GOVERNING ID

Estonia's E-Identity Programme

A project of the Centre for Internet and Society, India supported by Omidyar Network

→ digitalid.design ←

→ cis-india.org ←

RESEARCH & WRITING
Shruti Trikanad

REVIEW & EDITING
Yesha Tshering Paul and Amber Sinha

WITH INPUTS FROM
Dr. Katrin Nyman Metcalf*

DESIGN
Pooja Saxena

COVER ILLUSTRATION
Akash Sheshadri

THE CENTRE FOR internet & society

INTRODUCTION

This is the sixth in a series of case studies, using our evaluation framework for the governance of digital identity systems. These case studies, which analyse identity programmes and their uses, illustrate how our evaluation framework may be adapted to study instances of digital identity across different regions and contexts. This case study looks at the Estonian digital ID system.

The Estonian Digital ID landscape is unique both in terms of its complex legal framework, and the reliance of Estonian residents on their Digital IDs. Digital governance is viewed as integral parts of governance and identity, and focuses more on sector specific applications rather than "digital" legislation. The Population Register Act issues a unique number to every Estonian resident, termed the Personal Identification Code ("PIC"), and the Identity Documents Act governs the issue of the digital ID, or the e-ID, incorporating this PIC. The PIC is issued to every individual at birth or any time after, on application to the processor of the Population Register ("PR"), but it does not function independently as a digital ID. When a resident applies for the issue of a digital ID, the information they submit is checked against the Population Register, and they are issued a digital ID that is made unique by the inclusion of the PIC. Thus, the digital ID evaluated below is a sum of the parts issued under the Identity Documents framework, and the Population Register framework. On issue of the ID, the ID database acts as a repository of ID related personal data and documents, and the PR is a repository for other personal information. However, what is important to note is that the digital ID is not used merely to access these databases, but any other registered database storing personal information and allowing access through the ID, including private databases. This is done through the X road system, which is an interface that allows databases to communicate such that when data is needed, actors can access the relevant database directly. Access is determined by agreements entered into between different data collectors, and completely eliminates a system of requesting and releasing data.

RULE OF LAW TESTS

1.1 LEGISLATIVE MANDATE

Is the law governing digital ID a valid law?

The validity of a law governing digital ID can be tested on its clarity, foreseeability, and accessibility, and whether it categorically allows the use of the digital ID in the manner it is being used. The governing ID law — the Identity Documents Act — makes it mandatory for all residents and aliens who reside permanently in Estonia to possess an identity document, one of which is a digital ID. This Act was passed by the Legislature *(Riigikogu)*, is clear, foreseeable and easily accessible on the database *(Riigi Teataja)*, and explicitly regulates the issue and use of the digital ID.

However, the Act permits excessive delegation in the determination of its regulations; it allows the "minister responsible for the area" to issue regulations to decide the list of certificates and data to be submitted upon application for the issue of a document, the procedure for identification and verification of identity, the nature or governance of the identity documents database etc.[1] As these are some of the most crucial aspects of governance for a digital ID program, failing to adequately delineate them in legislation and allowing the Executive to regulate it falls foul of a strict interpretation of a "valid law".

Further, the Estonian legal system is designed such that there is little overarching legislation governing all aspects of the use of the ID. The ID is permitted to be used for any purpose provided there is a valid law that permits it. Thus, while the ID Act governs the issue of the ID, it does little to regulate any other aspect of the use of the ID itself — including the sharing of collected data — and thus leaves such critical matters unaddressed, to be determined by other laws or regulations. Although this is done deliberately, to have sector specific governance informed by the transaction that uses the digital ID, it creates a system where the Digital ID is not restricted by a purpose limitation, and just operates as a database of information to be leveraged by any sector and for any purpose.

Thus, the law that issues the Digital ID is valid, but it fails to govern crucial aspects of the use of the ID.

1 Section 15, 15(2), Identity Documents Act, 2000 ["ID Act"].

1.2 LEGITIMATE AIM

Does the law have a legitimate aim?

The Identity Documents Act does not explicitly lay out an aim or purpose, but does note that its purpose is to establish an "identity document requirement" and to regulate the issue of identity documents to Estonian citizens and aliens. Since the Act governs *all* identity documents issued by the Republic of Estonia, its implicit purpose can be identified as providing the means to identify and authenticate persons for all State purposes including national security, determination of citizenship, provisions of services, foreign relations, etc.

The aim backing the Act, of identifying and authenticating persons for different State purposes, is legitimate.

Another aim that influenced the ID system, one that is often touted as a great success in Estonia, is the Once Only Principles (OOP). Here citizens and businesses provide diverse data only once to public administration, after which the bodies internally share and reuse the data.[2] This is also open to private actors, who leverage the ID system to efficiently access data about the ID holder intending to use their services. The design of the ID system, as a web of interoperable databases connected through the X road system, point at the easy access of personal information as a primary criteria for its implementation. This is difficult to categorize as a 'legitimate aim' warranting the creation of a digital ID, and is more of a move favouring political expediency.

1.3 DEFINING PURPOSE

Does the law clearly define the purposes for which the ID can be used?

No, the Identity Documents Act does not delineate the uses of the digital ID.

It merely regulates the issue and revocation of digital IDs, and does not in any manner limit the purposes it may be used for. While it does mandate the use of

2 "Once-Only," The Once Only Principle, last accessed February 11, 2020, *http://toop.eu/once-only*; European Commission, "Trends in Electronic Verification: An Overview" (September 2018).

digital ID for the electronic provision of services, if such service provider requires it, it fails to place any limits on where else it might be used. It permits the ID to be leveraged by other service providers, provided it is within the contours of any other applicable law. While this once again points to a deliberate design to prevent parallel legislation for e-governance, with more legislative focus on the sector that uses the digital ID, it does fail the purpose limitation test. By not limiting the uses of the ID in the ID law, it permits data collected for the ID to be used for any purpose in the future, regardless of whether such a use was determined at the time of collecting data.

1.4 DEFINING ACTORS

Does the law governing digital ID clearly define all the actors that can use/manage or are connected to the ID database in any way?

The Identity Documents Act does not define the actors that use/manage the digital ID or the database. It categorizes the issuers based on the document they are issuing, which for the digital ID is the Police and Border Guard Board of Estonia[3], but does not prescribe other actors associated with the use or management of the database. In fact, it even permits the issuer to delegate the task of issuing (digital) certificates to any service provider,[4] the eligibility of whom is determined by the Electronic Identification and Trust Services Act. This Act does not in any way limit the number or types of actors that can manage the system, but merely imposes (largely security related) compliances. Further, it completely fails to address how the digital ID may be used. The task of regulating access to the Identity Documents Database—where data collected during the issue of the ID is stored, along with details of the ID itself— is delegated to the executive. The Statutes for the Maintenance of a Database of Identity Documents, enacted in 2016, govern the collection and access of ID information. Besides the identified public bodies who are permitted to access data in the system, the Statutes also allow data to be accessed by third parties "if there is a legal basis for their access" and in accordance with a contract concluded with the recipient.[5] However, since the ID system is intended as a series of interoperable databases accessible through the

3 Section 15(4), ID Act.

4 Section 9(4)(3), ID Act.

5 Section 16, Statutes for Maintenance of Identity Documents Database, 2016 ["ID Database Statutes"] *https://www.riigiteataja.ee/akt/102022018003* [In Estonian].

unique digital ID, and not one central repository, regulating merely the Identity Documents database is insufficient; it only addresses one particular use of the ID.

Similarly, the Population Register — which is also accessible through the digital ID — fails to define or limit the category of actors who may access personal data that it stores, but has broadly established certain controls for access of actors based on their duties and interests.

Although it fails to identify the categories of actors that can access the system, the Estonian Digital ID framework does have in place controls to ensure accountability and transparency in the use of the ID: the General Data Protection Regulation ("GDPR") mandates consent for private sector use, and a valid purpose outlined in law for public use; the design of the ID system is also such that any access of the system leaves behind a footprint of what data was accessed, at what time, by which actors, and for what purpose. However, even with such controls in place, by not limiting the actors that can access the Digital ID system, more risk is introduced into the system, and it moves further away from a purpose driven design.

The ID framework fails to identify the actors that can use the ID, but has in place controls to regulate their use.

1.5 REGULATING PRIVATE ACTORS

Is the use of the ID system by private actors adequately regulated?

No, the Estonian digital ID framework does not specify or limit access to personal information through the digital ID by private actors.

Both in the issue and the use of the ID, the role of private actors is sparsely regulated.

In the process of issuing the ID, private actors offer technological services in collaboration with the State. Section 9(8) of the Identity Documents Act allows the administrative authority to transfer personal data to third parties for identification and revocation of ID, and permits third parties to process data for this purpose. It does not restrict the role of private actors in the issue of certificates to enable digital IDs, and merely allows the issuing authority to regulate third parties via administrative contracts and standards. In November

2018, the Government recognised a new form of authentication for the digital ID, called the "Smart-ID". The Smart-ID is a mobile application developed by the banking sector in Estonia, that was used as an identification solution in banking services. By leveraging a technology that is essentially created and run by the private sector, for a function as important as authentication in the widely used digital ID, the Estonian Government's control over its e-governance system is further diluted.

Since there is no overarching Act regulating the uses of the ID, private actors are not in any manner restricted from using the ID system. The Statutes for the Maintenance of Identity Documents Database, issued by the "minister concerned for the area" under the Identity Documents Act, designates the data stored in the database for "internal purposes,"[6] but allows access to third parties if there exists a legal basis, and in accordance with the Public Information Act and the Personal Data Protection Act.[7] This is left to the discretion of the chief processor (the Police and Border Guard Board) of the database. Further, it allows the release of data to any party on a written application for release, if there is a legal basis for the release and if it is required for the verification of identity or identity document.[8]

The Population Register Act has some added controls for the use of the stored data by actors (other than those performing *public duties*), including an application for access, specified terms of processing, rights and obligations of processor, etc.[9] Thus, while it still does not prescribe the actors that have access, it does regulate the process of granting access in some manner.

Apart from the ID database and the PR, private actors can access all the personal data stored in databases created within the ID system, provided they have a legal basis for it. In these situations, the actors access data on a personal basis, after identifying themselves through their ID; to that extent, it is always possible to determine exactly who has accessed data, even within an institution or the State. This introduces transparency and accountability in the system, which does majorly contribute to effective regulation.

6 Section 16(1), ID Database Statutes.

7 Section 16(5), ID Database Statutes.

8 Section 17(1)(2), ID Database Statutes.

9 Sections 49, 51, Population Register Act, 2000 ["PR Act"].

1.6 DATA SPECIFICATION

Does the law clearly define the nature of data that will be collected?

Yes, the law is fairly prescriptive on the nature of data it collects for the issue of the digital ID.

The Identities Documents Act prescribes certain categories of personal data that may be entered in a document, and restricts entry of any other category unless a treaty, law, or legislation of general application allows it.[10] Within such boundaries, the law permits the 'minister for the concerned area' to determine by regulation the categories of data that can be collected for issue of the digital ID.[11] However, since the Act does not regulate the actual *use* of collected data, it does not address issues of the nature of data recorded on every use of the ID, and has no limitations or safeguards regarding such use whatsoever. The Personal Data Protection Act, together with the GDPR, fill these gaps, with safeguards concerning the use or purpose of data collected.[12]

Similarly, the Population Register Act prescribes several categories of data collected including ethnic nationality, residence and contact details, details of marital status, custody, voter registration data etc.[13] The Act also specifies the categories of data that will be periodically added/updated to the population register on the conclusion of certain events, such as the addition of data contained in identity documents on their issue.

However, it must be noted that the Digital ID system is such that it allows several databases to be created and accessed on the basis of the digital ID, all of which involve collection of fresh data. For instance, when the digital ID is used to access healthcare services, it involves the creation of a new database, that of electronic health records, which can subsequently be accessed by an insurance provider, when the ID holder avails insurance services. Because of the way these databases are interoperable and easily accessible through the digital ID, the collection of data at every instance of use is comparable to the collection of data during the issue of the ID. This is inadequately restricted or regulated by the Identity

10 Section 9, ID Act.

11 Section 15, ID Act.

12 Sections 14, 16, Personal Data Protection Act, 2019 ["PDP Act"].

13 Sections 20, 23, PR Act.

Documents Act, but there are regulations in place in the relevant sectors that use the ID that govern the nature of data collected.

1.7 USER NOTIFICATION

Does the ID system provide adequate user notification mechanisms?

Since the Identity Documents Act only deals with the issue of the documents, it does not set up any notification mechanism. However, some other laws are applicable to digital identity and form part of the ID system; the State Information System Management Act mandates traceability in the functioning of the system, such that all access to the database and responses to the user must be stored and recoverable.[14] This has been implemented through a portal, which allows users to check the dates and time of the use of their ID for authentication or digital signature purposes, along with the mode of ID (Digi ID card, Mobile ID, or Smart ID) [15] Thus, there is no mandate to proactively notify users every time their data is accessed, but the system allows easy access for records of when such data has been accessed. However, what must also be noted is that in the Estonian digital ID system, ID holders do not necessarily give consent each time their data is accessed for use by service providers; their consent is taken via a contract while applying for the digital ID, and data is easily transferred from one service provider to another through the Estonian information exchange system (X-Road), as the need arises. Thus, while an ID holder in a different digital ID system might otherwise be aware of every use of their ID because they have to consent to such use and authorize every transaction, the lack of an active notification system in Estonia means an ID holder may never be aware of all the times their personal data is accessed unless they make a proactive effort to check access records.

The Personal Data Protection Data Act mandates notifications for breach of data (to the Data Protection Inspectorate and the data subject) if it is likely to entail a high risk to the rights and freedoms of natural persons, within 72 hours of becoming aware of it. It also requires that the notification include a description

14 State Information System Management Act, 2008.

15 Information System Authority, "My ID-card activities", iD, *https://www.id.ee/index.php?id=31014*; Eesti.ee, *Estonian Government Information Portal, https://www.eesti.ee/en/*.

of the possible consequences of the personal data breach. Thus, through the applicability of the national data protection law, there is a user notification mechanism in place for breach of the system.

The data protection law mandates a notification mechanism for breach of data, but there is no system in place to notify ID holders every time their personal data is accessed.

1.8 USER RIGHTS

Do individuals have rights to access, confirmation, correction and opt out?

Since the Identity Documents Act only governs the issue of the ID, it does not provide for any right to access, correct, or opt out of the digital ID system. However, The Statutes for the Maintenance of Identity Documents Database allows the data subject to access their personal data stored in the database free of charge,[16] and mandates the controller of the database to amend incorrect data when notified of its inaccuracy. It does specify any right for ID holders to opt out of the ID or delete their personal data from the ID database.

It must be noted here that since the digital ID can be used for purposes outside the Identity Documents Act, and data may be collected independently for these purposes, the ID database itself does not comprise all the data involved in the digital ID; for this reason, governing the ID database is very limiting in terms of the entire scope of personal data involved in the digital ID. For instance, the use of the ID for the creation of electronic health records is governed by an entirely different framework of law, and may contain different rights and obligations on ID holders.[17]

With respect to the data contained in the PR, Section 45(1) read with Section 53 of the Population Register Act allows a person to access data in the registry about themselves, the agencies and persons who have the right to access data in the PR, and the purpose and legal basis of the processing of their data. Further, a person can dispute the accuracy of the data collected about them, based on which the processor will submit an inquiry about the accuracy of the data and temporarily restrict access to such data.[18]

16 Sections 17(1), 17(3), ID Database Statutes.

17 See Healthcare Services Organization Act, 2002, Statutes of Health Information System, 2016.

18 Sections 32, 33, PR Act.

As for opting out, Sections 17 and 19 of the Electronic Identification and Trust Services or Electronic Transactions Act ("Electronics Act") allows the certificate holder (the ID holder) to apply for the suspension and/or revocation of their certificate,[19] and effectively opt out of the ID system for that duration. However, reasons for such applications and durations of suspension are not identified in the Act, and therefore paint only an incomplete picture of how an ID holder may opt out of the system. There is also no indication as to whether the ID holder's personal data will be deleted from the ID system in case their ID is suspended.

Lastly, to the extent that the Personal Data Protection Act impacts the data in question, subjects have the right access and confirmation, and to demand rectification of inaccurate data. They may also demand erasure of data if the data was not collected pursuant to law, principles of processing were not adequately followed, or if erasure is required under any binding obligation.[20]

There are sufficient rights to access, confirmation, and correction in the governing framework, but an ID holder cannot effectively opt out of the ID system.

1.9 REDRESSAL MECHANISMS

Are there adequate civil and criminal redressal mechanisms in place to deal with violations of their rights arising from the use of digital ID?

The Identity Documents Act fails to set up *any* redressal mechanisms pertaining to the use of the ID. The Electronics Act, which governs electronic identification, requires that a person or authority who suspends or revokes a certificate without legal basis — intentionally or due to gross negligence — must compensate for damage caused.[21] The Personal Data Protection Act identifies the Data Protection Inspectorate as an extra-judicial body to settle complaints from persons whose rights have been violated under the Act.[22] It also sets up a system of fines in case

19 Electronic Identification and Trust Services for Electronic Transactions Act, 2016 ["Electronics Act"].

20 Chapter 4, PDP Act.

21 Section 21, Electronics Act.

22 Section 56, PDP Act.

of violation of rights by the controller or supervising agencies.[23] Compensation may also be payable for violation of rights, under the State Liability Act[24] in case of violations by State while performing public duties, or Law of Obligations Act[25] in case of private parties in contractual relationships. Thus, while the ID system itself fails to set up an adequate mechanism, the data protection framework sufficiently addresses this gap.

There are adequate redressal mechanisms, including compensation for victims whose rights are violated in the use of the ID, in the data protection law.

1.10 ACCOUNTABILITY

Is there an independent/adequate regulatory mechanism to ensure accountability of the administrator of the digital ID?

The Data protection Inspectorate, established under the Personal Data Protection Act, exists as an independent regulator and is empowered to take action against data controllers who violate the Act.

This would presumably apply to the Police and Border Guard Board as well, who is the administrator of the digital ID.

23 Chapter 6, PDP Act.

24 State Liability Act, 2002, accessible at *https://www.riigiteataja.ee/akt/113092011011* [in Estonian].

25 Law of Obligations Act, 2018.

1.11 MISSION CREEP

In case there are newer purposes identified, are there regulatory procedures in place to determine their legitimacy?

No; the relevant Acts that govern the digital ID system do not prescribe the purposes for which data is collected, and in fact encourage the sharing of collected data for new purposes such that duplicate data need never be collected. The Data Exchange Layer of Information Systems Regulation[26], together with the Electronics Act, regulate the agencies that may have access to collected data, but the controls that are in place relate to security and integrity of the data shared, and do not concern the purposes for which they may be used (neither do they entail fresh consent from users).

The Personal Data Protection Act, read with the General Data Protection Regulation[27], impose a purpose limitation on data, restricting its use for reasons other than that of its collection without fresh consent. However, it exempts this obligation if the data collection is permitted by a legitimate law (that is necessary and proportionate in a democratic society). Since the ID framework explicitly allows data collected during the issue of the ID to be used by actors if "there is a legal basis for it," this exception seems to be applied to indiscriminately allow new purposes and actors provided there is legal backing. This fails the purpose limitation test.

The Estonian digital ID framework does not limit the purposes that the ID can be used for, and fails to protect against mission creep.

26 Data Exchange Layer of Information Regulation, 2016 ["X-Road Regulation"].

27 Articles 5-7, General Data Protection Regulation, 2018 ["GDPR"].

RIGHTS BASED TESTS

2.1 DATA MINIMISATION

Are principles of data minimisation followed in the collection, use, and retention of personal data?

The Identity Documents Act does not prescribe a purpose for the creation and issue of identity documents, and therefore allows the collection of a wide range of details including iris images, signature, etc.[28] Further, it permits the specification of required data to be determined by a regulation of the 'minister concerned for the area'.[29] Biometric data is collected during the ID issue process, even though it is not (currently) being used for authentication (or any other) purposes.

The Population Register Act describes as its purpose "the collection of reliable information and grant of access to personal data".[30] This broad and overarching purpose does nothing to enable data minimization. Accordingly, the categories of data it collects is vast and includes ethnic nationality, residence and contact details, details of marital status, custody and voter registration data.[31] Further, all identity documents and citizenship documents are entered into the PR.[32] All the data continues to remain in the PR permanently[33] unless amended or replaced, until the validity of the documents in question. Even after, the data is stored as 'non-actual data.'[34] The PR also contains data on submission of data to PR, access and restrictions to access, etc.[35]

Lastly, since data is collected at every new use of the ID — with its primary purpose being *easy* access to data — and the system is highly interoperable without any need for user consent, it encourages the creation of a large repository of data spanning several categories and purposes. This is different from most other ID system designs, where data collected or accessed is largely for identification purposes, and such data is not permanently recorded for reuse.

28 Section 9, ID Act.

29 Section 20(2), ID Act.

30 Section 4, PR Act.

31 Section 20, 23, PR Act.

32 Sections 21,22, PR Act.

33 Section 8, PR Act.

34 Section 26, PR Act.

35 Section 25, PR Act.

The aim of the system is to collect and share data efficiently such that the ID holder may never have to submit the same data more than once; thus, it becomes difficult to estimate whether only the data necessary to achieve this aim is being collected, as the aim itself is vast and open-ended.

With extensive personal data being collected and indefinitely stored, the digital ID system does not follow principles of data minimization.

2.2 ACCESS TO DATA

Does the law specify access that various private and public actors have to personal data?

The Identity Documents Act does not prescribe or limit access of any (private or public) actors to data collected under the Act. The Statutes for the Maintenance of Identity Documents Database, though only an executive Regulation, regulates access that actors have to data in the Identity Documents Database. It designates the data as for "internal use" and permits employees of the chief processor access to the extent assigned to them for the performance of their supervisory duties[36], as well as to the parties developing or maintaining the database.[37] It is unclear if this party could be a private actor, in which case they have almost unrestrained access to the database, which is regulated by a maintenance or development contract. The Statue also permits employees of the Ministry of the Interior to access the database for the performance of their duties.[38] Finally, the chief processor can grant access to third parties if there exists a "legal basis", and in accordance with the Public Information Act and the Personal Data Protection Act.[39] This is, once again, regulated through a contract concluded between the processor and the recipient.

The Population Register Act, which governs the collection of information that is often used for digital identity, allows access to State and local governments, and natural and legal persons performing *public duties,* as well as legal persons and natural persons with *legitimate interest*. Access is allowed on an application submitted to the population registration information system, and is decided

36 Section 16(2), ID Database Statutes.

37 Section 16(4), ID Database Statutes.

38 Section 16(3), ID Database Statutes.

39 Section 16(5), ID Database Statutes.

based on an administrative Act that determines the purpose of the received data, its transferability to other databases and persons, time limits for processing, and rights and obligations of the applicant, among other factors.[40] The controller, which is the Ministry for Interior, decides the access that a person may have, and this access is typically done through the data exchange layer of the information system (X-Road).[41] The processor rules on the *legitimate interest* of an application to access data (after the person is granted access by the controller) on a case-by-case basis, and allows it only if it does not breach the inviolability of private life or endanger national security.[42] Further, access to data is also categorically refused if it may cause damage to the data subject, or if it is sought for research or advertising purposes.[43] However, according to Section 54 of the Act, this may be overridden by specific consent given by the data subject to the processor in case of a request by the applicant.[44]

X-Road is the primary mode of accessing information from various databases, and is regulated by the Data Exchange Layer of Information Regulation ("X-Road Regulation")[45]. To access information through X-Road, persons have to become members and sign contracts with the Estonian Information System Authority. The Authority can refuse membership if they fail to meet certain obligations prescribed in the Electronic Identification and Trust Services for Electronic Transactions Act[46] (and related EU Regulation) regarding eSeals. There are no restrictions on membership that depend on the nature of duties that the applicant performs, and therefore there is effectively no purpose-related classification of persons or authorities who can and cannot use X-Road to access personal data. An X-Road member will also have to register their sub-system (a particular organisational part of the X-Road system) with X-Road on meeting certain obligations regarding specifying natural person within the member responsible for its functioning, measures appointed to ensure integrity/security of data, etc. These sub-systems can then be accessed by other members of X-road.

The ID framework has in place controls to delineate the access that actors have to personal data, but it also allows for excessive discretion on part of executive bodies.

40 Sections 49, 50, PR Act.

41 Section 48, PR Act.

42 Section 51, PR Act.

43 Section 51, PR Act.

44 Section 54, PR Act.

45 X-Road Regulation.

46 Electronics Act.

2.3 EXCLUSIONS DUE TO DESIGN FLAWS

Is the use of digital ID to access services exclusionary?

Section 18(1)(3) of the Identity Documents Act allows the provider of a public service electronically with the right to require the use of a digital ID card (or digital certificates) for the provision of their service. However, for most other purposes, the digital ID card is simply one of many ways to prove their identity, and the Identity Documents Act does not prescribe any mandates for their use. Further, Estonia has managed to achieve near complete internet accessibility to its population, and therefore does not suffer the typical roadblocks in e-services that other countries do.[47]

The use of digital ID to access services in Estonia is not exclusionary.

2.4 EXCLUSIONS DUE TO FAILURE

Does failure of the ID system lead to exclusion?

Since use of the digital ID is not mandatory but used mainly for the purpose of convenience, failure of the digital ID system does not easily lead to exclusion (provided not many online public services *mandate* the use of the ID, which is consistent with what we have found so far). The Identity Documents Act permits identity to be verified with any valid document that has certain key categories of personal data on it,[48] and thus a resident may easily use a different ID in place of their digital ID. Further, it is the Personal Identification Code issued to every person on the entry of their data to the PR that can be used to link their information across databases, which continues to be usable without the digital ID.

Exclusion may also occur due to inaccurate data, leading to errors in authentication. This is adequately addressed by having in place a mechanism to identify and correct inaccurate data. The Statutes for the Maintenance of Identity Documents Database attributes the responsibility of ensuring accurate data to the provider of data (the applicant) when such data is being submitted, and to the

47 Mari Roonemaa, "Global lessons from Estonia's tech-savvy government," *The UNESCO Courier, https://en.unesco.org/courier/2017-april-june/global-lessons-estonia-s-tech-savvy-government*; *https://e-estonia.com/*.

48 Section 4, ID Act.

controller for accurately recording the data. It also imposes the responsibility of ensuring rectification of incorrect data, on becoming aware of inaccuracy, on the controller. The Population Register Act makes it mandatory for the person submitting the data (typically the authority/person who issued the identity document on the basis of which data is being entered) to ensure the accuracy of data and its compliance with the documents.[49] On being given notice, the processor is required to correct the data.[50] Further, in cases where it is suspected that the data stored is inaccurate,[51] the processor is required to restrict access to such data until such time it is verified and corrected (access must be allowed to persons performing public duties but with the notice of it being inaccurate).[52] However, in both cases, there is no liability imposed in case of inaccurate data or failure of the system. This does not adequately dissuade inaccuracy in data collection, or a failure of the system. There is also no mechanism, or redressal system, in place to safeguard the rights of those who have been excluded due to failure.

Failure of the ID system does not lead to exclusion, largely because use of the ID is not mandatory to access most services in Estonia.

49 Section 32, PR Act.

50 Section 33, PR Act.

51 Section 32(3), PR Act.

52 Section 59, PR Act.

RISK BASED TESTS

3.1 RISK ASSESSMENT

Is the ID system designed taking into account the potential risk of its use?

The design of the ID system introduces potential risk in its use in several ways. The complete lack of a purpose limitation on the use of the digital ID and collected personal data is alarming. The ID system, in the attempt to be highly interoperable and all-encompassing, creates a large repository of personal data of residents. Although this data is collected and stored in a federated manner, the ID documents database and the Population Register collect a lot more data than is seen in analogous digital ID programs. Thus a breach of these databases would gravely impact an ID holder's privacy, in a manner similar to having a central ID database. The use of private actors in the issue and management of the ID, and in offering authentication services, is also a risk-inducing factor to account for.

However, the system is also privacy enhancing in some other ways. The attributes for authentication of identity are restricted to chip-readers and passwords or OTPs, and thus the non-utilisation of biometrics limits the intrusive use of physical or bodily data. In terms of security measures, the Electronics Act (together with the Regulation (EU) No. 910/2014) mandates the active creation of a list of qualified trust service providers and trust services that have to consistently comply with obligations to maintain their status. Further, the Police and Border Guard Board has a Certificate Policy that defines the procedural and operational requirements that Certification Authority adheres to and requires entities to adhere to when issuing and managing the Certificates.[53] Having in place a strong data protection law with an independent data protection authority, and measures to introduce transparency and accountability into the system, are redeeming factors that impact the functioning of the system.

By not having a purpose driven design, or prioritising consent in the use of the ID, the system cannot be said to have been designed taking into account the risks of its use.

53 Id.ee, *"Police and Border Guard Board-Certificate Policy for identity card, digital identity card, residence permit card and diplomatic identity card,"* April 17, 2019, *https://www.id.ee/public/CP_ESTEID_v1.1.pdf*.

3.2 PRIVACY RISK MITIGATION

Is there a national data protection law in place?

The Personal Data Protection Act [54], read with the General Data Protection Regulation [55] governs the use of personal data in Estonia.

3.3 PRIVACY BY DESIGN

Are there privacy by design systems that minimise the harms from data breach?

The framework that governs access to data from the interoperable databases is the the set of laws and contracts that govern the X Road. Regulation No. 331,[56] governing the implementation of the X road, puts in place several privacy by design obligations, and requires a data sharing contract between the administrator and a participant (in the data sharing process) that elaborately sets out rights, obligations, and responsibilities of parties. However, even with these privacy mechanisms, it fails to adequately provide agency to the ID holder in the sharing of their data, as consent is taken only once — at the issue of the ID — and not at every instance their data is accessed. Other privacy by design mechanisms include pseudonymizing of personal data while logging data sharing transactions; anonymizing data when used for analytics; encrypting and requiring digital signatures for the sharing of data; and using blockchain technology for transaction logs to ensure their immutability.[57]

The digital ID framework incorporates some privacy by design systems that minimise harms arising from its use.

54 PDP Act.

55 GDPR.

56 Applying the data exchange layer of information systems, Regulation No. 331, accessible at *https://www.riigiteataja.ee/akt/688079* [in Estonian].

57 World Bank Group, "Privacy by Design: Current Practices in Estonia, India, and Austria," (2016), *https://id4d.worldbank.org/sites/id4d.worldbank.org/files/PrivacyByDesign_112918web.pdf*.

3.4 RESPONSE TO RISKS

Is there a mitigation strategy in place in case of failure or breach of the ID system?

The framework surrounding the ID system does not seem to identify a mitigation strategy for failure or breach of the system. However, the National Cyber Security strategy, read with the Digital Agenda for Estonia, hints at some consideration being given to crisis management in situations of breach: the 2017 National Cyber Security Strategy[58] identifies as a goal the creation of a system of alternate solutions to be used in cases where the normal functioning of ICT infrastructure and e-services, for 'important' services, is disrupted, and for ensuring the uninterrupted functioning of the infrastructure for essential/vital services.[59] Similarly, the Emergency Act and the Cybersecurity Act create a legal framework for responding to and managing risks, though once again it targets cyberthreats and responses with regard to vital services in the public or private sector, and is not specifically tailored toward risks in the ID system.[60] The 2022 Cyber Security Strategy also proposes regular joint cooperative exercises with political leaders and vital service providers to ensure readiness in case of crises.[61]

In its functioning, the Estonian system seems to be responsive to incidents impacting the safety of the ID system; in 2017, when the digital ID card chips were reportedly exposed to an unknown digital vulnerability, the PBGB, along with the Information System Authority and the Ministry of Economic Affairs and Communication, immediately (on being notified) suspended the certification of the Digital ID cards and mandated a an electronic renewal of all IDs.[62]

There is no identifiable mitigation strategy in the ID framework, but the e-governance system itself seems well equipped to handle failures and crises.

58 Cyber Security Strategy 2014-2017, Ministry of Economic Affairs and Communication, Republic of Estonia *https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf* ["Cyber Security Strategy, 2017"].

59 *Cyber Security Strategy, supra,* Page 8.

60 Cybersecurity Act, 2018; Emergency Act, 2017.

61 Cyber Security Strategy 2019-2022, Ministry of Economic Affairs and Communications, Republic of Estonia, *https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf*.

62 "What we learned from the eID card security risk?," e-estonia, last accessed February 11, 2020, https://e-estonia.com/card-security-risk/.

** We are grateful to Katrin Nyman Metcalf for taking the time to review this case study. As remote researchers, the perspectives of a local expert were of immense value to us. We would also note while Dr. Metcalf had disagreements with our approach and its suitability for Estonia, her feedback gave us a lot of insights into digital identity in Estonia.*