3 (3).
[34] *Ibid*, § $20^2$. Digital data to be entered on digital identity card.
[35] The first e-resident was the British journalist, Senior Editor to the Economist Magazine, Edward Lucas. See, for instance, his foreword to the e-Estonia newsletter.
[36] Estonian ID card and e-ID are actually quite similar to Belgium card. See Martens (2013) p. 216.
[37] The Concept, supra nota 16, p 4.
[38] *Ibid*.
[39] The proposals in the concept were developed in joint effort of representatives from Estonian Ministry of the Interior, Republic of Estonia Government Office, Ministry of Economic Affairs and Communications, Information System Authority, Police and Border Guard Board, Estonian Internal Security Service, Estonian Tax and Customs Board, Certification Centre, with consultations from other interested parties.

the contribution of such experts ought not to be dependent on their physical location, and therefore the e-residency would be a perfect solution for giving interested foreigners the possibilities to participate in everyday affairs with digital solutions equal to those available to Estonian citizens and residents, without actually having to be physically present.[40]

What concerns the compatriot policy, the instigators of e-residency see it as an appropriate medium for keeping emigrant Estonians in connection with their roots by offering the possibilities to get access to digital services regardless of their citizenship or state of residence. It is laid down: "insofar as the Estonian identity is first and foremost based on language and culture deriving from it, the Estonian language based communication with emigrant communities in other states becomes important […]. Thus the probability that current emigrants as well as second and third generations will maintain their connection to Estonia, some of them returning to Estonia or keeping cross-border connections, will increase."[41]

By receiving a verifiable digital identity and a digital ID-card, the e-resident becomes identifiable with an ID-card and can authenticate oneself as well as provide digital signatures in an electronic environment instead of physical signatures or facial recognition. Which in turn means access to digital services offered by Estonia, as well as, in the near future, use of electronic identification and trust services in cross border electronic transactions within the EU Digital Single Market.[42] Even though some services of the private sector, such as internet banking, telecommunications operators self-service, etc., alongside with, e.g., Eesti.ee (Estonian Point of Single Contact[43]), Estonian Tax and Customs Board, are accessible online without the ID-card via a bank link, this is not as secure nor as convenient as is access with the digital ID-card authentication.

### 2.3. Ambiguities of the concept

At the moment, the list of possible (non-exhaustive) users for utilisation of the "regular" ID-card include private and public services, e.g., access to governmental institutions, e-voting, e-school and e-kindegarten, banks, university study information systems, telecommunication and internet service providers, insurance, e-health system, etc.; yet not all of them are accessible

[40] The Concept, supra nota 16.
[41] *Ibid*, p 6. This argument is based on an analysis on multiple citizenship, conducted by the Ministry of the Interior in 2013. [Mitmikkodakondsus. Analüüs. Siseministeerium 2013].
[42] The Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation).
[43] The Points of Single Contact (PSCs) are e-government portals for entrepreneurs active in the service sector. It is a legal requirement to have a PSC in each EU country since December 2009 as set out in the EU Services Directive.

with the e-resident's ID-card.[44] E-residency card of digital Estonia, however, opens the virtual doors to registering a company online (via the Business Portal); signing documents digitally; exchanging encrypted documents; doing online reporting to business register; conducting secure online bank transfers[45]; declaring taxes online; submitting annual reports online; digital prescriptions in Estonian pharmacies.[46] The potential users of such services have been set forth in the Concept:

- Foreign investors and the employees of companies founded by such investors;
- Foreigners who are taking part in the management of such companies (in the managing board or council), or participate in the venture;
- Foreign experts and employees in Estonian companies;
- Foreign clients and partners of Estonian undertakings;
- Foreign researchers, scholars, students;
- Representatives of other states and international organisations in the Republic of Estonia (e.g., NATO Cyber Defence Centre of Excellence, EU IT Agency);
- Family members of the aforementioned persons.[47]

Assessing the target group and the threefold objective for issuing e-residencies, i.e., 1) attracting people to use the country's e-services, 2) boosting Estonian economy, educational, scientific and cultural development by taking the services to an international arena, and 3) pursuing the compatriot policy, the concept comes across a bit diffusive. It is apparent that the focus is almost entirely on people with a financial interest in Estonia. As there is no mention of former Estonian citizens who have emigrated, the aim of contributing to the compatriot policy becomes obsolete.[48] Retaining that by using Estonian e-services via the digital identity card, an e-Estonian is imposed with the responsibility to contribute to the development of Estonian economy, culture, education or science, it seems that this specific objective is not too forethoughtful. – Apart from foreign researchers, scholars and students, it is difficult to find a target group who would promote Estonian culture, science or education. Simultaneously, the evaluation criteria indicating the assessment of increase of respective aspects is undefined or merely not made public – it is not explained how should the e-Estonian prove that due to the

[44] These are listed as possible uses of ID Card. For more, see the ID-card and Mobile-ID official portal.
[45] An e-resident *may* be eligible to open a bank account in Estonia, however, it still requires a physical visit to Estonia, to the bank, and does not guarantee the opening of a bank account as it is up the bank to make the decision.
[46] Services for the so-called hassle-free transaction of affairs, see more at the e-Estonia website.
[47] The Concept, supra nota 16, p 6.
[48] To overly criticise, it seemed obsolete from the beginning. If the aim of the compatriot policy is to increase *communication* in Estonian language between migrant (ex)citizens, e-residency is surely not the tool.

activism of him or her using Estonian e-services, the level of science would be raised by a certain percentage; and considering that the e-residency is not an infinite benefit, it is not clear how should the e-resident indicate the contribution to increase of Estonian development, in order to avoid being subjected to revocation of the e-identity.[49] It is quite apparent that the most desirable e-resident is a business oriented person, boosting foremost the economic development.[50] This is, of course very remunerative for local businesses – engaging in business relationships with foreign colleagues and investors via digital and legally effective communication; and, of course, a thrust for the Estonian economy. Yet the added value of using e-services to scientists, artists or academic persons remains, at least at this point, ambiguous.

## 3. The conflicting regulatory framework

Estonia is undeniably leading a digital way of life and disclosing this lifestyle to foreign nationals. Although the same safe software is used for Estonian citizens', residents' ID-cards and for the e-residents' ID-cards, the digital identity of an e-resident is distinguishable from the digital identities of the former two by the certificates. Hence ensuring that by having the digital identity, the legal status of the person using the e-services remains legible.[51] Consequently, the service providers can separately monitor the use of e-residents' digital identifications or to restrict access to them whenever necessary. Even though e-services that are meant for citizens only – for instance, e-voting – are not accessible to e-residents which is made clear at authentication, providing a digital identity still requires scrutinising the applications and e-activity of the e-resident to see whether or not a person is a suitable candidate for becoming an e-Estonian and whether the person who has already received the e-residency, is using it judiciously.[52]

As is oft emphasised in the introductory concept of e-residency, it must be born in mind that the digital identity of an e-resident is a benefit, not a right,[53] implying that the Estonian officials deciding over its issuing can require something from the person seeking to have a

[49] Pursuant to IDA, supra nota 19, § $20^6$ (4), the card may be revoked if the basis specified in subsection (1) i.e., having a relationship with the Estonian state or legitimate interest in the use of e-services of the Estonian state, of this section ceases to exist.
[50] The Ministry of Economic Affairs and Communications introductory page to e-residency, under title „Why are we doing it?" declares – „Registration of businesses will bring investments to Estonia and create jobs and will thus accelerate the economic growth." Nothing about culture, education or science.
[51] The Concept, supra nota 16, p 4.
[52] *Ibid*, p. 12.
[53] *Ibid*, Section 2.1. Underlying Principles [Aluspõhimõtted].

digital liaison with Estonia, and can take the privilege away if the e-resident's activities do not comply with Estonian regulations or codes of conduct. The Estonian Identity Documents Act formulates the prerequisites for obtaining e-residency – the person applying for an Estonian digital identity must either have "a relationship with the Estonian state" *or* "legitimate interest in the use of e-services of the Estonian state."[54] Even though the Act sets forth the criteria of legitimate interest or previous relationship, it does not elaborate on the principles and leaves both open to interpretation. Previous relationship [in Estonian: "eelnev seos"] has an implausibly wide scope and could mean anything from a visit to Estonia to formerly renounced Estonian citizenship. By the same token, it is rather challenging to identify a legitimate interest to use the e-services if there is no formal way of formulating it.

### 3.1. Issuing, suspending, revoking the e-residency applications

The procedure of dispensing digital identity cards foresees that the potential e-resident has to substantiate legitimate interest in the form of a written statement or other proof laying down the intent and circumstances of use[55] (the assessment of which, is, in fact, not defined anywhere) or a prior connection with Estonia (not defined, either), as well as provide the Estonian Police and Border Guard Board with personal data (including sensitive data, i.e., biometrical data).[56] Subsequently, the application undergoes a review and processing of the information handed to Estonian officials from the Police and Border Guard Board in order to establish whether the applicant would be a proper Estonian e-citizen. Thus, it is the Police and Border Guard Board who has the right to decide over the application,[57] identify and verify the person,[58] as well as exercise state supervision over issued e-residencies together with the Estonian Internal Security Service and the Estonian Tax and Customs Board.[59] Even though at the launch of the e-residency programme, the applicant was obliged to travel to Estonia twice (once, to submit the application and identify oneself, and for the second time in order to obtain the document –

[54] IDA, supra nota 19, § $20^6$ (1). Conditions for issue, suspension of validity and revocation of e-resident's digital identity card.
[55] §$10^2$ (1) of Regulation of the Government of the Republic laying down the list of certificates and information to be submitted upon application and terms for the issue of an identity card, a residence permit card, a digital identity card, an Estonian citizen's passport, a seafarer's discharge book, a temporary travel document, a travel document for a refugee or a certificate of record of service on ships.
[56] IDA, supra nota 19, § 9. Standard format of documents and data entered in documents.
[57] IDA, supra nota 19, §$11^1$. Identification of person and verification of identity upon issue of document; § $12^1$. Issue of document; §15 Organisation of issue and revocation of document, (4). See also Estonian Ministry of the Interior website.
[58] *Ibid.* §$20^9$. Identification of person and verification of identity of e-resident.
[59] *Ibid.* §$20^8$. Exercise of state supervision. See further Chapter 6 of the Estonian Aliens Act.

identity documents cannot be posted), from April 1, 2015 it has been made possible to apply in Estonian embassies and consular offices in 34 countries, whereas applications are still sent to Estonia for review.[60] After submitting the application, the Police and Border Guard Board is granted the discretion to decide upon the issuing of e-residency to the applicant.[61] During the evaluation of the eligibility of the candidate and even after the issuing, for the purpose of follow-up monitoring, the Board officials can exercise the authority to check the reliability of an e-resident from all accessible sources, whereas they can involve relevant institutions and make inquiries into necessary data collections for verification of identity, process data without prior notification or consent.[62]

At the stage of application, whereat the Police and Border Guard Board is responsible for receiving the information from the application on the reason for applying, it is an intricate task assigned for the Board to determine whether that specific applicant, by using Estonian e-services (e-prescription or banking system, for instance) will be able to contribute to Estonian culture, education, science or economy. Starting from the latter, it is perhaps the easiest to decide upon the economic aspect – if the applicant proclaims that the legitimate interest is establishing a business in Estonia – this most likely enhances the business environment and possibly even economy. However, it must be awfully difficult, if not possible for the Board to determine whether the fact that a person who has twice visited Estonia (and thus has previous relationship with Estonia?) will be able to promote the country's culture, education or science. Thus it appears that the tasks concerning evaluation of the effect of the e-resident's use of e-services are in general uncharacteristic to the work of Estonian Police and Border Guard Board.

Moreover, in view of the aforementioned, if the Police and Border Guard Board accepts, handles the inquiries, decides upon issuing and exercises control over the applications[63], the institutional capacity of the Board must be increased to face the amplified working load. With that regard, it must be emphasised that there is a very obvious discrepancy between what the Digital Agenda 2020 for Estonia has laid down and what the developers of the idea had in mind in terms of number of e-residents. The former set a goal of 5000 e-ID cards issued to non-residents,[64] by 2020, which would roughly mean a thousand new e-residents per year. The latter

[60] IDA, supra nota 19, §$20^7$ ($1^1$). Additionally, after May 13, 2015, an online application site should be opened, which would mean that only one visit to the consular office, embassy or Estonian Police and Border Guard Representation is necessary for obtaining the document.
[61] *Ibid*, §§ $20^6$ and $20^7$.
[62] The Concept, supra nota 16, p 9.
[63] Even if initially submitted to foreign missions, the applications are referred to examination to the Board officials in Estonia.
[64] Digital Agenda 2020 for Estonia, p 30.

goal, namely 10 million e-Estonians by 2025, would either indicate that within the remaining five years there would be an additional 9 995 000 e-residencies issued or a "less intense" division over 10 years, i.e., a million new e-residents per year. A simple calculation shows that between the period of 1 December 2014 until 31 December 2024, this would entail issuing e-residencies for roughly 2 715 people per day, i.e., in case of a 24-hour working-system, including full time on weekends and public holidays 113 people per hour. With the abovementioned pace at 463 e-residents per month and a half, not only the goal will not be achieved unless the institutional capacity is enormously increased, but the concept itself must be made more attractive to receive more than 600 application within 36 days.

### 3.2. Legal certainty for e-residents

The fact that a relationship with Estonia or legitimate interest are prerequisites of becoming an e-resident, whereas it is not clearly indicated what those are, refers that the Estonian system can be considered to lack complete articulation and contain regulatory ambivalences. The Estonian Identity Documents Act has left much discretion for interpretation in terms of to whom the e-residencies and under which circumstances are issued which may create obscurity in terms of legal certainty of the e-residency candidates and e-residents. Even though marketed as the key for using Estonian e-services, the Concept provides that there is no ubiquitous access to what Estonia offers its residents and / or citizens. The e-residents can be bound by limits that private sector service providers choose to impose on accessing their services.[65] Therefore, on the premise that a service provider deems it more appropriate to offer its facilities only to residents and / or citizens, there is a discretion to leave the e-residents out of the scope of their services. In addition, the official explanatory concept lays down that it is plausible, in duly justified cases [põhjendatud juhtudel] to limit the access of e-residents to public digital services or to set forth additional preconditions, which help to reduce the risks accompanying e-residency.[66] The aforementioned combined means that the e-resident cannot and perhaps should not expect unlimited access to the realm of e-Estonia.

In accordance with the Identity Documents Act and pursuant to the Concept[67], the legal status of an e-resident is similar to the status of an alien and is analogous to the situation of issuing a visa – there exists no subjective right to stay in Estonia nor a right to obtain an identity

[65] The Concept, supra nota 16, p. 8.
[66] *Ibid*, p. 8.
[67] The Concept, supra nota 16, p. 10.

document from Estonia. Furthermore, the issuing, refusal to issue or exercising supervision does not require further reasoning on behalf of the state.[68] Thus, it is emphasised that neither the latter mentioned actions nor suspension of validity or exercising state supervision can violate "*a non-existing fundamental right or freedom*" insofar as the situation of an e-resident is analogous to that of a person on temporary stay.[69] This leaves the legal status of the e-resident abstruse – that he or she is not a resident nor a citizen of Estonia, is clear; however, having received a digital identity and an identity number based on which that person can be identified through the use national public key infrastructure should give that person a fiduciary relation with Estonia beyond that of an alien on temporary stay. On top of it all, the authors of the Concept must have failed to understand the meaning of fundamental rights and freedoms.

### 3.3.More security – less privacy?

As outstretched in the preceding section, the Police and Border Guard Board, to whom the e-residency candidates submit (via embassies) the personal data, decide over the granting of the e-ID by identifying and verifying the applicant and assessing their justification of interest. The potential digital resident submits to the Estonian authorities the standard format of documents and data (including biometric data[70]) that is also required for issuing national identity documents, i.e., passports and Estonian identity cards that can be used for physical identification, e.g., for travelling purposes. In accordance with Estonian law, the identity documents together with the data submitted are stored in a specific Government established database, the purpose of which is to "ensure the interior security of the state by keeping record of the identification of persons and the issue and revocation of identity documents."[71] Services accessed with digital authentication via the X-Road system are stored in state information system databases which are interfaced with the data exchange layer of the state information system.[72]

The data processed in IT systems are secured by three-level IT baseline security system (ISKE) which was specifically adapted for Estonian public sector based on a German information security standard – IT Baseline Protection Manual (IT-Grundschutz in German) – and is mandatory to be followed by state and local government institutions handling

[68] *Ibid*, pp 10-11 and the IDA, supra nota 19, § $20^7$ (3).
[69] The Concept, supra nota 16, pp 11-12.
[70] IDA, supra nota 19, §9.
[71] *Ibid*, §$15^2$.
[72] Public Information Act, § $43^2$. State information system.

databases/registers.[73] Pursuant to ISKE, there are three levels of security, low (L), medium (M), and high (H). The information stored in the identity documents database has the highest security level (H). As explained in section 2.1. regarding the technological basis for the e-IDs, there is one single authentication system that has proven to be secure and reliable for both, national identity cards as well as for e-residents. Nevertheless, on top of this, in order to support the system of digital identities and ensure its integrity at the core, biometric data of all individuals who have applied for or own Estonian identity cards, irrespective whether they are national identity documents or digital identity documents meant exclusively for e-identification, are stored on digital database cards, archived and retained for 50 years[74] (in case of e-residency, this is done to avoid conferring duplicate identities to one person[75]).

The integration of biometric features in passports and travel documents is being done in accordance with the EC Regulation 2252/2004;[76] whereas the pressure for the EU to introduce the biometric passport in the first place came from the US Government in their context of "war on terror,"[77] *inter alia* for aligning the Member States' legislation with the US relevant legislation for the purpose of being eligible to participate in the United States Visa Waiver Program in order to allow the EU nationals to enter the US territory without a visa.[78] From the perspective of e-residents, this is immaterial – the digital identity documents issued do not serve as travel documents, as has been established above. Nevertheless, due to the fact that under the Estonian Identity Documents Act, the term "digital identity card" denotes both the e-IDs of nationals as well as e-residents' e-ID cards, the requirement of biometric identifiers also applies to both.

Drawing on the aforementioned, the authors of given chapter claim that the failure to differentiate between the two types of documents leads to unnecessary collection of biometric data that is in contradiction with the Data Protection Directive Article 6 principles of purpose and proportionality[79] (Article 5 in the draft Data Protection Regulation[80]). Article 29 Data

[73] Government Regulation No. 252 of 20.12.2007, Information systems security measures sytem [Infosüsteemide turvameetmete süsteem]. Only available in Estonian. For and overview in English, please see the Information Systems Authority website.
[74] Government Regulation No. 109 of 03.07.2008, Statutes on maintaining the database on identity documents. [Isikut tõendavate dokumentide andmekogu pidamise põhimäärus] §§4 and 18. Only available in Estonian.
[75] The Concept, supra nota 16, p 9.
[76] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.
[77] Goncalves and Gameiro (2012) p. 324.
[78] Background to Regulation 2252/2005, available at EUR-Lex.
[79] Directive 95/46/EC.
[80] Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM(2012) 11 final.

Protection Working Party has acknowledged that the increased use of biometrics presents specific data protection risks which are further increased if biometric identifiers are kept in external databases, whereas if there are alternative less intrusive means available, biometric data should not be used.[81] They have accentuated that there should at the outset be clear determination for which such data will be used and subsequently the taking of personal data should not be excessive in relation to the purposes for which they are collected, "[i]n other words, authentication/verification applications which can be carried out without a central storage of biometric data should not implement excessive identification techniques." [82]

Bearing in mind that the e-residents' identity card is only valid for digital identification and not for physical identification, the requirement for biometric data seems to be straightforwardly unreasonable and disproportionate and Estonian legislation on e-residency contradicting the aforementioned assertions from every angle. The necessity of the use of biometrics for physical identifications as prescribed by the EU regulatory framework should not extend to digital identification; various authors have avouched that even for use in travel documents and passports, the advantages of biometrics are often overshadowed by subsequent storing of the data that results in nonrepudiation use of biometrics, such as increased levels of control and surveillance, leading to a "so-called big brother scenario,"[83] or to a "global police state."[84] In case of e-residency, the justification for using biometrics is to avoid granting duplicate identities, as stated above. At present it can only be speculated whether or not this is proportional and purposeful.

The authors contributing to the previous volume of this book have analysed the various challenges and novel problems with respect to privacy and protection of personal data for national and supranational legal systems in terms of intensified digitalisation and technological innovations adapted for e-governance systems.[85] Dutt and Kerikmäe, who provided introspect to the concepts and problems associated with e-Democracy saw "a secure, private and safe online identity for citizens" to be one of the key aspects for e-Democracy to succeed "as a more pivotal feature of democracy."[86] However, juxtaposing the secure multi-layered technological

[81] Article 29 Data Protection Working Party. Working Party on Police and Justice. The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, pp 14, 26 and 27.
[82] Article 29 Data Protection Working Party. Working document on biometrics, p. 6.
[83] Schouten and Jacobs (2009) p. 311.
[84] J. Ashbourn (2005) p. 20.
[85] See the contributions of, for instance Katrin Nyman-Metcalf, Ülle Madise, Priit Vinkel, Pawan Dutt, Agnes Kasper, Addi Rull, Ermo Täks and Alexander Norta in Kerikmäe, T. (ed). Regulating eTechnologies in the European Union. Normative Realities and Trends. Springer International Publishing Switzerland. 2014.
[86] Dutt and Kerikmäe (2014) p. 294.

infrastructure encircling the e-IDs with yet another security technology – the biometrics – there is a possible reverse effect to (e-)democracy. It has been ratiocinated that giving too much leeway to new technological developments without proper analysis of the fundamental rights perspective, the (often) subtle multiplication of security measures may pose an ultimate risk to democracy instead.[87] Biometrics as security technology cannot be "thrown in" for good measure, as Estonia seems to have done, without proper analysis of risks for protection of fundamental rights and freedoms, not considering whether the purpose to be achieved could not be achieved by less intrusive means.

Ten years ago, Ashbourn condemned biometrics-favouring governments, referring to them as having "rushed headlong into what can only be described as a frenzy of biometric related initiatives accompanied by clouds of emotionally misleading and technically incorrect rhetoric."[88] Even though innovative identity verifications pose interesting technological challenges – he wrote – we should not act as children playing with technological toys.[89] Prior to introduction of e-residency, Nyman-Metcalf, a notable e-governance expert, professed, when considering legal framework of e-governance, including the future of digital identities, that fields such as e-signatures or e-identification demand special or specifically customised existing legislation for their proper regulation.[90] She emphasised that law is the background against which to assess the applicability of new technological developments.[91] Estonian way for "making room" for e-residency within the Identity Documents Act is not precisely in harmony with the range of prospective challenges to violation of use of biometrics but rather resembles attempts to play with that technological toy. Thus, from legal point of view, it looks like the introduction of the concept was pushed through too abruptly, not fully considering the multitude of facets surrounding e-residency.

## 4. Can e-residency create a global digital citizen?

Despite the contradictions presented in the preceding sections, the e-residency concept in itself is innovative and unforeseen, corresponding to the need for a cross-border recognition of digital identities - it has been noted that due to ongoing technological developments and enormous increase in information flow, secure and reliable dissemination of information,

[87] Goncalves and Gameiro (2012) pp 322-323.
[88] Ashbourne (2005) p. 21.
[89] *Ibid*.
[90] Nyman-Metcalf (2014) p. 41.
[91] *Ibid*, p. 34.

especially what concerns digital verification of the individual, is certainly challenging. Scholars, such as Al-Khouri argue that the lack of secure and dependable tool connecting physical and digital identities impedes development and precludes the use of full potential of cross-globe digital economy.[92] His argumentation relies on the OECD 2011 report, which accentuated the need for global digital identity management offering means for "trusted remote interactions" and further cultivating the Internet economy.[93] The report encouraged governments to adopt national identity management strategies, align their e-government services with the strategy and subsequently cooperate at international level for mutual recognition of enabling cross-border digital management.[94]

At the EU level, cross-border use of online services by secure electronic identification and authentication is seen as an integral part of the Europe 2020 strategy for smart, sustainable and inclusive growth.[95] In the process of effectuating the strategy, a regulation was proposed and adopted for EU-wide mutual recognition of e-identification and digital signatures[96] in order to provide a framework for secure and trustworthy cross-border digital communication and an interoperable system of e-government services between citizens, businesses and public authorities across the EU.[97] The Regulation foresees, among other things the need for creation of a public key infrastructure at pan-European level for increasing the security of digital transactions and is not intended to interfere with existing national infrastructure on electronic identity managements systems (such as Estonian national e-ID system), but enforced to make them interoperable.

An effective solution seems to subsist at the small corner of Europe, in the form of a programme providing e-trust services to foreign nationals based on the previously existing national identity documents, state-backed by the PKI, enabling access to private and public services by secure means of authentication and verification, and it is called e-residency. Except that it is only there to make contributions to Estonian economy, science, education or culture; and to increase the visibility of Estonia as a technologically advanced state (who perhaps had what it takes to effectuate a global – at least EU-wide – digital identity management even before the world realised they needed one); and except that it exists as a closed system not designed to

[92] Al-Khouri (2014). See also Graux (2013), De Andrade (2012) and De Andrade (2013)
[93] OECD (2011). Digital Identity Management. Enabling Innovation and Trust in the Internet Economy.
[94] *Ibid.*
[95] Communication from the Commission Europe 2020. A strategy for smart, sustainable and inclusive growth. COM(2010) 2020 final.
[96] Regulation (EU) No. 910/2014
[97] Even though there was a legal framework for digital signatures at the EU level even prior to the Digital Agenda 2020, it existed solely only e-signatures (Directive 1999/93/EC) and did not encompass e-identification or other trust services, e.g., time stamping.

serve as *modus operandi* for global effectuation of mutual digital identification management. Then again, Estonian ID-card is one of numerous national e-identity systems, although indeed one of the most successful schemes in terms of integration and use at national level. Estonian solutions stand out in the era of proliferation of identity management systems and techniques in the marketplace[98] (like the Apple's trackpad signature) as a result of the all-encompassing use of digital identification for both private and public digital services. Thus, although it can at first be perceived as the key for cross-border digital authentication, the e-residency programme has since the beginning advertised itself as being a closed, Estonia-patronising system and never shown any philanthropic purpose at the global scale.[99] Therewith, e-residency should not be seen as the sought-for panacea for a global digital citizen, but considering the attention it has brought to Estonia, is seems to be an exuberant national start-up splendidly serving its purpose of retaining the image of a tech-savvy country.

## 5. Concluding Remarks

This chapter has indicated that the idea of making a foreign national, for example, a Sri Lankan an e-Estonian is a very ambitions one, and despite certain deficiencies in Estonian legal framework as well as the dubious capacity of the responsible institutions enforcing the e-residency programme, the concept has been pushed through and received great attention worldwide. E-residency has enticed people from across the world to become Estonian digital citizens, including for instance, the well-known British Journalist Edward Lucas (also the first e-resident) and high-ranked officials, such as the Prime Minister of Japan, Shinzō Abe. Therefore, by virtue of the fact that e-residency was launched to operate within a closed national system providing to foreign nationals Estonian e-services and gathering them under the umbrella of Estonian e-ID system with contributions to Estonian development in mind, the programme can be regarded a successful ICT-tool. What has not been successful, thought, is the implementation of the e-residency concept in coordination of it with national and supranational regulatory framework.

Even though it has been made clear that the e-residency programme does not seek to serve as a model for global or EU-wide effectuation of digital identity management, certain

[98] See Hoikkanen, *et al*. (2010) p.6.
[99] Curiously enough, Graux, when analysing the problematics of the EU eSignatures Directive noted that the comprehensive electronic authentication framework common to the EU could be regarded a business opportunity since the EU has failed to act upon this at supranational level. See Graux (2011).

reconsiderations should be made with regard to data protection aspects of the concept in order to make it resemble the cyberdream it has been referred to. Currently, the Estonian government plays a twofold role for e-residents – being simultaneously a friend and a foe. – On the one hand, Estonia offers the proven system of secure government-provided and state-backed identity that supports the safe access via e-identification and authentication to Estonian e-services; on the other hand, there is challenge to the data privacy in the form of long-term storage of the e-residents' personal information in Estonian databases.[100] The uptake of ICTs for e-governance solutions demands methodological approach and careful analysis for a consistent regulatory system that could coexist with innovation and technological advancements[101] but e-residency was unsystematically merged with existing regulation.

The bottom line is that in terms of general framework surrounding the concept of e-residency, the layers of protection of digital identities are sound from technical security perspective but are not completely in coherence with the EU legal principles on data protection. These indications are not meant to accuse Estonia of potential violations of data confidentiality, integrity and security, or question its cyber security strategy but rather are intended to come across as a *caveat* for a country that will possibly be digitally storing the data of thousands of foreign nationals in the era where cyberattacks are not uncommon. Likewise, if Estonia sees the idea of 10 000 or 10 million e-residents as a tangible prospect, the authors see the re-evaluation of the current legislation supporting the e-residency – i.e., the Estonian Identity Documents Act which was merely amended to "accommodate" the provisions related to e-residency – as indispensable.

[100] Hoikkanen, *et al.* (2010) p. 4.

[101] Innovative technologies need e-regulation that is consistent and interoperable with "traditional" regulation. With developing implementable e-regulation, a need arises for progressive methodological basis. An example of 10 policy principles for such methodological approach are provided for instance by Kerikmäe and Dutt; see Kerikmäe and Dutt (2014) pp 28-29.

## References

### Books and Articles


Al-Khouri, A. M. (2014). Digital identity: Transforming GCC economies. *Innovation: Management, policy & practice*,16 (2), pp 184–194.

Ashbourn, J. (2005). "The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies", Background paper for the Institute of Prospective Technological Studies, DG Joint Research Centre, European Commission.

De Andrade, N. N. G. (2012). Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's competences and legal basis for eID. *Computer Law & Security Review*, 28, pp 153-162.

De Andrade, N. N. G. (2013). "Electronic Identity for Europe": Moving from Problems to Solutions. *Journal of International Commercial Law and Technology*, 8 (2), pp 104-109.

Dutt, P; Kerikmäe, T. (2014). Concepts and Problems Associated with eDemocracy. In Kerikmäe, T. (Ed.). *Regulating eTechnologies in the European Union: Normative Realities and Trends* (pp 285 - 323).Springer Verlag.

Goncalves, M. E. and Gameiro, M. I. (2012). Security, privacy and freedom and the EU legal and policy framework for biometrics. *Computer Law & Security Review*, 28, pp 320-327.

Graux, H. (2011). Rethinking the e-signatures directive: on laws, trust services, and the digital single market. *Digital Evidence and Electronic Signature Law Review*, 8, pp 9-24.

Graux, H. (2013). Moving towards a comprehensive legal framework for electronic identification as a trust service in the European Union. *Journal of International Commercial Law and Technology*, 8 (2), pp 110-117.

Hoikkanen, A.; Bacigalupo, M.; Compano, R.; Lusoli, W.; Maghiros, I. (2010). New Challenges and Possible Policy Options for the Regulation of Electronic Identity. *Journal of International Commercial Law and Technology*, 5 (1), pp 1-10.

Kerikmäe, T. (ed). (2014). *Regulating eTechnologies in the European Union. Normative Realities and Trends*. Springer International Publishing.

Kerikmäe, T; Dutt, P. (2014). Conceptualization of Emerging Legal Framework of E-regulation in the European Union. T. Kerikmäe (Eds.). In Kerikmäe, T. (Ed.). *Regulating*

*eTechnologies in the European Union: Normative Realities and Trends* (pp 7-32).Springer Verlag.

Madise, Ü., & Vinkel, P. (2014). Internet Voting in Estonia: From Constitutional Debate to Evaluation of Experience Over Six Elections. In Kerikmäe, T. (Ed.). *Regulating eTechnologies in the European Union: Normative Realities and Trends* (pp 53-72). Springer Verlag.

Martens, T. (2010). Electronic identity management in Estonia between market and state governance. *Identity in the Information Society*,3 (1), pp 213-233.

Nyman-Metcalf, K. (2014). e-Governance in Law and by Law. The Legal Framework of e-governance. In Kerikmäe, T. (Ed.). *Regulating eTechnologies in the European Union: Normative Realities and Trends* (pp 33-52).Springer Verlag.

Schouten, B. and Jacobs, B. (2009). Biometrics and their Use in e-passports. *Image and Vision Computing*, 27, pp 305–312.

**Legal framework**

Estonian:

Aliens Act. Available in English at: https://www.riigiteataja.ee/en/eli/513042015008/consolide

Constitution of the Republic of Estonia. Available in English at: https://www.riigiteataja.ee/en/eli/530102013003/consolide

Digital Signatures Act. Available in English at: https://www.riigiteataja.ee/en/eli/ee/530102013080/consolide/current

Government Regulation No. 109 of 03.07.2008, Statutes on maintaining the database on identity documents. [Isikut tõendavate dokumentide andmekogu pidamise põhimäärus]. Only available in Estonian.

Government Regulation No. 252 of 20.12.2007, Information systems security measures sytem [Infosüsteemide turvameetmete süsteem]. Only available in Estonian.

Identity Documents Act of the Republic of Estonia. § $20^5$. E-resident's digital identity card. Available in English at: https://www.riigiteataja.ee/en/eli/512112014001/consolide

Issuing digital identities to non-residents: creating e-residency. Concept. Appendix to explanatory memorandum to draft legislation of Estonian Identity Documents Act and State Fees Act. Appendix 1." [Mitteresidentidele digitaalse isikutunnistuse väljaandmine: e-residentsuse loomine. Kontseptsioon. Isikut tõendavate dokumentide seaduse ja riigilõivuseaduse muutmise seaduse eelnõu seletuskirja juurde. Lisa 1.] 2014.

Public Information Act. Available in English at: https://www.riigiteataja.ee/en/eli/522122014002/consolide

Regulation of the Government of the Republic laying down the list of certificates and information to be submitted upon application and terms for the issue of an identity card, a residence permit card, a digital identity card, an Estonian citizen's passport, a seafarer's discharge book, a temporary travel document, a travel document for a refugee or a certificate of record of service on ships. Only available in Estonian.

EU:

The Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM(2012) 11 final.

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

Communication from the Commission Europe 2020. A strategy for smart, sustainable and inclusive growth. COM(2010) 2020 final.

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

Digital Agenda for Europe (Communication from the Commission of 19 May 2010 to the European Parliament, the Council, the European Economic and Social Committee and the

Committee of the Regions – A Digital Agenda for Europe [COM(2010) 245 final – Not published in the Official Journal].).

Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

**Electronic sources**

Newspaper Articles:

"Digital identity cards. Estonia takes the plunge." The Economist. 28 June 2014. Available at: http://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge.

Elisabeth Braw, "'E-stonia' Attempts to Become the Uber of Economies by Introducing Virtual Residency." 30 October 2014. Newsweek. Available in English at: http://www.newsweek.com/2014/11/07/estonia-attempts-boost-economy-introducing-virtual-residency-280571.html

The Economist explains: How did Estonia become a leader in technology? The Economist. 30 July 2013, by A.A.K, describing Estonia as having a "strong tech culture." Available at: http://www.economist.com/blogs/economist-explains/2013/07/economist-explains-21.

Reports, working papers:

Article 29 Data Protection Working Party. Working document on biometrics. Adopted on 1 August 2003. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf

Article 29 Data Protection Working Party. Working Party on Police and Justice. The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. Adopted on 01 December 2009. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

Digital Agenda 2020 for Estonia. Ministry of Economic Affairs and Communications. Available at: https://e-estonia.com/wp-content/uploads/2014/04/Digital-Agenda-2020_Estonia_ENG.pdf

Freedom House Freedom on the Net 2014. Estonia country report: https://freedomhouse.org/report/freedom-net/2014/estonia

OECD (2011). Digital Identity Management. Enabling Innovation and Trust in the Internet Economy. Available at: http://www.oecd.org/sti/ieconomy/49338380.pdf

The D5 Charter: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386290/D5Charter_signed.pdf

Other:

Background to Regulation 2252/2005. Available at EUR-Lex: http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32004R2252.

Digital Agenda for Europe. Progress by country. Available at: https://ec.europa.eu/digital-agenda/en/scoreboard/estonia

e-Estonia. The Digital Society. Available in English at: https://e-estonia.com/

Electronic ID-Card. E-Estonia.com Available in English at: https://e-estonia.com/component/electronic-id-card/

Estonian Development Fund. Available in English at: http://www.arengufond.ee/en/.

Estonian Information System Authority. Facts about e-Estonia. Available in English at: https://www.ria.ee/facts-about-e-estonia/

Estonian Information Systems Authority website. Available in English at: https://www.ria.ee/iske-en/

Estonian Ministry of the Interior. E-residency. Available in English at: https://www.siseministeerium.ee/e-residency/

Estonian National Electoral Committee. Statistics on Internet voting. Available in English at: http://vvv.vvk.ee/voting-methods-in-estonia/engindex/statistics/.

Estonian Tax and Customs Board Yearbooks. Available in English and Estonian at: http://www.emta.ee/index.php?id=34149&tpl=1026 and http://www.emta.ee/index.php?id=14595

Foreword of Edward Lucas to the e-Estonia newsletter at: https://e-estonia.com/foreword-to-the-e-estonia-newsletter-by-edward-lucas/

ID-Card. Computer protection. Information security signpost. ID-kaart. Arvutikaitse. Infoturvalisuse teeviit. Only available in Estonian at: http://www.arvutikaitse.ee/arvutikaitse-algtoed/id-kaart/

Memorandum of Understanding between Finland and Estonia on cooperation in the field of ICT. Available in English at: https://valitsus.ee/sites/default/files/news-related-files/ict_mou_fi-ee_10dec2013.pdf.

Official ID-card and Mobile-ID portal. Available in English at: http://www.id.ee/?lang=en&id

The Minister of the Interior of the Republic of Estonia, Mr Hanno Pevkur at 05.02.2015 weekly press conference of the Government of the Republic of Estonia. Available in Estonian at: http://meediaveeb.valitsus.ee/show.php?path=/2015/pressikonverents-2015-02-05-rnd32757.f4v

The Twitter Post of the Prime Minister of Estonia: https://twitter.com/TaaviRoivas/status/523530893613617152?utm_source=fb&utm_medium=fb&utm_campaign=TaaviRoivas&utm_content=523530893613617152

## Conclusions

The image of digitally advanced society is clearly what Estonia has been pursuing as has been laid down by, *inter alia* the national Digital Agenda 2020. Continuous international, supranational and national cooperation between different public-private authorities has provided Estonia the possibility to take up and to teach the effective implementation e-governance solutions and to share best practices at the EU as well as global level.[102] Other European Union Member States safely follow; for instance Finland is partially taking over the X-Road system that was developed in Estonia in 2001. There has been a rapid development of the digital economy, perhaps due to its small size, but mostly by virtue of the fact that Estonia had to re-build its governance after the restoration of the Independence, where implementing the e-solutions has played a marginal role. Estonia's strong technical framework surrounding the microchip on the back of the nationally successful Estonian's digital identity card gave an incentive to seize the chance where most countries are still searching for secure means of digitally identifying their citizens. Therewith Estonia launched a national start-up to offer foreign nationals digital identities (although under the Estonian terms, having Estonian development in mind) making it the first national digital society to become cross-border and giving its e-services a global reach.

The previously presented chapter of a book indicated that the conception of e-residency is surrounded by a judicially interdisciplinary framework that embodies fundamental rights and freedoms, legal principles of public international law, data protection law as well as administrative law. The compliance with national and supranational regulatory framework was presented in section 3 of the publication. There, attention was drawn to the fact that for the execution of the e-residency programme no new legal acts were introduced. Instead, the Estonian Identity Documents Act was amended, categorising the documents issued to non-nationals as e-resident's digital identity cards and integrating the necessary legal framework for the concept into the Act. It must be emphasised that due to the fact that the Estonian Identity Documents Act had already beforehand applied the term "digital identity card" for Estonian national e-IDs, after coming into force of the e-residency, i.e., starting from December 1, 2014,

[102] See more about the Estonian success in implementation of e-government services and centralised IT solutions Pappel, I., and Pappel, I. (2011). Implementation of Service-based E-government and Establishment of State IT Components Interoperability at Local Authorities. *2011 3rd International Conference on Advanced Computer Control (ICACC 2011)*.

one single term has two meanings – in addition to its original implication, "digital identity card" also refers to e-IDs of e-residents, even though the two cards do not serve the same purpose.

The examination of regulatory background revealed that concept of e-residency is not fully compatible with neither the Estonian nor the European Union legal principles. Since the Identity Documents Act first and foremost surrounds the identity documents of physical residents and citizens of Estonia, it contains the requirement of integration of biometric data to passports and travel documents (including digital identity card of Estonia) in accordance with the EU regulation for the purpose of improving the security of travel documents and passports as well as to prevent falsification of such documents.[103] By virtue of the aforementioned fact that the Estonian Identity Documents Act had already beforehand applied the term "digital identity card" and does not differentiate between a digital identity document of the citizen and that of the e-resident, the EU requirement of integrating biometric features automatically became applicable to e-residents' identity cards despite the detail that the digital identity cards of e-residents' do not serve as travel documents. Section 3.3. of the research publication presented why this is not only unnecessary but also potentially interfering with the data protection principles of the EU.

The research further indicated that the need for a common electronic identity is especially high for effectuating the European Digital Single Market, for which it is seen as a backbone of modern communications and transactions in the digital world, as well as a key driver for the growth of the EU economy and the completion of the Digital Single Market.[104] The publication presented that the Estonian success in using the identity cards for digital signatures and e-services has contributed to one of the most successful e-governments in the world. Estonian technical advancements are widely known and accepted, and now Estonia has introduced a concept which could create a global digital citizen. However, the research further revealed that e-residency works on a closed-system basis, meaning that every e-residency issued is a national decision and the e-residency does not serve as a model for global identity management that can be licensed to be used by other countries or private entities. Therefore, the country leaves itself the right to assess whether it is remunerable for the state to have a certain person as its e-

[103] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States; including its amending and supplementing acts.
[104] De Andrade, N. N. G. "Electronic Identity for Europe": Moving from Problems to Solutions. Journal of International Commercial Law and Technology, 2013, 8 (2), p 104.

resident, rendering the system of e-residency to resemble a marketing campaign instead of a *modus operandi* for systematic global identity management it could very effectively be.

Nevertheless, even though the e-residency is a benefit not a right, once accepting a person to the country's system, Estonia has to ensure the integrity of the personal data trusted to it. The security of the e-residency system means preventing certain data from being transferred to wrong hands in case of unsecure authentication systems; but it should also mean careful handling of the same data in information databases, prevention of unnecessary interference with the data as well as just and fair access to e-systems equally to citizens and e-residents. The plan to have 10 million e-Estonians by 2025 is a rather ambitious one. Based on hitherto existing information on e-residency, it is difficult, if not impossible, to see whether the system, both from legal as well as technical aspects can endure the prodigious burden on the system. However, the research conducted for this thesis revealed that the role of human rights in the regulation and protection of digital identity of e-residents is undervalued by the developers of e-residency. The discrepancies presented in the research provide room further critical assessment of the topic.

### IV. Future Research

Due to obviously lacking systematic methodology for assessing the various aspects of e-residency and potentially other ICT-enabled e-government solutions, the author of the thesis sees future need for a large-scale research. One methodological approach to the challenges the Estonian e-residency has to face can be analysed based on criteria adjusted by the author that was initially generated for assessing the effectiveness of European various eID frameworks[105] and would include following aspects:

1) **Techno-legal integration***:* How should the Estonian national identity management system be compatible with architecturally different infrastructures of other EU Member States within the meaning of mutual recognition of e-identification and digital signatures regulation of the EU? What should be changed or which implementing acts adopted in order for the Estonian national legal framework to enable the recognition of authentication

[105] Published by De Andrade, N. N. G. "Electronic Identity for Europe": Moving from Problems to Solutions. Journal of International Commercial Law and Technology, 2013, 8 (2), p 106 as an outcome of a workshop on "Electronic Identity for Europe", at the European level in 6th International Conference on Legal, Security and Privacy Issues in IT Law (LSPI). See also http://www.lspi.net/

processes involving different Member States? How can the flows of identity-related data of Estonian citizens as well as e-residents be regulated in a privacy-controlled manner suitable for a technology-driven society?

It has been presented that there is a need for specifically drafted legal provisions on new emerging technologies.[106] Substantial research could be conducted on the privacy and integrity aspects of the data submitted by e-residents' upon the application, with regard to the necessity of biometrics in the digital identity cards that can only be used for electronic identification purposes as well as what concerns the national requirements of storing the data in Governmental databases, bearing in mind grounds the invalidation of the Data Retention Directive.[107] Digital databases containing traffic data of potentially millions of citizens from tens of countries may incur the "big-brother-scenarios" as well as cyber attacks to Estonian critical infrastructure as was indicated in section 3.3. of the chapter. Privacy is a fundamental right protected under EU and international law and especially since the Estonian e-services open to foreign nationals have the potential to become successful at a global level (even if via closed-system approach), the legal framework surrounding the issuing of digital identities, especially concerning the review of applications, should be reconsidered. The focus must also be on the proposed Data Protection Regulation in the EU and its effectiveness to surround technological developments.[108]

2) **Liability of actors***:* Is there a need, and if there is, then what kind of amendments must be made or implementing acts adopted at the Estonian level for a most effective division of responsibilities with regard to issuing, suspension and revocation of the e-residency applications. What is a clearly formulated legal status of the e-residents and what is expected of them within the meaning of "promoting the development of the Estonian economy, science, education or culture by providing access to e-services with the Estonian digital document"?

   One aspect of future research thereto could include assessment of the quality and efficiency of handling the applications by the Police and Border Guard Board - to see whether it needs

[106] Nyman-Metcalf, K. (2014). e-Governance in Law and by Law. The Legal Framework of e-governance. In Kerikmäe, T. (Ed.). *Regulating eTechnologies in the European Union: Normative Realities and Trends*, p. 41.
[107] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
[108] For instance, Zhang has recently pointed out the deficines in the EU Data Protection regulatory framework. Zhang, K. (2014) Incomplete Data Protection Law. *German Law Journal*, 15 (6), pp 1071-1104.

to be taken as a priority to create a separate Board for assessing and reviewing the applications as the current capacity of the Board is questionable, both, in terms of competence on analysing whether the future e-residency is compatible with the objective of issuing the digital identities to foreign nationals, as well as in terms of quantity – more than 10 million applications to be reviewed is not an extraneous task. In addition, for the purpose of reducing any risks, for ensuring the reliability of e-residents and to exercise supervision over the use of services accessible to e-residents, the official Concept has set forth certain precautionary activities that should ensure the legal use of digital identities:

- a thorough background check on the e-residency applicants, involving relevant authorities and conducting relevant enquiries in data collections – if there are any doubts with regard to the applicant's reliability, the e-residency will not be issued;
- if there is a need, the service providers must monitor the use of digital identities in order to find misuse and aberration from normal use;
- The State Information System Authority provides expert support to digital service providers for monitoring the use of digital identities
- The Police and Border Guard Board as issuer of the e-residencies can investigate cases whereat there is a justified reason to believe that the digital identity card has been given to third parties for use. [109]

The scope of such measures with regard to the rights and liabilities of both the end-user, i.e., the e-resident as the service user, as well as of the state could be assessed in order to determine their proportionality and need.

3) **User-centricity***:* Is the principle of user-centricity[110] that ought to provide the e-residents with greater control over their own digital records, an integral part of the e-residency concept within the Estonian legal system? If no, is advancement of user-centricity a necessary goal to be achieved?

The European Commission Vice-President for DSM has emphasised the one of the key aspects of engaging the European citizens in digital economy is to have their freedoms

[109] The Concept, p 14.

[110] User-centricity refers to a situation whereby it is the user not a public authority or service provider who maintains control over ''what, where, when, and to whom'' the user identity information and traffic is released. See for instance, De Hert, P. Identity management of e-ID, privacy and security in Europe. A human rights view. Information Security Technical Report, 2008, 13, p. 72. Also, Rundle, M. *et al.*At a Crossroads:''Personhood'' and Digital Identity in the Information Society. STI Working Paper 2007/7, OECD, 2008, p. 22. Available at: (http://www.oecd.org/dataoecd/31/6/40204773.doc).

equally protected online and offline.[111] In identity management generally, the trend is towards moving stronger control to the user.[112] Thus, in combination with the first aspect, i.e., the techno-legal integration and requirement of coherence between technological advancements and legislation, the relationship between efficient data protection legislation and user empowerment could be analysed; including the scope of rights of the e-resident or any other end user whose data are being collected, disclosed and processed. It has been noted that violations of privacy issues on cross-border flow of data arise by the mere fact that privacy rules are mostly national.[113] If Estonia hosts the data of foreign nationals to whom it does not grant any rights, the conflict between laws of different legal systems could be analysed. Hoikanen, *et al*. have warned how the balance from user-centricity shifting in favour of governments in terms of storing the data may give them the possibility to dictate the data handling standards. The latter standards, however, tens to be "justified" on moral grounds, i.e., the government-side statements that even though they have more data than they need, they will only use in appropriately.[114] Recently a completely opposite perspective has been provided – namely, that the states are rather moving towards "nationalism of Internet," and governments, based on concerns related to privacy and security, are making efforts to keep data within national borders.[115] Therefore, another completely new angle for the concept of e-residency would be to analyse the meaning of localisation of data for the concept.

4) **Verification of identity*:*** Are there options for complete anonymisation of the traffic data or the identity of Estonian digital identity card users? Insofar as the digital identity card serves the purpose of digital identification and authentication, is there room for fraudulent activities, i.e., identity theft?

   The drafters of the concept have predicted that the e-residency itself does not cause misuse but may contribute to misdemeanours by making committing fraud easier and cheaper.[116]

[111] Ansip, A. Mission Letter of the Vice President for the Digital Single Market. Brussels, 1 November 2014.
[112] Strauss, S., and Aichholzer, G. (2010). National Electronic Identity Management: The Challenge of a citizen-centric Approach beyond Technical Design. *International Journal on Advances in Intelligent Systems,* 1-2 (3), p. 12.
[113] LeSieur, F. (2012). Regulating cross-border data flows and privacy in the networked digitaal environment and global knowledge economy. *International Data Privacy Law*, 2(2), p. 93.
[114] Hoikkanen, A.; Bacigalupo, M.; Compano, R.; Lusoli, W.; Maghiros, I. (2010). New Challenges and Possible Policy Options for the Regulation of Electronic Identity. *Journal of International Commercial Law and Technology*, 5 (1), p. 5.
[115] Chander, A., and Le, P. U. (2015). Data Nationalism. *Emory Law Journal*, 64 (3), p. 679.
[116] The Concept, p. 14.

The digital identity card issued to e-residents is an important identity document within the meaning of Estonian Penal Code[117] and thus, falsification, obtaining the use of, the use itself of falsified documents, or granting permission to use falsified documents, the fraudulent use of the e-ID as well as destruction, damaging, theft, withholding or concealment are punishable by pecuniary punishment or imprisonment.[118] Additionally, the providing of false information for the purpose of obtaining the e-resident's digital identity to the administrative authority, is also punishable as a criminal offence.[119] The need for a common system of identification in general stems from the "agnostic" nature of the Internet with regard to the identities of users;[120] however, in terms of large amount of cross-border data flows and e-services, it is more difficult to scrutinise the person actually sitting in front of the computer – which could easily lead to identity thefts.[121] Therefore, the possible risks that hosting a database of global digital citizens' identities may incur, e.g., money laundering, tax evasions, or hackers going after the e-services,[122] could be further analysed.

[117] The Penal Code. RT I, 23.12.2014, 16, §350. Available in English at: https://www.riigiteataja.ee/en/eli/522012015002/consolide

[118] §§ 346-340 of the Penal Code.

[119] §280 of the Penal Code.

[120] Mahler, T. (2013). Governance Models for Interoperable Electronic Identities. *Journal of Internatioral Commercial Law and Technology*, 8 (2), p. 149.

[121] Anandarajan, Murugan. et al. "Safeguarding consumers against identity-related fraud." International Data Privacy Law, 2013, Vol. 3, No. 1.

[122] Identity fraud occurs when a false identity or someone else's identity details are used to support unlawful activity or when someone avoids an obligation or liability by falsely claiming that they were victims of identity fraud. See Collings, T. (2008). Some thoughts on the underlying logic and process underpinning Electronic Identity (e-ID). *Information Security Technical Report,* 13, pp 68-69.

## Kokkuvõte

Eesti on loonud endast eduka e-riigi kuvandi, mida toestatakse uudsete IKT-lahendustega, milleks innovaatilisemaiks on e-residentsus. 2014. aasta 1. detsembrist avas Eesti esimese riigina maailmas oma e-teenused võõrriigi kodanikele. Eesti poolt väljastatav digitaalne identiteet – e-residentsus – ei too kaasa Eesti Vabariigi kodakondsust või residentsust, vaid annab võimaluse isiku turvaliseks tõendamiseks digitaalses keskkonnas. E-residentsuse väljastamise tehnoloogiline alus põhineb Eesti Vabariigi ID-kaardiga identselt avaliku võtme infrastruktuuril (PKI), mis võimaldab digitaalses keskkonnas turvaliselt digiallkirjastada ja autentida. Samas ei ole e-residendi ID-kaart füüsilises keskkonnas isikut tõendava dokumendina kasutatav. Kuivõrd tegemist on maailmas ainulaadse programmiga, puudub e-residentsuse õigusliku aluse, seda nii Eesti-siseselt kui supranatsionaalsel tasandil, mastaapne analüüs.

Seetõttu on magistritöö eesmärk anda konstruktiivne ülevaade e-residentsusele kolmest põhilisest aspektist. Esimene osa keskendub e-residentsuse kontseptsioonile üldiselt, sealhulgas tutvustades tehnoloogilist alust, poliitilisi taotlusi ning Eesti ootusi e-residendile. Väitekirja põhiline fookus on e-residentsuse seadusandliku baasi analüüsil, sh antakse ülevaade ka Euroopa Liidu õigusliku raamistiku mõjust e-residentsusele. Kuivõrd Eesti on sidunud oma e-riikluse arhitektuuri ka Euroopa Liidu digitaalarengu (õigus)poliitikaga läbi Infoühiskonna Arengukava 2020, mis omakord seab e-residentsusele eesmärgi Eesti kui eduka e-riigi kuvandi hoidmine, analüüsib artikli viimane põhiosa e-residentsuse võimalikku rolli globaalse ja EL-i tasandil toimiva digitaalse identiteedi haldamisel. Käesolev magistritöö ei paku lahendusi e-residentsusega kaasnevatele probleemkohtadele, vaid pigem kaardistab kriitilised ebakõlad kontseptsiooni ja regulatiivse raamistiku vahel.

# Common List of References

## Books and Articles


- Alekand, A. (2015). Osaühingu osanikeregistri pidamine. *Juridica*,(1), pp 10-15
- Al-Khouri, A. M. (2014). Digital identity: Transforming GCC economies. *Innovation: Management, policy & practice*, 16 (2), pp 184–194.
- Anandarajan, M., D'Ovidio, R., & Jenkins, A. (2013). Safeguarding consumers against identity-related fraud. *International Data Privacy Law*, 3 (1), pp 51-60.
- Annus, R. (2014). E-residentsus. *Juridica*, (10), pp 740-750.
- Ashbourn, J. (2005). "The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies", Background paper for the Institute of Prospective Technological Studies, DG Joint Research Centre, European Commission.
- Chander, A., and Le, P. U. (2015). Data Nationalism. *Emory Law Journal*, 64 (3), pp 677-739.
- Collings, T. (2008). Some thoughts on the underlying logic and process underpinning Electronic Identity (e-ID). *Information Security Technical Report*, 13, pp 61-70.
- De Andrade, N. N. G. (2012). Regulating electronic identity in the European Union: An analysis of the Lisbon Treaty's competences and legal basis for eID. *Computer Law & Security Review*, 28, pp 153-162.
- De Andrade, N. N. G. (2013). "Electronic Identity for Europe": Moving from Problems to Solutions. *Journal of International Commercial Law and Technology*, 8 (2), pp 104-109.
- De Hert, P. (2008). Identity management of e-ID, privacy and security in Europe. *A human rights view. Information Security Technical Report*, 13, pp 71-75.
- Dutt, P; Kerikmäe, T. (2014). Concepts and Problems Associated with eDemocracy. In Kerikmäe, T. (Ed.). *Regulating eTechnologies in the European Union: Normative Realities and Trends* (pp 285 - 323).Springer Verlag.
- Goncalves, M. E. and Gameiro, M. I. (2012). Security, privacy and freedom and the EU legal and policy framework for biometrics. *Computer Law & Security Review*, 28, pp 320-327.

- Graux, H. (2011). Rethinking the e-signatures directive: on laws, trust services, and the digital single market. *Digital Evidence and Electronic Signature Law Review*, 8, pp 9-24.
- Graux, H. (2013). Moving towards a comprehensive legal framework for electronic identification as a trust service in the European Union. *Journal of International Commercial Law and Technology*, 8 (2), pp 110-117.
- Hansen, M., Berlich, P., Camenisch, J., Claus, S., Pfitzmann, A., Waidner, M. Privacy-Enhancing Identity Management. Information Security Technical Report, 2004, 9 (1), pp 35-44.
- Hoikkanen, A.; Bacigalupo, M.; Compano, R.; Lusoli, W.; Maghiros, I. (2010). New Challenges and Possible Policy Options for the Regulation of Electronic Identity. *Journal of International Commercial Law and Technology*, 5 (1), pp 1-10.
- Kerikmäe, T. (ed). (2014). *Regulating eTechnologies in the European Union. Normative Realities and Trends*. Springer International Publishing.
- Kerikmäe, T; Dutt, P. (2014). Conceptualization of Emerging Legal Framework of E-regulation in the European Union. T. Kerikmäe (Eds.). In Kerikmäe, T. (Ed.). *Regulating eTechnologies in the European Union: Normative Realities and Trends* (pp 7-32).Springer Verlag.
- LeSieur, F. (2012). Regulating cross-border data flows and privacy in the networked digitaal environment and global knowledge economy. *International Data Privacy Law*, 2(2), pp 93-104.
- Madise, Ü., & Vinkel, P. (2014). Internet Voting in Estonia: From Constitutional Debate to Evaluation of Experience Over Six Elections. In Kerikmäe, T. (Ed.). *Regulating eTechnologies in the European Union: Normative Realities and Trends* (pp 53-72). Springer Verlag.
- Mahler, T. (2013). Governance Models for Interoperable Electronic Identities. *Journal of Internatioral Commercial Law and Technology*, 8 (2), pp 148-159.
- Martens, T. (2010). Electronic identity management in Estonia between market and state governance. *Identity in the Information Society*, 3 (1), pp 213-233.
- Nyman-Metcalf, K. (2014). e-Governance in Law and by Law. The Legal Framework of e-governance. In Kerikmäe, T. (Ed.). *Regulating eTechnologies in the European Union: Normative Realities and Trends* (pp 33-52).Springer Verlag.

- Pappel, I., and Pappel, I. (2011). Implementation of Service-based E-government and Establishment of State IT Components Interoperability at Local Authorities. *2011 3rd International Conference on Advanced Computer Control* (ICACC 2011), pp 371-377.
- Price, G. (2008). The benefits and drawbacks of using electronic identities. *Information Security Technical Report*, 13, pp 95-103.
- Rosentau, M. (2015) E-tempora, e-mores. *Juridica*, (2), pp 138-153
- Saxby, S. (2014). Electronic identity: The global challenge. Presented at the 8th International Conference on Legal, Security and Privacy issues in IT Law (LSPI) November 11e15, 2013, Tilleke & Gibbins International Ltd., Bangkok, Thailand. *Computer law & Security review*, 30, pp. 112-125.
- Schouten, B. and Jacobs, B. (2009). Biometrics and their Use in e-passports. *Image and Vision Computing*, 27, pp 305–312.
- Strauss, S., and Aichholzer, G. (2010). National Electronic Identity Management: The Challenge of a citizen-centric Approach beyond Technical Design. *International Journal on Advances in Intelligent Systems*, 1-2(3), pp 12-23.
- Tupay, P. K., & Mikiver, M. (2015). E-riik ja põhiõigused. *Juridica*, (3), pp 163-176.
- Zhang, K. (2014) Incomplete Data Protection Law. *German Law Journal*, 15 (6), pp 1071-1104.

**Legal framework**

Estonian:

- Aliens Act. Available in English at: https://www.riigiteataja.ee/en/eli/513042015008/consolide
- Constitution of the Republic of Estonia. Available in English at: https://www.riigiteataja.ee/en/eli/530102013003/consolide
- Digital Signatures Act. Available in English at: https://www.riigiteataja.ee/en/eli/ee/530102013080/consolide/current
- Government Regulation No. 109 of 03.07.2008, Statutes on maintaining the database on identity documents. [Isikut tõendavate dokumentide andmekogu pidamise põhimäärus]. Only available in Estonian.

- Government Regulation No. 252 of 20.12.2007, Information systems security measures sytem [Infosüsteemide turvameetmete süsteem]. Only available in Estonian.
- Identity Documents Act of the Republic of Estonia. § $20^5$. E-resident's digital identity card. Available in English at: https://www.riigiteataja.ee/en/eli/512112014001/consolide
- Issuing digital identities to non-residents: creating e-residency. Concept. Appendix to explanatory memorandum to draft legislation of Estonian Identity Documents Act and State Fees Act. Appendix 1." [Mitteresidentidele digitaalse isikutunnistuse väljaandmine: e-residentsuse loomine. Kontseptsioon. Isikut tõendavate dokumentide seaduse ja riigilõivuseaduse muutmise seaduse eelnõu seletuskirja juurde. Lisa 1.] 2014.
- The Penal Code. Available in English at: https://www.riigiteataja.ee/en/eli/522012015002/consolide
- Public Information Act. Available in English at: https://www.riigiteataja.ee/en/eli/522122014002/consolide
- Regulation of the Government of the Republic laying down the list of certificates and information to be submitted upon application and terms for the issue of an identity card, a residence permit card, a digital identity card, an Estonian citizen's passport, a seafarer's discharge book, a temporary travel document, a travel document for a refugee or a certificate of record of service on ships. Only available in Estonian.

EU:

- Communication from the Commission Europe 2020. A strategy for smart, sustainable and inclusive growth. COM(2010) 2020 final.
- Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.
- Digital Agenda for Europe (Communication from the Commission of 19 May 2010 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Digital Agenda for Europe [COM(2010) 245 final – Not published in the Official Journal].).

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.
- Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- Proposal for a Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM(2012) 11 final.
- 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.
- The Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

**Electronic sources**

Newspaper Articles:

- "Digital identity cards. Estonia takes the plunge." The Economist. 28 June 2014. Available at: http://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge.
- Elisabeth Braw, "'E-stonia' Attempts to Become the Uber of Economies by Introducing Virtual Residency." 30 October 2014. Newsweek. Available in English at: http://www.newsweek.com/2014/11/07/estonia-attempts-boost-economy-introducing-virtual-residency-280571.html
- The Economist explains: How did Estonia become a leader in technology? The Economist. 30 July 2013, by A.A.K, describing Estonia as having a "strong tech culture." Available at: http://www.economist.com/blogs/economist-explains/2013/07/economist-explains-21.

Reports, working papers:


- Article 29 Data Protection Working Party. Working document on biometrics. Adopted on 1 August 2003. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp80_en.pdf
- Article 29 Data Protection Working Party. Working Party on Police and Justice. The Future of Privacy. Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data. Adopted on 01 December 2009. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf
- Digital Agenda 2020 for Estonia. Ministry of Economic Affairs and Communications. Available at: https://e-estonia.com/wp-content/uploads/2014/04/Digital-Agenda-2020_Estonia_ENG.pdf
- Freedom House Freedom on the Net 2014. Estonia country report: https://freedomhouse.org/report/freedom-net/2014/estonia
- OECD (2011). Digital Identity Management. Enabling Innovation and Trust in the Internet Economy. Available at: http://www.oecd.org/sti/ieconomy/49338380.pdf
- Rundle, M. et al. At a Crossroads:''Personhood'' and Digital Identity in the Information Society. STI Working Paper 2007/7, OECD, 2008. Available at: http://www.oecd.org/dataoecd/31/6/40204773.doc
- The D5 Charter: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386290/D5Charter_signed.pdf
- Mission Letter of the Vice President for the Digital Single Market, Andrus Ansip. Brussels, 1 November 2014. Jean-Claude Juncker, President of the European Commission. Available at: https://ec.europa.eu/commission/sites/cwt/files/commissioner_mission_letters/ansip_en.pdf


Other:

- 6th International Conference on Legal, Security and Privacy Issues in IT Law (LSPI). See also http://www.lspi.net/
- Background to Regulation 2252/2005. Available at EUR-Lex: http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32004R2252.
- Digital Agenda for Europe. Progress by country. Available at: https://ec.europa.eu/digital-agenda/en/scoreboard/estonia
- e-Estonia. The Digital Society. Available in English at: https://e-estonia.com/
- Electronic ID-Card. E-Estonia.com Available in English at: https://e-estonia.com/component/electronic-id-card/
- Estonian Development Fund on price winning award of e-residency: http://www.arengufond.ee/2014/06/arenguidee-konkursi-2014-loppurituse-salvestused/
- Estonian Development Fund. Available in English at: http://www.arengufond.ee/en/.
- Estonian Information System Authority. Facts about e-Estonia. Available in English at: https://www.ria.ee/facts-about-e-estonia/
- Estonian Information Systems Authority website. Available in English at: https://www.ria.ee/iske-en/
- Estonian Ministry of the Interior. E-residency. Available in English at: https://www.siseministeerium.ee/e-residency/
- Estonian National Electoral Committee. Statistics on Internet voting. Available in English at: http://vvv.vvk.ee/voting-methods-in-estonia/engindex/statistics/.
- Estonian Tax and Customs Board Yearbooks. Available in English and Estonian at: http://www.emta.ee/index.php?id=34149&tpl=1026 and http://www.emta.ee/index.php?id=14595
- European Commission Directorate General for Communications Networks, Content and Technology introduction to eIDAs, available at: http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond.
- Foreword of Edward Lucas to the e-Estonia newsletter at: https://e-estonia.com/foreword-to-the-e-estonia-newsletter-by-edward-lucas/

- ID-Card. Computer protection. Information security signpost. ID-kaart. Arvutikaitse. Infoturvalisuse teeviit. Only available in Estonian at: http://www.arvutikaitse.ee/arvutikaitse-algtoed/id-kaart/
- Memorandum of Understanding between Finland and Estonia on cooperation in the field of ICT. Available in English at: https://valitsus.ee/sites/default/files/news-related-files/ict_mou_fi-ee_10dec2013.pdf.
- Official ID-card and Mobile-ID portal. Available in English at: http://www.id.ee/?lang=en&id
- The Minister of the Interior of the Republic of Estonia, Mr Hanno Pevkur at 05.02.2015 weekly press conference of the Government of the Republic of Estonia. Available in Estonian at: http://meediaveeb.valitsus.ee/show.php?path=/2015/pressikonverents-2015-02-05-rnd32757.f4v
- The Twitter Post of the Prime Minister of Estonia: https://twitter.com/TaaviRoivas/status/523530893613617152?utm_source=fb&utm_medium=fb&utm_campaign=TaaviRoivas&utm_content=523530893613617152