Designing an Effective Long-Term Identity Management Strategy for a Mature e-State

Silvia Lips[1](✉), Krista Aas[2], Ingrid Pappel[1], and Dirk Draheim[1]

[1] Tallinn University of Technology, Akadeemia tee 15a, Tallinn 12616, Estonia
{silvia.lips,ingrid.pappel,dirk.draheim}@taltech.ee
[2] Estonian Police and Border Guard Board, Pärnu mnt 139,
Tallinn 15060, Estonia
krista.aas@politsei.ee

Abstract. Countries that have a well-functioning e-governance ecosystem (infrastructure, processes, interoperability network, user-friendly e-services etc.) reach a particularly high e-governance maturity level. To ensure continuous development and adoption to the changing technological environment the systematic consideration of users' needs is important in the definition of long-term strategical goals. Identity management is a corner stone of each mature e-governance ecosystem. This paper focuses on the process of creating the new Estonian strategy for identity management and identity documents and the analysis of this process from different aspects (responsibilities, engaged stakeholders and interest groups, key competences, scope, implementation). In addition, we give an overview of the underlying strategical and legal regulatory framework. The objective is to map the best practices and bottlenecks of the strategy creation process and propose a model for area specific long-term strategical documents. We aim at understanding best practices and bottlenecks in the process of creating the ID strategy. In service of this, we have conducted qualitative interviews with several high-ranking experts that have been involved as stakeholders in the strategy building process. Based on this, we propose a model for area-specific long-term strategical documents. Furthermore, the research results indicate that it is necessary to invest continuously into public-private partnership.

Keywords: Identity management · Strategy building · Electronic identity · Change management

1 Introduction

Estonia has significant experience in the field of e-governance and e-services from almost twenty years. The established PKI (public key infrastructure)-based e-governance system is intensively used. 98% of the Estonian population have an ID-card that hosts an eID (electronic identity) token; and about 2/3 of them use it regularly. During these twenty years, more than 500 million digital signatures has been given and, at the present time, it is possible to use more than 5000 e-services [1].

Since 2002, the system has remained quite similar with only minor changes. In the end of the year 2018, new contract partner started to issue the fourth generation of eID

A. Kő et al. (Eds.): EGOVIS 2019, LNCS 11709, pp. 221–234, 2019.
https://doi.org/10.1007/978-3-030-27523-5_16

documents. It is clear that the whole system has reached to the maturity level where dealing with concrete developments or needs is not sufficient and there is a clear need for an overall framework and long-term development strategy. Therefore, in September 2017, the Estonian Police and Border Guard Board (PBGB) together with the Estonian Information System Authority (EISA) initiated a process at the level of the public and the private sector level to agree on a long-term identity management view. The process lasted almost one and a half years and resulted into a white paper on identity management and identity documents, henceforth abbreviated as IMIDS white paper or just IMIDS for short.

The current article concentrates mainly on the creation process of the IMIDS white paper and not so much on analyzing the content of the document. The aim is to map the best practices and design an effective model for mature e-states who feel the need for a long-term view.

During the process, common understanding on the terminology level is crucial. If we talk about identity management and identity documents, then it is important to understand the meaning of the term “identity management”. There is no single definition of identity management. On a very general level identity management is a security system, which authorizes users to access to certain information or systems [2]. In the current context, identity management means keeping consistent record of a person’s identity and managing it by the state during its whole lifecycle. Identity documents are all documents issued by the state and stated in the Identity Documents Act paragraph 2 Section 2 [3]. It means identity card and digital identity card (including e-residency digital identity card), residence permit card, diplomatic identity card, 7 types of travel documents (passports) and mobile-ID [4].

Taking into account previously described framework, it is important to emphasize that in this article we do not focus only on the electronic part of the identity management because the strategical view is much broader covering additionally physical identity management issues, tokens, physical identity carriers, data protection, security issues etc.

In addition, if we talk about identity management and identity documents strategical view then at the same time, we talk at least partly about the strategic management of related information systems and IT innovation. Therefore, it is important to understand if there is an actual need and will for innovation and this type of long-term strategy. The same question raised during the IMIDS creation process – does Estonia actually want to be an innovative and leading country in terms of identity management and eID. According to the answers, Estonia clearly wants to be a successful e-country, but this also means that the country shall be ready for early adoption of new technologies and/or applications [5]. From that point of view, it is crucial to have a long-term perspective and common understating in the identity management area ensuring the implementation and funding of the innovative ideas, solutions and increase user satisfaction [6].

This article contains three main chapters. Firstly, we formulate the research problem and give methodological background with related frameworks. Then, we give an overview about the identity management and identity documents strategy building process and outcomes and analyze different aspects of the process. Finally, we present the most important and interesting findings.

2 Problem Formulation and Frameworks

2.1 Problem Formulation and Theoretical Framework

Central question of the current article is about designing an effective long-term identity management and identity documents strategy for a mature e-state through public and private cooperation. We analyze different aspects like responsibilities, engaged stakeholders and interest groups, key competences, scope and implementation issues. To support the main theme, we give an overview about the identity management and identity documents creation process, outcomes and propose a model of best practices.

Our research methodology is oriented towards action design research (ADR) as we were involved directly to the IMIDS creation process [7]. After the strategy document was ready, we conducted twelve individual structured non-standardized interviews with public and private sector experts who participated in the process (approximate duration one hour each). Five interviewees from the twelve were public and seven private sector representatives. Some of the examples of interviewees: PBGB head of identity and status bureau, EISA head of eID branch, CEO of SK ID Solutions AS, head of citizen markets of IDEMIA, CEO and vice-president of the Estonian Association of Information Technology and Telecommunications (ITL) etc.

Theoretical background of this article bases on the three main concepts: identity theory [8], change management [9] and public private partnership (PPP) [10]. All previously named concepts relate and supplement each other.

2.2 Strategical and Regulatory Framework

In the context of building the national identity management strategy, it is important to understand what kind of legal and strategical documents already exist and how they influence the area. Political and vision documents that has no direct legal impact and legislative acts having direct juridical impact must be distinguished.

On the state level there are in total 47 strategical documents. They are all different in terms of their juridical status, structure, purpose and their relation to the state budget [11]. Directly connected to the identity management area are only two of them: Internal Security Development Plan (STAK) and Estonian Information Society Development Plan (EISDP).

Internal Security Development Plan has eight sub programs and one of the programs is reliable and secure identity management that contains following three main policy instruments: development of secure and smart solutions, effective and systematic administration and management of the identity area, ensuring high quality personal data [12].

EISDP is more detailed policy document focusing inter alia to the eID area. The main aim of the document is to find smart solutions how to use ICT and solve nationwide challenges [13].

Juridical framework is more determined and has direct binding effect to the parties. Therefore, it is important to have an overview of the existing legal regulations related to the identity management and identity documents area. In addition to that, it is important to remark that new technological approaches and innovative solutions might presume changes in the existing legal environment or even establishing new regulatory framework.

Legal framework in the identity management and identity documents area has conditionally three main layers: pre-juridical framework, international law and EU legislation and state law (Fig. 1).

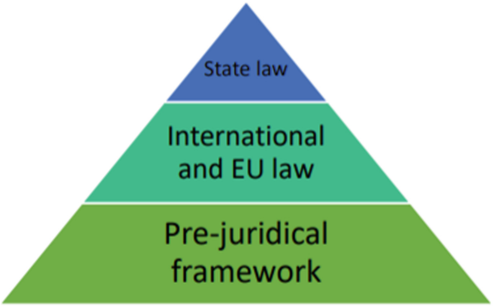

Fig. 1. Identity management legal framework layers.

Pre-juridical framework plays an important role especially in the identity management field consisting different technical standards (ISO, ETSI, PCI etc.) and recommendations (ICAO 9303 etc.) [14]. Even these documents do not have direct juridical impact, they are recognized and accepted worldwide and often used, referenced similarly to legal acts. International and EU law level is a set of different directives and directly applicable regulations that directly or indirectly relate to the identity management area.

On the state level, the main legal acts regulating the identity management regulatory environment in Estonia are Identity Documents Act and Electronic Identification and Trust Services for Electronic Transactions Act [4, 15].

3 Identity Management Strategy Building Process and Outcome

3.1 Strategy Building Process

Estonian identity management field (including eID ecosystem) is complex environment engaging public and private sector expertise and based on a close cooperation of both sectors. It is a well-operating network consisting of different players and roles [16].

During the first half of 2017, EISA initiated to PBGB that they would like to have a long-term view on the eID field. As the topic is wider than digital identity and eID, parties started to build the identity management strategy. 22.09.2017 PBGB and EISA sent an official IMIDS creation proposal to the public sector stakeholders.[1]

Based on the initiative 04.10.2017 public sector stakeholders met in the PBGB. Representatives of three different ministries (Ministry of the Interior, Ministry of Foreign Affairs and Ministry of Economic Affairs and Communications) participated. One of the main concerns brought out in the meeting was the juridical status of the planned strategical document. PBGB and EISA explained that the document becomes an input for already existing political strategical documents. It was clear that public sector did not have a common understanding of different identity management related issues. Therefore, the representatives decided that firstly it is important to achieve common understanding among public sector authorities and then engage private sector stakeholders.

First workshop for public sector stakeholders was 01.12.2017. After brief introduction, the work continued in two main sections: (1) electronic identity and related services (2) physical identity management and related topics. During the first part of the workshop on both sections' participants listed all bottlenecks and shortcomings related to the theme. After that, solution brainstorming followed. The aim was to find innovative solutions to the existing problems and try to think without borders. Finally, both groups presented their results and findings.

Based on the 01.12.2017 workshop results PBGB decided to have one additional internal workshop on 16.01.2018 where all service owners in the PBGB identity and status bureau and one representative of EISA participated. The aim was to think through together once more the broader picture and create links and synergies between different services. Based on the results of these two workshops first draft of the IMIDS was created and sent 02.02.2018 to the PBGB and EISA and shortly after to other public sector stakeholders.

The first draft based on the overlapping part of the mission and vision of the PBGB and EISA, as they are main implementing authorities on the identity management and identity documents field. Second workshop for public sector stakeholders was 03.04.2018. The focus of the meeting was to discuss the received feedback and make amendments to the IMIDS documentation.

01.06.2018 PBGB sent the IMIDS draft to the private sector stakeholders together with a meeting proposal.[2] The meeting was at EISA on 19.06.2018. EISA and PBGB introduced the IMIDS documentation and principles, open discussion followed. Private sector was clearly cautious and expressed their disappointment not being on engaged to the process already earlier. It was clear that there is a need for more meetings.

IMIDS documentation was little bit modified and 06.09.2018 next meeting was held. During the meeting, experts decided to change the document structure. Therefore, the decision was that before planned workshop in October 2018 public and private

[1] Ministry of the Interior, Ministry of Economic Affairs and Communication, IT and development center (SMIT), Tallinn Technical University (TeleTech), Estonian Data Protection Inspectorate, former Technical Regulatory Authority now known as Consumer Protection and Technical Regulatory Authority and Centre of Registers and Information Systems.

[2] SK ID Solutions AS, ITL, Estonian Banking Association, Cybernetica AS, Guardtime AS and IDEMIA - representing the interest of information technology companies.

sector experts meet one more time in a smaller circle. The task was to argue and negotiate new IMIDS structure that is acceptable for the private and public sector.

26.10.2018 final public-private workshop took place. Based on already agreed structure and with the help of outside moderator, experts worked in smaller groups. During the workshop, experts mapped relevant services and roles; identified challenges related with the services and offered possible solutions. In the end of December 2018, new draft version of the document was ready.

On February 15, 2019, EISA presented IMIDS to the e-Estonia Council who supported the identity management, eID and identity documents long-term plan [17].

After one and a half years of work, finally the identity management field had a starting point. Experts started to call the IMIDS as "white paper".

3.2 Process Outcome

IMIDS is a valuable set of area specific principles and guidelines and a starting point for the long-term visioning.

During the discussion experts found that term identity management is too broad, and they defined the document scope as follows:

- Identity of a person attributed by the state;
- Identity life cycle – all processes and activities;
- Identity management – management of data, tokens, Online Certificate Status Protocol (OCSP) service etc.;
- Usage - authentication, digital signature, encryption and decryption functionalities, eesti.ee e-mail address, NFC based services, biometrics;
- Ecosystem and cooperation – public vs private sector, research and development activities.

It means that the IMIDS focuses on the state created identities and does not deal with private sector identity solutions like Google or Facebook identities. Document covers the state created identity whole life cycle management and usage from the physical and electronic perspective.

During the process appeared that public and private sector experts understand and use professional terminology differently. For example, term "identity" had already various meanings and experts used it differently. Therefore, experts agreed most important definitions like identity document, identity carrier and carrier management, information service, clients etc. A separate glossary is a part of the document to increase the level of common understanding among public and private sector experts.

The document itself is twenty pages long and consist of five main chapters:

1. Market and Background (Estonia, EU, international level, service providers);
2. Predictable Future Developments;
3. National Identity Management Pillars and Principles;
4. Services Related to the Identity Management;
5. IMIDS Update Mechanisms.

First two chapters give general overview of the existing market situation and possible future trends on the state and international level. Next chapter is a set of general principles and guidelines for the development activities. Fourth chapter is the core of IMIDS and reflects future development vision of identity management related services.

First chapter contains Estonian identity management and identity documents ecosystem brief overview and description of main players and their roles. Estonian identity management framework bases on four main pillars:

- Clients - physical persons, private and public sector entities;
- Identity carriers/tokens – all ID-1 format cards, eID, mobile-ID, smart-ID, travel documents/passports;
- Channels – service points, e-service portal, phone, development environment;
- Services – personal identification, confirmation of the will of the person, validity confirmation services, identity carrier management (including carrier recognition), information services, official e-mail address, development services, service support etc.

In addition to the Estonian identity environment overview, the chapter contains key points that influence and shape the European Union and international market. One interesting finding was that in past three/four years several international service providers in the security documents market have merged. For example, in 2015, Gemalto AG acquired Swiss company Trüb AG and currently Gemalto AG merger process with Thales Group is almost finished. In 2017, French company Morpho S.A.S merged with Oberthur Technologies currently named IDEMIA. This situation illustrates the consolidation of the technologies and competences and the decrease of competition on the international level.

Second chapter analyses possible future developments that affect identity management and identity documents field. Use of biometrics will be one of the key elements in next ten years. Countries experiment with different technologies and biometric identifiers (face, iris, behavioral features etc.). People dependency from the technology and relative importance of the mobile technologies increase. Smart cities become more popular and the block-chain field of application expands. Increasing IoT numbers cause data exchange overload. In the identity management area important developments in the field of machine learning, mathematical modelling of nervous systems and behavior predictability enable accurate identification from the pictures and videos. By 2035, airports have to be able to serve highly increased number of passengers.

Third chapter presents the identity management basic principles. Estonia is open for innovation and ready to pilot new technological solutions. On the other hand, state ensures readiness to cope with technological crisis and creates risk management plan with mitigation measures. To mitigate the risks the state prefers to purchase ID-1 format documents and travel documents from different companies. There is one central identity management database and state analyses possibilities how to offer identification service to the private sector. State wants to review and re-organize the current eID roles and work allocation. These were only some examples of the general principles.

Identity management and related services is a central part of the strategy. Experts pointed out under every service main challenges and directions. Personal identification service challenges are record keeping and access management, international cooperation, aging of the main information system, service availability, and unmanaged risks.

Experts offered solutions for facing these challenges. For example, finding way to process personal data outside of Estonia, implementing automatic biometrical identification system (ABIS), cooperating with international identity providers (GSMA, CITIC etc.).

Carrier management contains different aspects starting from issuance process to risk management. Identity documents application moves to the electronic environment and state engages private businesses in the identity document issuance process. State plans to implement Artificial Intelligence (AI) based solutions in the working processes and searches effective PKI independent and post-quantum solutions.

In the context of digital authentication and signing, state analyzes the possibility to use Estonian eID in international environments (Facebook, eBay, Google) and builds more services on the Near Field Communication (NFC) technology implemented on the new eID card starting from December 2018.

Identity systems developers need more support and attention. Experts suggested different solutions that help to cope with the changing technical environment. Usage of more standardized solutions is just one example.

IMIDS has no separate juridical power, but it will be an input to other political level strategical documents as Internal Security Development Plan (STAK) in the governing area of the Ministry of the Interior and Estonian Information Society Development Plan in the governing area of the Ministry of Economic Affairs and Communications.

According to the strategy document, public and private sector representatives meet once a year in the last quarter initiated by the PBGB and discuss if the document needs to be changed. The full text of the IMIDS is publicly available in Estonian on the PBGB and EISA web pages [3].

4 Important Findings and Discussions

4.1 General Organization

First part of the interviews focused on the IMIDS organizational side. As a warm-up question, we asked about the experience in the identity management field. All interviewees brought out approximate number of years they have worked in the area. Remarkable was the difference in experience between the private and public sector representatives. Public sector median experience in the area was 7.1 years and the same result in private sector was 19.28 years. It is quite remarkable difference and may be one of the reasons why two sectors have different views on the area.

All interviewees evaluated the necessity of the IMIDS on a ten-point scale, where one meant that the creation of the IMIDS was not relevant and ten referred that the strategy document was very necessary. Median score given by all interviewees was 8.92. Public sector median score was 8.8 and private sector score 9. Mainly, the interviewees said that real actions have to follow; otherwise, the strategy document has no practical value. In addition, it is not necessary to repeat already existing principles. Interviewees also marked that the importance was not only coming from the documented part but from the process itself. Experts had not meet to discuss area related issues already long time. Therefore, it was a good opportunity to create mutual understanding among the public and private sector.

Interviewees had a chance to bring out positive and negative elements regarding the IMIDS creation process. The focus of the question was on the overall process structure, meetings held during the process, e-mail communication etc.

Interviewees found positive that the white paper finally created, and the community was around the table. They also pointed out that possibility to meet between private and public sector representatives in a smaller round was very helpful. All interviewees liked 26.10.2018 workshop moderated by professional.

Based on the received feedback it was clear that there is room for process improvement. Most important takeaways and findings are following:

- Engage professional methodical competence already to the strategy preparatory activities.
- Engage public and private sector representatives at the same time.
- Using iterative workshops format is most effective (as many iterations as needed).
- It is important to answer to all comments made during the process.
- Active participation and presence of ministries and policy makers level is very important.
- Interviewees pointed out that engaging the association level (ITL, Banking Association) was not sufficient.
- Telecommunication service providers (mobile operators), public sector IT houses (RMIT, KeMIT, TEHIK etc.) and experts from standardization authority were according to interviewees missing.
- Identity management and identity documents international level and industry view was missing.
- Too many people from the manager level participated.
- Too long periods between the meetings.

Time planning is another relevant issue in every project context. Therefore, we asked from the interviewees their opinion about the time actually spent (one and a half years). It was very interesting how interviewees' opinions about the IMIDS timeframe differed (the range was 3 months to 1.5 years). Most optimal duration seems to be up to six months. However, it is possible to make the document faster. The question is more about the optimal process planning.

4.2 Substantive Analysis

Last part of the interview concentrated on the IMIDS substantive analysis. During the IMIDS building process one of the questions that raised the debate was the juridical status of the document and on what level and by whom it should be approved. There is probably no right or wrong answer but based on the interviewee answers it is possible to fit the document better in the existing framework.

Most of the interviewees (46%) found that juridical status of the document is not necessary or important until the principles stated in the document adopt by the wider political documents like STAK and Information Society Development Plan. Others found that some kind of juridical or legal approval by the government or on the ministry level is important to ensure the enforcement of the document. Others remained neutral or had no opinion about the topic.

Weather the document approved or not, more important is the actual enforcement of principles. The document is expression of expert opinions and the technical environment changes very fast; therefore, it is reasonable to keep the approval procedure rather simple and flexible. The maximum is ministry level, who can organize the introduction of the principles to the government and make the political selection from the IMIDS principles.

Currently PBGB and EISA led the IMIDS creation process. One of the interview questions was about the leadership of the project. Aim was to understand if this kind of dual leadership earned its purpose or are there any good alternatives. Opinions about the leadership were divergent. Interviewees who did not prefer concrete authority brought out that PBGB and EISA could both lead their area of competence separately. Then of course raises the question who will be responsible for putting together the overall picture. More important was the engagement of all related experts and authorities. To summarize this question, the leadership role can be on the ministry or implementation authority level, more important is involvement of the stakeholders and one responsible institution who coordinates the whole process.

In addition to concrete leadership issues, interviewees mentioned that there should be a centralized methodical competence center on a state level, assisting, guiding and advising the creation of similar expert level white papers. The idea is worth of considering if expert level white papers become more common in public sector.

Interviewees brought out following topics that should have been included to the IMIDS or presented more in detail:

- AI and machine learning development (how to use AI in different processes), because it brings lot of benefits and additional risks that need to be analyzed.
- Identity management of the things (AI-s, robots etc.).
- Risk management and related activities.
- Field of biometric solutions.
- Border crossing technical solutions (how to make border crossing faster and more convenient).
- International dimension representation. More specifically Estonian citizens in the international environment with tokens enabling the identification issued by Estonian public and private sector.
- Real actions planning part and input giving to the other implementation plans.

Strategy building and visioning is only one part of the whole picture, because after finalizing the strategy the real planning and work starts. Therefore, we asked from the interviewees how the IMIDS principles become reality. According to the answers, ministries should take a lead and integrate the principles coming from the IMIDS to STAK and ISDP. It was also emphasized that strong community and stakeholder's own attitude is very important, and all engaged parties should take the principles agreed in IMIDS account while planning future activities. One challenge in the implementation process is building up strong public and private partnership again.

Based on the answers it was possible to create a simplified model of the IMIDS implementation cycle. As first step interviewees found that it would be good to meet shortly in a smaller group of public and private sector representatives, prioritize the actions, and select the most important issues that need urgent handling already during the year 2019. After prioritization, the experts have to describe a 10-step action plan and agree responsible authorities.

In the future, the meetings take place regularly once a year preferably in October or November. During these meetings, parties give an overview about implementing status and upcoming activities for the next and for the year after will be discussed (priorities and responsibilities overlooked or set, activities added or removed etc.). The reason for looking year and year after is the state budget planning principles that have direct influence on the implementation actions.

Close question to the previous one was how to keep the IMIDS document itself up to date. According to the document, experts overlook the IMIDS once a year initiated by the PBGB [3]. Interviewees approached to the question differently. Most of them found that need evaluation once a year is enough. Others found that evaluation shall happen more often or based on a necessity without any excessive administrative burden. They found that the focus should be more on flexibility and community-based interaction.

Based on the feedback we should consider CA/Browser Forum work format-based solution as an alternative. It is a strong and active expert community of certification authorities and Internet browser software vendors discussing and influencing international standards and principles [18]. The possibility to use similar format in Estonian identity management field for the public and private expert's cooperation needs further analysis. Therefore, current research is not concentrating to this particular topic in detail.

Two final questions were oriented to the main takeaways from the process and freely expressed comments if interviewees had any. As follows, we present only those takeaways and observations of the interviewees not already covered in the previous chapters:

- Some of the participants did not realize changed context – people who participated in the process were focusing too much to the historical context and did not realize that the situation is changed, and the same models are not applicable.
- Using the same terminology is important (i.e. the term "identity" is overwhelmed).
- Cooperation between the public and private cooperation has become very complex mainly because of the excessive regulatory environment and the feeling of unity is missing.
- Private sector was more active, interested and contributed more.
- Making this kind of white papers should be a common practice in public sector.
- Academic sector could be the bridge between different sectors.

Based on interviewee's answers to these two questions we noticed two main important conclusions. Firstly, interviewees mentioned multiple times that the cooperation between the public and private sector that once was much closer has become more reserved and complex. Mainly because of the too detailed regulatory framework (standards, laws, policies etc.). One of the solutions to overcome this situation offered during the interview was the engagement of academic sector who could be the bridge between the public and private sector. This idea very interesting but of course the concept, format and readiness need separate analysis.

Secondly, interviewees suggested that the format of such white papers as IMIDS should be more widely used in public sector practice. It means that on the expert level in different areas the cooperation will become more active and documented. This wider view and its applicability need also more detailed analysis. As mentioned previously by one interviewee that in such cases there should be on a state level a methodical competence center who helps to guide the process and keeps track of different existing white papers and their changes.

4.3 Recommendations

Based on the analysis of the interviews and outcomes in combination with change management theory and approaches it is possible to design a model for the area specific long-term strategical documents.

The source of the initiative is not that important but usually it comes from the implementation authority who is working on the expert level on the specific area. As a first step, the implementation authority and responsible ministry shall meet and agree the division of labor, general principles and the list of involved stakeholders. After that, it is reasonable to engage methodical help. The role of the methodical help will be coordination and preparation of the meetings and workshops on a joint and smaller working group's level.

It would be good to have the first meeting jointly with public and private parties. The aim of the meeting is to introduce the initiative, agree main principles, work allocation, further steps and time schedule. In addition, the division of work between smaller working groups has to be agreed. Detailed work with concrete proposals shall continue in smaller working groups. The number of meetings in smaller working groups is not limited.

When the working groups are finished their discussions and formed their concrete proposals, the second joint meeting will take place. It is important to consider all proposals, negotiate if necessary and finally prioritize them. To have a systematic and uniform approach to the topic it would be good to use "why-what-how" technique for establishing a hierarchy for the expressed viewpoints [19]. If one meeting is not enough for that purpose, then it is possible to arrange more meetings until achieving mutual understanding and the public and private representatives confirm that the strategy is ready. After that, the document moves on the political level. The responsible ministry introduces the principles to the government, makes selection from the strategy taking into account the priorities, and integrates them in the political strategy document. Implementation actions will follow.

During the implementation, approximately once a year the implementation status and the principles agreed in the strategy will be gone through by the private and public sector representatives and changed if needed.

In addition to already above-mentioned aspects, it is important to keep in mind following principles:

- The whole process should not take more than six months;

- Uniform use of terminology shall be agreed in the beginning of the process;
- Continuous community building and public and private sector cooperation shall be happening as a parallel process;
- State shall provide centrally methodical help and relation management for sector specific strategies.

4.4 Future Direction

In the future, we would like to investigate the applicability of our findings internationally. Every country is different and therefore it is important to find universal aspects and make generalizations while investigating other mature e-countries. As a concrete next step, we will conduct a project with partners from the Netherlands, comparing the Estonian eID solution with cloud-based eID solution in the Netherlands with respect to eIDAS tiers.

5 Conclusion

Identity management and identity documents area is a complex system influencing almost invisibly different areas of life. Estonia as one of the leading e-countries has reached to the maturity level in terms of e-governance and it is crucial to think through the strategic next steps to bring innovation to the existing environment and retain competitive position on the international level.

Therefore, in the beginning of 2017 Estonian Police and Border Guard Board and Estonian Information System Authority initiated the strategy building process in the identity management area. After one and a half years of public and private sector stakeholder's meetings and workshops identity management white paper was finally ready.

Current article focus is on the previously named white paper building process analysis. The aim of the research was to find the answer to the main research question – how to design an effective long-term identity management strategy for a mature e-state. By using approach oriented towards action design research and based on qualitative individual structured non-standardized interviews in combination with theoretical framework, we proposed a model for building strategies on the identity management and identity documents field.

As strategy building is only one part of the change management process it is important that identity management and identity documents strategy does not remain on paper and implementation actions will follow in parallel with the public and private sector community building activities enabling one-step further as a mature e-state.

References

1. e-Estonia Briefing Centre Homepage. https://e-estonia.com/solutions/e-identity/id-card/. Accessed 21 Feb 2019

2. Laurent, M., Bouzefrane, S., Pomerol, J.: Digital Identity Management. ISTE Press, London (2015)
3. Identity Management and Identity Documents. White Paper 1.0. https://www.ria.ee/sites/default/files/content-editors/EID/valge-raamat-2018.pdf. Accessed 13 Mar 2019
4. Identity Documents Act. https://www.riigiteataja.ee/en/eli/526042018001/consolide. Accessed 13 Mar 2019
5. Peppard, J., Ward, J.: The Strategic Management of Information Systems, 4th edn. Wiley, Hoboken (2016)
6. Muldme, A., Pappel, I., Lauk, M., Draheim, D.: A survey on customer satisfaction in national electronic ID user support. In: Terán, L., Meier, A. (ed.) Piscataway 5th International Conference on eDemocracy & eGovernment (ICEDEG), Piscataway, NJ, Quito, pp. 31–37 (2018)
7. Petersson, A., Lundberg, J.: Applying action design research (ADR) to develop concept generation and selection methods. In: Wang, L., Kjellberg, T. (eds.) Procedia 26th CIRP Design Conference, vol. 50, pp. 222–227. Elseiver, Amsterdam (2016)
8. Tsap, V., Pappel, I., Draheim, D.: Key success factors in introducing national e-identification systems. In: Dang, T.K., Wagner, R., Küng, J., Thoai, N., Takizawa, M., Neuhold, E.J. (eds.) FDSE 2017. LNCS, vol. 10646, pp. 455–471. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70004-5_33
9. Cameron, E., Green, M.: Making Sense of Change Management, 4th edn. Kogan Page Limited, London (2015)
10. Paide, K., Pappel, I., Vainsalu, H., Draheim, D.: On the systematic exploitation of the Estonian data exchange layer X-road for strengthening public private partnerships. In: Kankanhalli, A., Ojo, A., Soares, D. (eds.) 11th International Conference on Theory and Practice of Electronic Governance, ICEGOV 2018, pp. 34–41. ACM Press, Galaway (2018)
11. Development Plans. https://www.valitsus.ee/et/eesmargid-tegevused/arengukavad. Accessed 24 Feb 2019
12. Internal Security Development Plan. https://www.valitsus.ee/sites/default/files/contenteditors/arengukavad/taiendatud_siseturvalisuse_arengukava_2015-2020.pdf. Accessed 13 Mar 2019
13. Estonian Information Society Development Plan. https://www.mkm.ee/sites/default/files/elfinder/article_files/eesti_infouhiskonna_arengukava.pdf. Accessed 25 Feb 2019
14. Järvsoo, M., Norta, A., Tsap, V., Pappel, I., Draheim, D.: Implementation of information security in the EU information systems. In: Al-Sharhan, S.A., et al. (eds.) I3E 2018. LNCS, vol. 11195, pp. 150–163. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-02131-3_15
15. Electronic Identification and Trust Services for Electronic Transactions Act. https://www.riigiteataja.ee/en/eli/511012019010/consolide. Accessed 30 Mar 2019
16. Lips, S., Pappel, I., Tsap, V., Draheim, D.: Key factors in coping with large-scale security vulnerabilities in the eID field. In: Kő, A., Francesconi, E. (eds.) EGOVIS 2018. LNCS, vol. 11032, pp. 60–70. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-98349-3_5
17. E-Eesti nõukogu toetas ID-kaardi ja eidentiteedi 10 aasta arenguplaani. https://www.ria.ee/et/uudised/e-eesti-noukogu-toetas-id-kaardi-ja-eidentiteedi-10-aasta-arenguplaani.html. Accessed 24 Feb 2019
18. CAB Forum Homepage. About the CA/Browser Forum - CAB Forum. https://cabforum.org/about-us/. Accessed 13 Mar 2019
19. APMG-international: Effective Change Manager's Handbook - Essential guidance to the change management body of knowledge, 1st ed. Kogan Page Limited, London (2015)