Notified eID Scheme

Feasibility study for North Macedonia

RegionalCooperationCouncil

Co-funded by the European Union

good.
better.
regional.

Title: Notified eID Scheme
Feasibility study for North Macedonia

Publisher: Regional Cooperation Council
Trg Bosne i Hercegovine 1/V, 71000 Sarajevo
Bosnia and Herzegovina

Tel: +387 33 561 700; Fax: +387 33 561 701

E-mail: rcc@rcc.int

Website: www.rcc.int

Authors: Raul Kaidro

Andres Käärik

Editors: Solza Kovachevska and Sandra Anastasovska

Coeditor: Tanja Maras

Design: Samir Dedić

July 2022

The report is prepared by RaulWalter and with the financial support of the European Commission.

NOTIFIED eID SCHEME

Feasibility study for North Macedonia

TABLE OF CONTENTS

ABBREVIATIONS

The following terms and abbreviations have been used in the document in hand:

Abbreviation	Description
2FA	Two-factor authentication
API	Application programming interface
CA	Certification Authority
CAB	Conformity Assessment Body
CCB	Central Coordinating Body
CRM	Common Regional Market 2021-2024 Action Plan
Digital signature	Qualified electronic signature in context of the current Feasibility Study
EC	European Commission
eID	Electronic identification, in the context of the current Feasibility Study, the eID denotes both electronic identification and electronic signing capabilities
eIDAS	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
eIDAS Node	eIDAS Network connector for cross-border/boundary authentication
EIF	European Interoperability Framework
EU	European Union
GG	Government gateway
IF	Interoperability framework
IOP	Interoperability platform
LOTL	List of Trusted Lists
MAP REA	Multi-annual Action Plan for a Regional Economic Area
MRA	Mutual recognition agreement
PIN	Personal Identification Number - the activation code for using private keys on token

Abbreviation	Description
QES	Qualified electronic signature aka digital signature
QSCD	Qualified Signature Creation Device
QTS	Qualified Trust Service
QTSP/CTSP	Qualified Trust Service Provider/Certified Trust Service Provider
RCC	Regional Cooperation Council
RFID	Radio-frequency identification
SB	Supervisory Body
SEE	South East Europe
SSQD	Secure Signature Creation Device
TL	Trusted List/Trust List
TSP	Trust Service Provider
USB	Universal Serial Bus
WB	Western Balkans

1.

EXECUTIVE SUMMARY

One of the key building elements for successful e-Transformation is a well-functioning, secure, and easy-to-use eID. North Macedonia has made significant progress in transforming the eIDAS legislative framework into economy level legislation, and there is a strong legal foundation in place to implement secure eID schemes with coverage across the economy and with cross-border/boundary acceptance potential.

The existing national ID card does not have any eID or electronic signature capabilities, however the Ministry of Interior is examining options for issuing a new type of national ID card with eID and digital signature capabilities. A mobile-based economy level issued eID scheme with high assurance might also be viewed as a viable option.

The overall objective of the Feasibility Study is to support the Government of North Macedonia in the process of planning an economy level eID solution, which can be accepted cross-border/boundary among the WB economies and could potentially be notified in the EU under eIDAS.

Chapter 3 gives a synoptic overview of eID and trust services related regulatory aspects and implemented due date state of play.

According to the eIDAS levels of assurance, defined in the Commission Implementing Regulation (EU) 2015/1502 pursuant to Article 8(3) of eIDAS Regulation (EU) 910/2014, Chapter 4 provides a detailed overview of three different European Union electronic identity schemes notified at the assurance level "high." The schemes were chosen based on their technical solutions, which included card-, mobile-, and cloud-based options. The German national identity card system, the Estonian mobileID system, and the Belgian itsme system are analysed. Focus has been put on three aspects in all situations to make the schemes more comparable: enrolment, eID solution description, and finally management and organisation. These are the main issues that member states evaluate throughout the notification procedure for authentication schemes.

Chapter 5 describes the main recommendations for National eID system Strategic Positioning and Key Characteristics. Also, national eID system main use-cases and corresponding recommendations in line wit the strategic positioning principles are given.

Chapter 6 introduces the primary components of North Macedonia eID system and outlines recommendations to consider in designing an eIDAS compliant solution corresponding to level 'high'. It gives a general description of each proposed component with relevant general requirements applicable. However, detailed technical requirements should be specified during the ToR preparation process.

The components addressed in the chapter are eID token (carrier), eID issuance process, tasks and role of the Certification Authority and user environments.

Chapter 7 highlights importance and suggestions for the Business and Organisational Models of the national eID system. Based on the global best practices it is of utmost importance that the Business Model is set up in a way to support eID usage in public and private sector.

Chapter 8 describes and analyses potential carrier options for the National eID system and summarises key recommendations as following:

- Considering the currently perceived need to replace the existing National ID card with a new version with electronic capabilities, accelerating growth in e-services development and increasing the need for secure eID means for electronic transactions, it is recommended that North Macedonia considers implementation of both National ID card based and mobile application based Mobile eID;
- As described in Chapters 5-7, Strategic Positioning, Legal and Policy Adjustments, Organisational and Business Models and majority of Key Components are exactly the same for both eID carrier solutions.

National ID card with eID functionality will establish default economy-wide eID coverage and will allow secure online onboarding of mobile application based Mobile eID. Based on best practices the Mobile eID will be very attractive for the private sector, especially for the banking sector and will drive the usage experience;

- National ID card based eID can be an alternative to the Mobile eID for those who do not want to use smartphone, or just prefer using National ID card based eID solution. Also, as importance of electronic transactions in our everyday lives is growing rapidly, it is always good to have alternative solution as a fallback;
- Design and issuance of the new National ID card as a travel document in accordance with ICAO requirements (Doc 9303) to minimise card-reader-related (mass) usage blocks and to maximise National ID card-based eID carrier benefits. Adding biometric information on the ID card significantly expands the ID card usage potential and convenience to the holder, such as the possibility of use in automated boarder control or check in to air flights, just to mention some examples. From eID scheme perspective it creates capability for highly secure online onboarding and renewal of secondary eIDs like mobile-based eIDs which are the most convenient for everyday mass usage and attractive to private sector to integrate into their service offering processes;
- On ID card electronic side, avoid using RFID technology only as it leads to significant investments into readers infrastructure and inconvenience for daily use-cases;
- Use hybrid chip technology instead of combining contact-chip and RFID technologies. Clear rulesets can define what technologies can be used with what applications/use-cases. As explained earlier, contact-chip technology will facilitate the use of ID card based eID for secure authentication and digital signature creation as readers are cheap and easy-to-use compared to the RFID card readers;
- It is highly recommended to implement both solutions in parallel or at least under the same project framework to avoid duplication and interoperability issues. Also, we recommend to add National ID card visual presentation and its validity online check functionalities into the application based Mobile eID. National ID card visual presentation in Mobile eID application without online validation capability is not recommended because it can be attractive for fraudsters.

Chapter 9, Implementation Timeline, gives an overview of all required activities, their dependencies and estimated duration by four sections:

- Strategic Positioning and Requirements section covers the main principles the eIDAS compliant eID system should correspond to;
- Legal and Policy Framework Adjustments section handles questions to be solved in relation to implementing the eID Strategic Positioning;
- Business Model and Organisational Setup section covers topics related to the eID and trust services organisational activities to set up well-functioning organisation and customer support activities;
- Technical Infrastructure and Processes section handles the main activities related to technical and procedural preparation to insure well-functioning eID issuance and TSP services.

2.

INTRODUCTION

2.1. Background

Well-functioning, secure and easy-to-use eID is one of the fundamental building blocks for successful e-transformation. North Macedonia has made good progress to transform eIDAS legislation framework into economy level legislation and there is a solid legal ground to implement secure eID schemes with economy-wide coverage and cross-border/boundary acceptance potential.

National ID card, currently in use, does not have any eID scheme or electronic signature related capabilities, but Ministry of Interior is considering possible solutions to issue new type of national ID card with eID and digital signature functionalities. Also, mobile-based economy level issued eID scheme with high assurance can be considered as a potential solution.

According to the RCC study"Regional Interoperability and Trust Services in Western Balkans, lack of government-issued and recognised eID scheme is one of the main obstacles for full-scale cross border/boundary eID and trust services interoperability implementation. Currently, eID scheme that can be notified with full confidence does not exist in North Macedonia, as notification of eID scheme issued by third party may rise trust issues.

As seen from best practices easy-to-use and secure government level issued eID with high assurance level would be attractive not only for the public sector entities but also for the banking sector, and via increasing usage intensity could significantly support both public and private e-services development.

Furthermore, RCC study states that eID schemes issued by private entities can also be accepted by government or other private entities in service offering processes according to their assurance level, but for government level cross-border/boundary acceptance those eID schemes cannot be notified in line with eIDAS principles. As the notification in principle means taking responsibility for the eID means issued to the certain physical person, the government cannot take such responsibility for eID means issued by third parties towards other governments.

2.2. Objectives and scope

The overall objective of the Feasibility Study is to support the Government of North Macedonia in the process of planning an economy level eID solution, which can be accepted cross-border/boundary among the WB economies and could potentially be notified in the EU under eIDAS. To do this, due consideration was given to the current state of play in the economy, as well as the EU best practices, exploring successful implementations in three EU MS.

The scope of current Feasibility Study includes:

- Developing proposals for potential economy level notified eID scheme under eIDAS, introducing best practices and approaches from the EU;
- Providing expert advice on resources needed to implement the proposed solutions.

The scope covers descriptions and recommendations regarding all important areas related to the implementation of eID system on economy level, including Strategic Positioning, Key Characteristics, Key Components, Main Use-Cases, and Business and Organisational Models.

3.

OVERVIEW OF THE CURRENT SITUATION

3.1. Legal Perspective

North Macedonia has made good progress to transform eIDAS legislation framework into economy level legislation. In September 2020, the Law on Electronic Documents, Electronic Identification and Trust Services (LeDEIDTS) and relevant bylaws came into force and from the legal perspective North Macedonia is fully compliant with eIDAS.

Article 20 of the LeDEIDTS prescribes that eID schemes and trust services provided by trust service providers, established within the EU are legally recognised in North Macedonia without additional requirements which the trust service providers, established in EU, must meet, so that they should be legally recognised at economy level[1].

With regards to bilateral treaties on mutual recognition of trust services, North Macedonia has signed bilateral treaties with Serbia and Montenegro. Due date operational level activities have been initiated with both economies and as a result the Trust Lists of North Macedonia and Serbia are mutually integrated. That is a good example of practical implementation of the mutual recognition of trust services based on bilateral agreement.

Currently, under the coordination of RCC, there is an ongoing project to identify mutually beneficial cross-border/boundary use-cases between all WB economies. Those identified use-cases will form a practical ground on which mutual recognition of eID schemes and trust services will be built.

National Interoperability (IOP) Framework was adopted in 2015, and new IOP platform was launched in 2016. It is mandatory for all government entities to interconnect their information systems via IOP, and from 2019 private companies are allowed to be connected to the IOP when defined security requirements are met. This in fact facilitates economy level interoperability and forms solid ground for fast digitalisation of services, both public and private.

The findings lead to a conclusion that from the legal perspective, there are no barriers to interoperable cross-border/boundary services including use of electronic identification and trust services.

3.2. Implementing Practice - State of Play

The designated supervisory body for electronic identification and trust services in North Macedonia is the Ministry of Information Society and Administration and has been operational since June 2020. As part of the ministry's website, there is a trusted[2] website which provides a good overview of eID and trust services regulation related documents. Actual information is available for:

- Register of Trust Service Providers and Electronic Identification Schemes[3] (Register), containing information on:
  - Electronic Identification Service Providers and Electronic Identification Schemes;
  - Qualified Trust Service Providers (Register of QTSP);

1 Assessment of the Level of Approximation of the Legislation of the Western Balkans Economies with eIDAS and Interoperability Readiness. Law and Internet Foundation. 2019. Reference Number 032-019.

2 North Macedonia, Ministry of Information Society and Administration, list of trust service providers - https://trusteid.mioa.gov.mk/registar_listi/

3 https://trusteid.mioa.gov.mk/en/home/register-and-lists/

- Trust Service Providers (Register of TSP).

- List of Means for Creating Qualified Electronic Signature or Qualified Electronic Seal.[4]

Currently, some links do not open correctly and will be fixed in the nearest future. To support practical interoperability with other economies and EU MSAs the above website is available in English.

As at mid of January 2022 there are four registered eID schemes in the Register. Three of them correspond to the assurance level 'high', offered by Evrotrust Technologies DOOEL Skopje, Clearing House Clearing Interbank Systems AD Skopje (KIBS AD Skopje, trademark OneID) and Ministry of Information Society and Administration (MISA). eID scheme registered by MISA for the Public Revenue Office has assurance level 'low'. The existence of several eID schemes make a good basis for eID economy-wide take off, but it should be considered that availability of useful e-services, usability and business models of eID schemes have all significant impact on the eID usage take off speed.

National ID card, currently in use, does not have any eID scheme or electronic signature related capabilities, but Ministry of Interior is considering possible solutions to issue new type of national ID card with eID and digital signature functionalities. Also, mobile-based economy level issued eID scheme with high assurance can be considered as a potential solution.

Currently, there is no economy level node for linking eID schemes used on economy level as there is no need for such a node.

There are four QTSPs in the Register are:

- KIBS AD Skopje, offering Qualified Timestamp, Qualified Signature issued on QSCD and non QSCD, Qualified Seals issued on QSCD and non-QSCD, and also Cloud Signature services. Qualified certificates for private and professional use are available for HDD of the PC and PKI tokens;
- Makedonski Telekom AD offering Qualified Timestamp, Qualified Signature issued on QSCD and non QSCD and Qualified Seals issued on QSCD and non-QSCD services for various use-cases;
- Inbox DOOEL offering qualified electronic archiving of signed documents;
- Kontego DOO offering qualified electronic archiving of signed documents.

Qualified electronic archiving of signed documents is additional qualified trust services introduced by domestic legislation beyond the eIDAS scope.

Government services portal has built-in electronic signing/sealing functionality, but in general the End User Software and API solutions for service providers to authenticate and create/validate electronic signatures are not well developed. User software of one QTSP is not able to validate QES created by means of other QTSP. Lack of easy-to-get and easy-to-use User Software and API solution components can be considered serious obstacle for e-services take-off and eID schemes and electronic signature usage in service offering processes. Creation of economy level eID and trust services interoperability is a prerequisite for corresponding cross-border/boundary - implementation.

National Interoperability Platform (IOP) is well designed and ensures end-to-end encryption and central logging of all messages. Implemented IOP forms a solid ground for the government to push forward e-services development. Currently, close to total of 800 services are available, out of which over 150 are electronically available and there are several roadmaps to continue with intensive digitalisation. All new public e-services

4 https://trusteid.mioa.gov.mk/wp-content/uploads/Listi/Lista_Sredstva_20201126_final.pdf

on the national e-services portal are interconnected with IOP, while there are still many government information systems not interconnected via IOP.

In summary, there are several key components necessary for cross-border/boundary eID, trust services and service level interoperability in place, practically implemented and operational. Lack of government-issued and recognised eID scheme might constitute significant obstacle to speeding up e-transformation and full-scale cross-border/boundary eID and trust services interoperability implementation as there is no such eID scheme that North Macedonia can present for notification with full confidence.

4.

EXAMPLES FROM EU

This chapter provides a detailed overview of three different European Union electronic identity schemes notified at the assurance level "high" according to the eIDAS levels of assurance, defined in the Commission Implementing Regulation (EU) 2015/1502 pursuant to Article 8(3) of eIDAS Regulation (EU) 910/2014. We have chosen the schemes based on their technical solution, representing card-, mobile- and cloud-based solution. We have analysed German national identity card scheme, Estonian mobileID scheme and Belgium itsme® solution. To make the schemes more comparable, in all cases we focused on three aspects – enrolment, eID solution description, and finally management and organisation. These are the main topics that member states assess during the authentication schemes notification process.

Analysis of the eID schemes is based on the official publicly available materials and documents provided by the EU MS.

4.1. ID card based eID (Germany)

Germany issues national identity cards since 2010. Germany notified their eID scheme on the level "high" under the eIDAS regulation on 26.09.2017.[5] The German eID is based on government-issued smart cards (eID cards) containing certified contactless chip and on the Extended Access Control v2.

Germany issues two types of eID cards:

- German identity cards (*Personalausweis*) issued only to German citizens regardless of their country of residence.

- Residence permit cards (*Aufenthaltstitel*) issued to non-EU nationals residing in Germany.

Both types of eID cards contain an eID functionality that enables secure electronic identification of natural persons based on a two-factor authentication. Digital signature functionality is not included by default on the eID cards and card holders can purchase digital signature certificate and corresponding key-pairs from certified service providers. This means that digital signature component is not handled as part of government provided eID infrastructure, and it can be argued that it has restrictive impact on e-services take off in Germany.

5 https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Germany

The German eID user environment consists of a computer (e.g. desktop PC, notebook, tablet, cell phone, etc.), eID Client software and a certified RFID card reader. Certified RFID card reader adds additional security layer to transact with the eID card but on the other hand it forms a significant cost component of the user environment and makes it almost unreasonable for personal wide-scale usage.

Applicable main legal environment:

- eIDAS regulation;[6]
- Act on Identity Cards and Electronic Identification (Gesetz über Personalausweise und den elektronischen Identitätsnachweis - PAuswG);[7]
- Act to Promote Electronic Government (Gesetz zur Förderung der elektronischen Verwaltung – EgovG);[8]
- Act on Residence, Employment and Integration of Foreigners in Federal Territory (Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet – AufenthG).[9]

4.1.1. Enrolment

Applicants from the age of 16 can apply for German ID cards on their own and do not require the consent of their parents. Germany recognises different kinds of documents as identity evidence. For foreigners, authorities can verify the presented documents against samples provided in various databases and check the plausibility of the person's information in the foreigner records. If a foreigner's identity cannot be verified with a sufficient degree of certainty, the Resident Permits will be issued with no activated certificate. Germany does not allow remote identification.

The responsible issuing authorities issue German eID in accordance with the procedures defined by the applicable national laws. The issuing authority captures the necessary personal data of the applicant and subsequently transmits these data to the eID card manufacturer. The card manufacturer produces and personalises the eID card. As part of production the manufacturer produces a PIN letter, containing an initial randomly generated activation PIN, together with a PIN unblocking key (PUK) and a revocation password. The card manufacturer sends the PIN letter to the applicant.

Responsible issuing authority delivers the German eID card in person to the applicant or to a person authorised by the applicant to receive the card.

4.1.2. eID Solution Description

The German eID is ID-1 format card, corresponding to the International Civil Aviation Organisation (ICAO) specification Doc 9303.[10] The eID card contains a contactless RFID chip that communicates in accordance with the international ISO[11] standards. The technology of the German eID is based on the Federal Office for Information Security (BSI) standard TR-03110 that specifies security mechanisms for machine-readable

6 EUR-Lex - 32014R0910 - EN - EUR-Lex (europa.eu)
7 PAuswG - nichtamtliches Inhaltsverzeichnis (gesetze-im-internet.de)
8 EGovG - nichtamtliches Inhaltsverzeichnis (gesetze-im-internet.de)
9 AufenthG - nichtamtliches Inhaltsverzeichnis (gesetze-im-internet.de)
10 https://www.icao.int/publications/pages/publication.aspx?docnum=9303
11 ISO/IEC 14443 and ISO/IEC 7816

travel documents and eIDAS token. BSI document TR-03127 defines detailed system architecture of the German eID.[12]

The German eID card uses two-factor authentication. The contactless RFID chip stores the personal data and the relevant keys that enable authentication. The card holder must enter 6-digit PIN to start the authentication process.

From the technical side, the German eID is based on a modular system of technical specifications and protection profiles that defines all necessary interoperability and security requirements within this framework.

The RFID chip of the German eID includes an eID application and the following personal data of the card holder:

- Family name;
- Name at birth (optional);
- Given names;
- Doctoral degree (optional);
- Date of birth;
- Place of birth;
- Address;
- Type of document;
- Expiry date;
- Service- and card-specific identifier (pseudonym);
- Indication whether the card holder is older or younger than a particular age;
- Indication whether a place of residence matches the requested place of residence;
- Religious name/stage or pen name (optional).

The German eID is characterised by end-to-end cryptographic protection for the whole path from the eID card to the middleware operated by the eIDAS connector. Mutual authentication is provided where the eID card verifies an authorisation certificate issued to the middleware operator (at the relying party or a centralised eIDAS connector), vice versa the middleware verifies the eID card.

The authentication mechanism of the German eID is called the General Authentication Procedure containing the following steps:

- PIN Verification via PACE;
- Mutual authentication via Extended Access Control v2;
- Validity check and reading personal data.

Figure 1 below presents the detailed description of the general authentication procedure.[13]

12 BSI - Technical Guideline BSI TR-03127 - BSI TR-03127 eID documents based on Extended Access Control, Version 1.40 (bund.de)

13 https://ec.europa.eu/cefdigital/wiki/download/attachments/48762401/2017_02_20_German%20eID_01_Whitepaper_final.pdf?version=1&modificationDate=1499172188962&api=v2

Online authentication with the German eID is based on a direct mutual authentication between the relying party and the user.

The online authentication process flow consists of the following steps:

- The holder of the German eID requests a web service that requires an authentication;
- The service provider sends an authentication request to the eID-Server and activates the eID Client via the user's application (e.g. browser);
- The eID Client is redirected to the eID Server of the service provider;

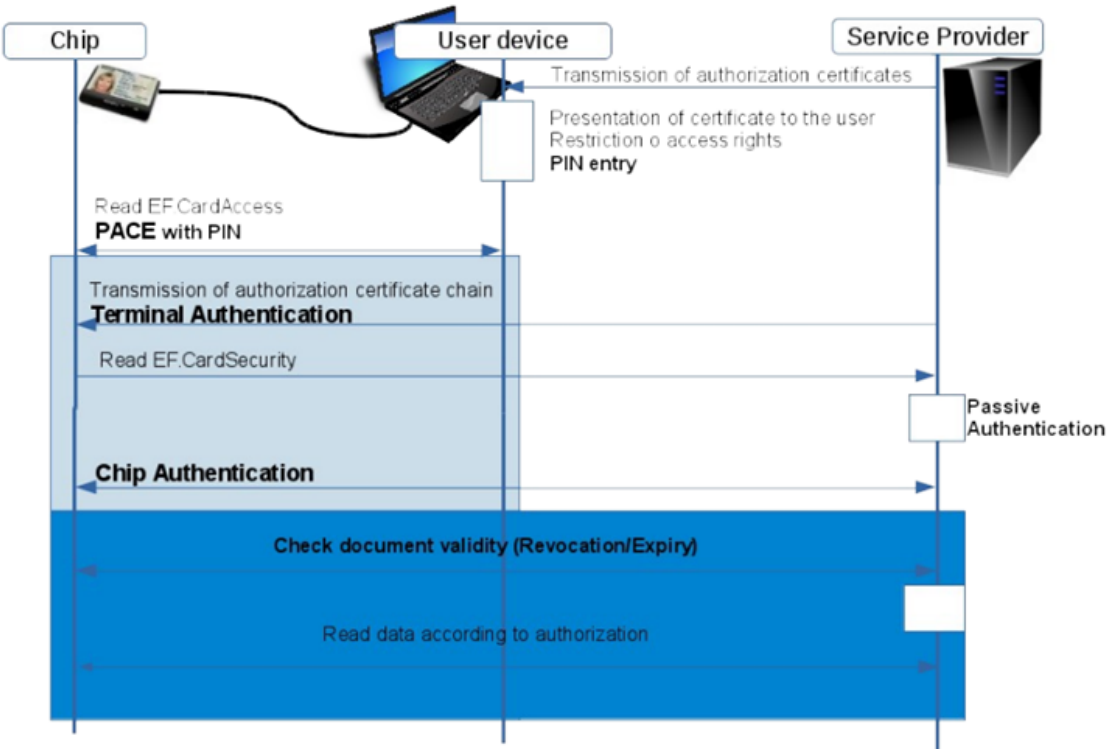

Figure 1. Description of the general authentication procedure

- The eID Client enables the holder of the German eID to view the information on the service provider and the corresponding access rights. The holder of the eID may deselect particular access rights or deny authentication;
- The holder of the eID gives consent to the authentication process and proves the required 'knowledge' by entering the PIN;
- The General Authentication Procedure is performed. As part of the authentication, the eID-Client verifies that the certificates of the web session fit with the authorisation certificate of the relying party. Only after successful verification are the relevant personal data transmitted from the German eID to the eID Server;
- The eID Server transmits the authentication response containing the corresponding personal data to the service provider and redirects the eID Client back to the web session;

- The service provider checks the authentication response and the corresponding personal data and decides whether to give the holder of the German eID access to the requested service.

4.1.3. Management and Organisation

The German federal government is the provider of German national eID scheme governed by federal law and subordinate regulations. All entities providing services for the scheme are either public authorities or private entities contracted by such authorities, which have a direct responsibility to fulfil certain functions in the scheme.

According to the eIDAS regulation, all participants providing a service related to electronic identification in a cross-border/boundary context shall have documented information security management practices, policies, and approaches to risk management in place. In Germany, Federal Office for Information Security (BSI) is mainly responsible for IT security related activities and information security management system. The *Bundesministerium* des *Innern* is responsible for the German eID scheme, and the IT Security Plan is applicable to all relevant IT components and entities providing such services of the scheme.

4.2. SIM card based Mobile eID (Estonia)

Estonian *Mobiil-ID* solution is a SIM card based mobile eID solution enabling authentication in electronic environments and digital signature (qualified electronic signature) creation over a mobile phone. Estonian *Mobiil-ID* solution is available to users since April 2007. Estonia notified their *Mobiil-ID* authentication scheme on the level "high" under the eIDAS regulation on 07.11.2018.

Mobiil-ID is an additional eID carrier that national ID card and residence permit (RP) card owners can use.

Certificates for electronic authentication and digital signature creation on National ID card, RP and *Mobiil-ID* are handled as electronic documents issued on national level and are tied to the identity management on national level. All public entities are obligatory to accept digitally signed documents.

Applicable legal environment:

- eIDAS Regulation;[14]
- Identity Documents Act;[15]
- Electronic Identification and Trust Services for Electronic Transactions Act;[16]
- Certificate Policy for Mobile ID of the Republic of Estonia;[17]
- Certificate, CRL and OCSP Profile for Personal Identification Documents of the Republic of Estonia.[18]

4.2.1. Enrolment

Mobiil-ID is a voluntary to have eID promoting easy-to-use capabilities for national level issued electronic documents. Mobile operators (MO) issue the *Mobiil-ID* to holders of an Estonian ID card or Estonian resi-

14 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
15 https://www.riigiteataja.ee/en/eli/501112021001/consolide
16 https://www.riigiteataja.ee/en/eli/518102021002/consolide
17 https://www.politsei.ee/files/sertifikaatide-kasutustingimused/2018/sk-tcu-esteid-en-20180701.pdf
18 https://www.skidsolutions.eu/en/repository/profiles

dence permit (RP) card upon their request. Only natural persons can apply for the *Mobiil-ID*. It is possible to apply for *Mobiil-ID* only in person to ensure accurate identification of an applicant. In case of expiry, loss or theft, the owner of *Mobiil-ID* is obliged to inform the mobile operator without undue delay.

When a person applies for a *Mobiil-ID*, MO personal checks the applicant data against the identity documents database. The identity documents database provides information about the personal data of the holder of a document (including a facial image) and the validity of the presented document. The personnel of the MO verifies whether an identity document provided by a person is valid, whether the photo and the person presenting the identity document match. MO personnel checks the validity of a document physically and against the identity document database.

The MO personnel introduces the basic terms and conditions related to the use of the eID means of *Mobiil-ID* during the application process. The recipient signs physically (or with a qualified electronic signature) the *Mobiil-ID* contract, acknowledging and accepting the terms and conditions, confirming also that the received SIM card is not damaged. MO archives the signed contract together with the evidence of identity proofing provided in the contract. The terms and conditions of certificates are referred to during signing of the *Mobiil-ID* contract, publicly available on the certification service provider (CSP) website.

After the receipt of the *Mobiil-ID* SIM card from the MO, the person should activate his/her electronic authentication and digital signature certificates on the website of the Police and Border Guard Board responsible for the identity management on the national level. Activation can be done with ID card or RP respectively and is an important step to tie issued electronic documents to the identity management on national level.

4.2.2. eID Solution Description

Mobiil-ID is a SSCD/QSCD SIM-card based solution relying on the Estonian PKI-based eID scheme. It is secure and easy-to-use solution for electronic authentication (eIDAS level high) and qualified electronic signature creation. The certificates of *Mobiil-ID* are valid for up to five years.

There are four private keys on the *Mobiil-ID* chip:

- Two keys for electronic authentication (one with RSA and one with ECC algorithm);
- Two keys for providing a qualified electronic signature (one with RSA and one with ECC algorithm).

The private key is stored in a secure module of a microchip on the SIM card. A two-factor authentication is required for using *Mobiil-ID*: a SIM card and PIN codes to use the private keys. The private key is stored in a secure module of a microchip on the SIM card.

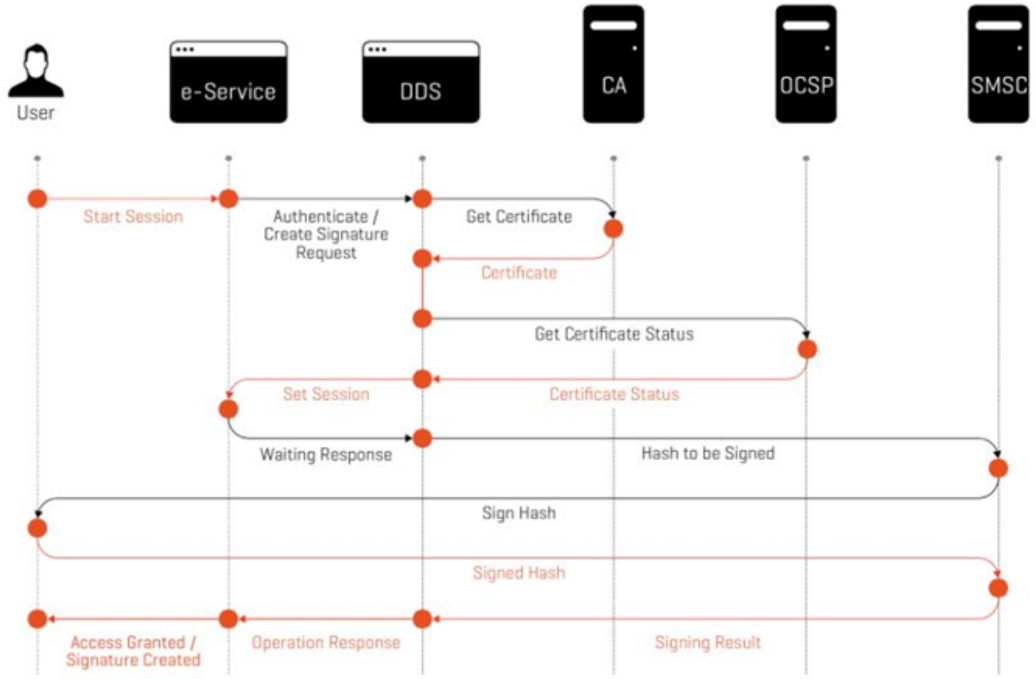

Figure 2. Description of the *Mobiil-ID* authentication procedure

The private key is under the sole control of the user, which prevents guessing, eavesdropping, replay, or manipulation of communication. For authentication, it is required to insert initiation credentials to the e-service authentication session which can be the user's mobile phone number and/or personal identity code and/or username or any combination of those. Figure 2 presents the detailed description of the *Mobiil-ID* authentication procedure.[19]

4.2.3. Management and Organisation

Public and private sector authorities participate in the management of the Estonian eID scheme. The Estonian Police and Border Guard Board is responsible for identity management on national level and issuing personal identification documents, and performs the functions of a point of single contact under eIDAS regulation. The Information System Authority (EISA) is responsible for eID technical architecture, development of client/end-user software and chip technical specification, application for eID middleware and cybersecurity incident management. Private sector authorities provide certification service, certificate validation and time-stamping services, etc. and are responsible for personalisation of *Mobiil-ID* SIM cards.

Security and risk management:

- The user can check the history of use of one's certificate through a self-service portal if the OCSP service is used (available 24/7);
- For emergency patches, there are separate, secure procedures which require involvement of independent parties (CA, Card producer, RA);

19 https://ec.europa.eu/cefdigital/wiki/display/EIDCOMMUNITY/Estonia?preview=/62885749/65972515/EE%20eID%20LoA%20mapping%20-%20Mobiil-ID.pdf

- It is possible to revoke all certificates immediately in case of a large-scale security breach;
- It is not possible to renew Mobiil-ID certificates without replacing the SIM card due to the lack of functionality to generate a new pair of keys on the card.

4.3. Application based Mobile eID (Belgium)

Belgium notified their mobile application-based authentication scheme FAS/*itsme®* on the level "high" under the eIDAS regulation on 18.12.2019. The scheme consists of the Belgian government's Federal Authentication Service (FAS) and a digital identity solution called *itsme®*. The solution was developed by Belgian Mobile eID, a consortium of leading banks and mobile network operators. Royal Decree of 21 December 2017 recognised *itsme®* which has been integrated into FAS since January 2018. Belgian solution enables authentication in electronic environments and qualified electronic signature.

itsme® scheme is based on an open ecosystem that allows different parties to become a member of the scheme in three different roles:

- Identity Registrar - to provide the secure process to identify *itsme®* users and provide up-to-date identity information;
- SIM Controller - to provide the additional hardware security element to raise further security. Telecom providers that are "Full Mobile Network Operator" can act as SIM Controllers;
- Service Provider (direct customer) or Value Added Resellers (indirect customer) to offer *itsme®* services on web-applications, platforms or apps.

Figure 3 provides a holistic overview of the *itsme®* scheme.[20]

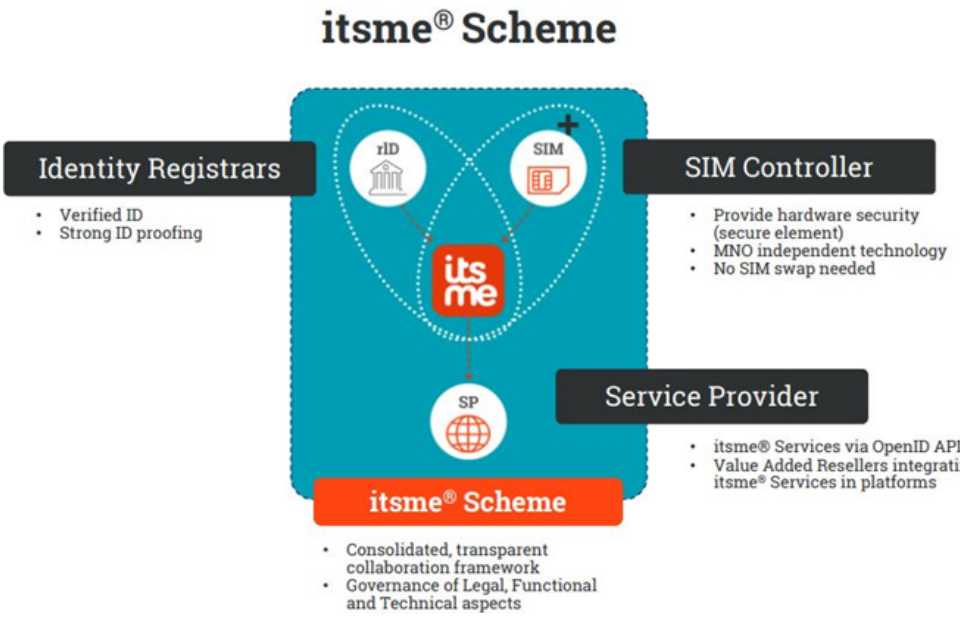

Figure 3. Overview of the *itsme®* scheme

20 https://www.itsme.be/files/10000-Rulebook-General-Policy-1.5.3.pdf

As *itsme®* identity is issued by the private company, it is not tied to the identity management on national level. However, via eID notification process Belgian government has taken the responsibility in front of other EU member states that the person presenting *itsme®* eID is the person he/she claims to be.

Applicable legal environment:

- eIDAS Regulation[21];
- Royal Decree of 22 October 2017 setting forth the conditions, procedure and implications of the recognition of electronic identification services for public applications[22].

4.3.1. Enrolment

Any resident older than 18 years with a Belgian eCard ID or a Foreigner eCard, a SIM card from Belgian mobile operator and a mobile phone can create an electronic identity with *itsme®*.

There are two possible ways for the enrolment:

- Bank enrolment, where Belgian Mobile ID (BMID) reuses the face-to-face registration data of the client (end user) that was collected in a bank during the Know Your Customer (KYC) procedures;
- Remote identity verification, where the user has his/her Belgian Citizen eCard or Foreigner eCard remotely read out by BMID or one of its Identity Registrars and signs an agreement document electronically with the same Citizen eCard or Foreigner eCard by entering his/her eCard authentication and digital signature creation PIN codes respectively during the identity verification and digital signature creation process.

In both cases, the identity proofing is based on the verification of Citizen eCard or Foreigner eCard.

During bank enrolment, the user is requested to indicate his/her agreement with the itsme® terms and conditions via the use of card reader and M2 CPA EMV confirmation or equivalent. During eID self-enrolment, the user accepts the terms and conditions by signing digitally the terms and conditions document and privacy policy using Citizen eCard or Foreigner eCard.

4.3.2. eID Solution Description

The authentication flow between the *itsme®* user and the FAS, using the *itsme®* App, is based on the OpenID Connect standard. Figure 4 below represents the federation framework of OpenID.[23]

21 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

22 Publications | BOSA (belgium.be)

23 https://bosa.belgium.be/sites/default/files/publication/file/techspecshandbook_v1.0_20171106.pdf

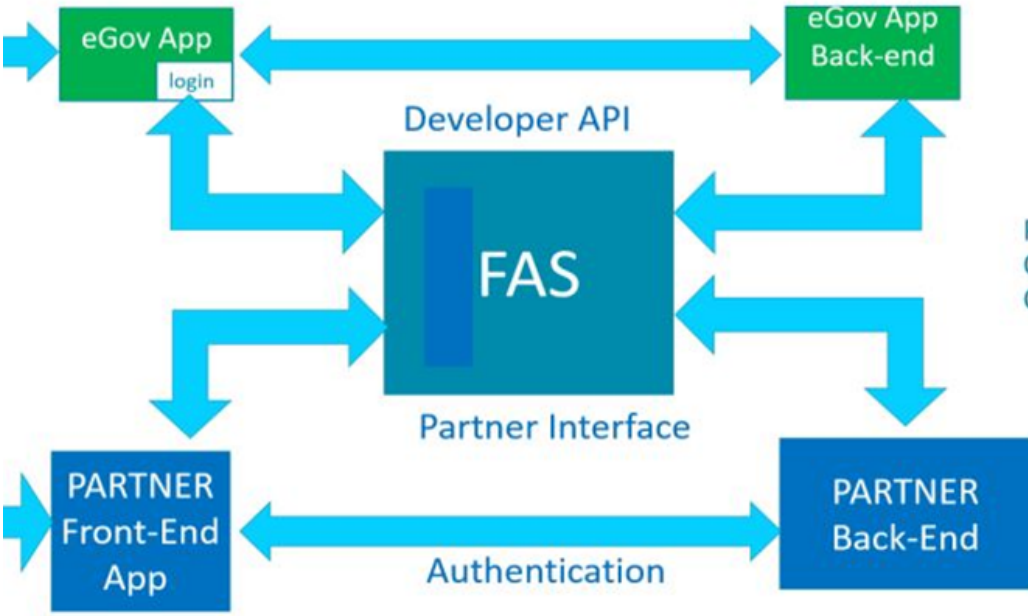

Figure 4. *itsme®* federation framework of OpenID

Detailed integration requirements are set in the technical specifications handbook related to the Royal Decree of Recognition of Partner's Electronic Identification Services issued by BOSA (Belgian national agency for Public Service Policy and Support).[24]

FAS is a gateway that supervises identification and authentication of users, without interacting with the app's internal processes. The Belgian eIDAS node is implemented as part of FAS. It means that users can use *itsme®* to authenticate and log-in to other EU member states' online services that are connected to the eIDAS network.

The diagram in Figure 5 outlines the communication flow that takes place between the (end) user, customer, CM Identity Services and *itsme®*.[25]

During the *itsme®* authentication flow, the browser redirects the *itsme®* users browser to the *itsme®* login page with the authentication context, where it requests the mobile phone number (MSISDN) from the *itsme®* user. The MSISDN is the unique identifier for this *itsme®* user, *itsme®* app instance as well as the device on which it is installed (1 Unique itsme®

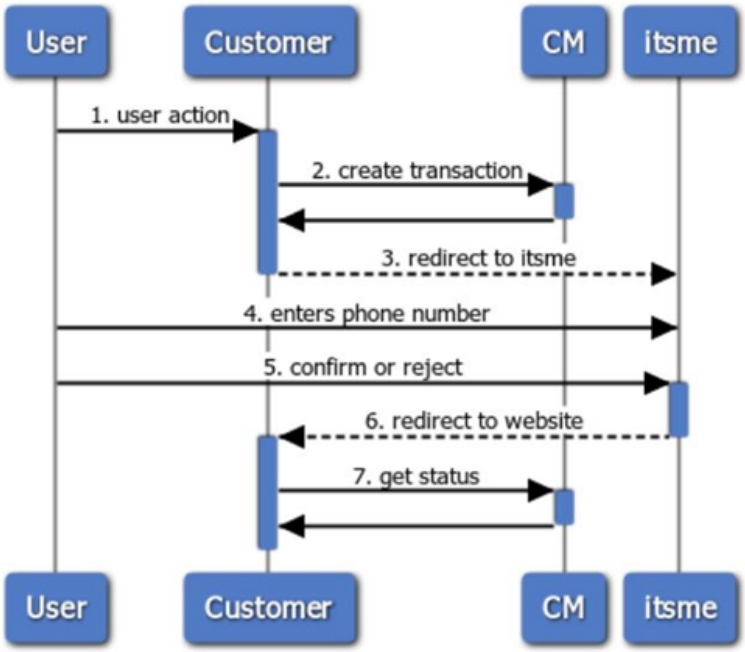

Figure 5. *itsme®* communication flow

24 https://bosa.belgium.be/sites/default/files/publication/file/techspecshandbook_v1.0_20171106.pdf
25 https://docs.cmdisp.com/itsme/CM_itsme_implementation_guide.pdf

user = 1 MSISDN = 1 Device = 1 App). The central *itsme®* service will request the *itsme®* app to answer a challenge for which the user enters the correct *itsme®* PIN (or uses the correct fingerprint if that was configured by the user). Based on the response received, including the device and/or SIM fingerprint information, the login transaction is validated and approved.

Figure 6 below illustrates the *itsme®* workflow from the user perspective.[26]

Belgian Mobile ID is a Qualified Trust Service Provider for validation of seals and signatures, accredited by the Belgian Supervisory Body.

4.3.3. Management and Organisation

Federal Public Service Policy & Support/ Directorate General for Digital Transformation (BOSA / DG DT) are responsible for the Belgium FAS/*Itsme®* eID scheme. BOSA/DG DT develops, manages and operates the Federal Authentication Service (FAS). Belgian Mobile ID NV/SA (BMID) is responsible for issuance and operations of the Belgian Mobile ID itsme® Login Services and mobile app (*itsme®*).

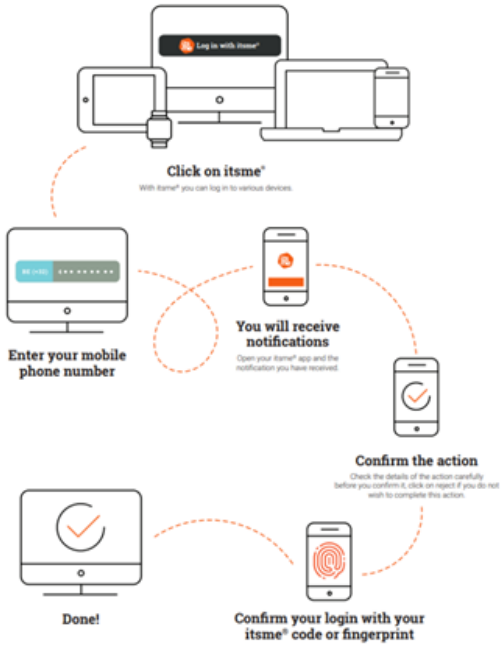

Figure 6. *itsme®* workflow from the user perspective

26 https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=227083826

5.

STRATEGIC POSITIONING OF THE NATIONAL eID

Nationally accepted North Macedonia's eID[27] can be considered one of the main building blocks of a contemporary e-Governance, and by-default element for simplifying the use of e-services on economy level and to remove the borders/boundaries between the RCC participants and EU member states. It should enable the trustful identification of persons in electronic environments and facilitate legally accepted digital signatures.[28] North Macedonia's national eID is expected to facilitate public and private entities to transfer their services to e-channels, and minimise physical visits to the service centres. It can be argued that the main reasons hindering e-Transformation in North Macedonia are absence of easy-to-use and easy-to-get economy level accepted eID and lack of user friendly environments, including APIs for service providers, facilitating the economy-wide eID usage.

Based on best practices, North Macedonia's national eID should be ideally characterised by the following capabilities:

- **eID and all its components (i.e. carrier, software, application) are implemented following the principle "easy to get and easy to use" in different service environments;**

  People should be able to use the eID in all governmental electronic channels. Simplicity is a key - no special technical skills are required to get and use the eID.

- **100% penetration among North Macedonia residents;**

  Government provides proper incentives for users to use electronic channels, which are clearly more cost-effective for service providers. Legislation should allow to distinguish government fees based on service offering channels, and allow applying lower fees to electronic channels. Some services directed to most active user groups could be accessible only via electronic channels to motivate the usage.

- **Comprehensive public services are digitised and accessible through eID;**

  All public services are available through electronic channels and accessible via nationally accepted eID means. eID is the primary electronic authentication method for all government institutions.

- **The most frequently used private sector services (banking, utility services, etc.) are accessible through eID;**

  eID has a legal basis, and technical and operational capabilities strong enough that private sector entities like banks, insurance companies, telecoms, utility and other companies with large and intensive user base will trust and implement the eID into their service offering processes.

- **Supporting "Once-Only" principle that applies to all public services at all levels;**

  When using eID, all public sector digital services should be accessible to users as end-to-end services. Operationally, this means that a user applies for a service once and receives defined result in electronic form. Users do not have to be involved in the information exchange between government entities in the process of the provision of public services. Service offering processes should work seamlessly for users.

27 In the context of the current Feasibility Study, the eID denotes both electronic identification and digital signing capabilities.

28 The term "digital signature" (i.e. digi-signature, digital signing, etc.) should be understood only as a signature that is legally valid and legally equivalent to a handwritten signature. This means that the identity of the user and the background of the issuer of the certificate have been verified and that the time of issuance of the signature is precisely fixed. To put it plainly, it has been identified who signed it and it is ensured that no third party has changed the document to be signed since it was signed (https://www.id.ee/en/article/digital-signing-and-electronic-signatures/)

- **eID is widely used in public sector internal processes;**

  The best indicator of trust towards the eID is internal use by all North Macedonia government entities. This means eID is used internally in all government entities and in inter-entity transactions, as well as for any exchange or transmission of information between the public sector authorities. Therefore, eID usage should be mandatory for government entities.[29]

- **eID consists of electronic identity and digital signature as separate and clearly distinguishable functions;**

  eID could also include means for information encryption and anonymous authentication, but those functions can be covered by using electronic identity means and proper attributes in the service provision processes.

  Similarly to the physical world, identifying oneself and signing are clearly different procedures with different legal consequences. To ensure better public understanding, the same principle should apply in the electronic world. To ensure better legal certainty and assurance, the electronic identity and digital signature should not be separated only at user interface level, but also at technical level.

- **eID as integral part on the identity management on economy level;**

  To ensure high level of assurance and level of trust, it is highly recommended to handle eID as integral part of the identity management on the economy level. This means that certificates located on the economy level issued eID means (ID card and/or mobile devices) should be deemed as electronic documents issued by the government to all entitled residents. In terms of legal entities, these always have natural persons acting as representatives and entity certificates should be tied to corresponding persons.[30]

- **eID has national and cross-border/boundary acceptance.**

  Economy level issued eID should be made mandatory for all government entities to accept. To ensure effective cross-border/boundary usage, the solution should fully correspond to eIDAS framework - electronic identity/electronic authentication should be notified by the government on level 'high', and digital signature solution should match to the qualified electronic signature and meet Qualified Signature Creation Device (QSCD) requirements.[31] All necessary infrastructure components and procedures should be certified in line with eIDAS framework and requirements.

29 In the context of eIDAS Regulation, recital 69 stresses that the Union institutions, bodies, offices and agencies are encouraged to recognise electronic identification and trust services covered by the Regulation for the purpose of administrative cooperation capitalising, in particular, on existing good practices and the results of ongoing projects in the areas covered by the Regulation.

30 Conditions for binding between the electronic identification means of natural and legal persons and the electronic identification means of a legal person ('binding') are set down by secondary eIDAS legislation, and more specifically in Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of eIDAS Regulation. Available: https://eur-lex.europa.eu/legal-content/EN-ET/TXT/?from=EN&uri=CELEX%3A32015R1502.

31 The process of selecting the appropriate standards can be identified according to European Telecommunication Standardisation Institute (ETSI) TR 119 000 and ETSI TR 119 400.

5.1. Main Characteristics of eID System

It is recommended that the North Macedonia national eID should have the following main characteristics:

- North Macedonia's eID system must provide secure authentication and digital signature services for Government, Businesses and Physical persons (G2G, G2B, G2C, B2C);
- The eID means shall be recognised as a Qualified Signature Creation Device (QSCD) under eIDAS framework;
- eID system should support the mobile initiatives. Taking into account the mobile devices market trends, electronic identity and digital signature should not be tied to specific hardware such as a SIM-card;
- eID system should be interoperable with existing eID-s systems in the EU, based on eIDAS Regulation and North Macedonia's legal framework;
- Electronic identity and digital signature certificates must be tied with the physical identity as much as possible. It is recommended to treat these as integral part of the identity management on economy level;
- Technical solution and organisational procedures must ensure highest level of fraud protection (fraud proof) and non-compromisability;
- The solution should be easy-to-use in web as well as in mobile environments for authentication and for signing;
- To increase the usability, the users should not be required to have additional devices for electronic authentication and/or digital signature creation;
- The solution should have a convenient and intuitive user interface;
- Minimal interactions should be required for authentication and/or digital signature creation. Transaction security should be ensured at the same time;
- The user should have full control over the electronic authentication and digital signature creation processes. It should be technically impossible to carry out those procedures without the user's consent;
- The solution should be easy to obtain. Utilisation of mobile technologies and existing service infrastructures provides appropriate prerequisites to that end;
- The solution should support different mobile as well as service provider infrastructure platforms;
- The solution should target maximum re-use of existing infrastructure components, technology systems and procedures;
- The solution should make use of universal and standardised components to help ensure support for cross-border/boundary usage;
- The technical solution and operational procedures must ensure high availability and security as electronic identity and digital signature are critical infrastructure components;
- Users must be provided with well-functioning 24/7 customer support via multiple channels such as web, phone, email and live chat.

5.2. Main Use Cases

eID mean consists of key-pairs and corresponding certificates for authentication and e-signature creation. Authentication key-pair can be also used for encryption/decryption functionality.

This chapter outlines four main use cases of eID in the context of eIDAS Regulation, namely:

- Electronic authentication;
- Digital signature creation;
- Digital signature verification;
- Data encryption/decryption.

These eID use cases are universal and applicable in all business processes and transactions where electronic involvement is preferred or even required by law - regardless of whether these are related to public services, interactions between individuals, or constitute concluding an agreement between several private sector entities. Thus, the potential of properly functioning eID is notably wide and covers - without limitations - all possible formats in terms of G2G, G2B, G2C, B2C communication, and transactions. Remarkably, electronic authentication functionality can be easily integrated into all business processes, where identification of a natural person or entity is required. Importantly, the process corresponds exactly to the procedures we used to apply in a conventional world where any person - natural or legal - has to present his/her/its identity document to be identified prior to applying for a service or entering into a transaction. Further, the digital signature creation functionality can be integrated into all business processes where a person's signature is required to confirm his/her will or consent.

5.2.1. Electronic Authentication

Electronic authentication means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed.[32] Secure and trusted electronic authentication is one of the key components to be in place to offer end-to-end e-services, especially those which have legal or financial effect or are related to sensitive personal data.

eID for authentication must:

- Provide an universal key to access all government and possibly private business e-services;
- Be usable for both web- and mobile-based service environments;
- Be tied to the physical identity at economy level, best if it will be handled as an integral part of the identity management on the economy level;
- Have high assurance level so that frequently used private e-service providers (like banks, insurance companies, telecom operators) will accept and implement support to it.

To facilitate easy-to-use principle, Single Sign On (SSO) across all public service environments should be used as per service provider acceptance.

With respect to the authentication mechanism through which the natural or legal person uses the electronic identification eID means to confirm its identity to a relying party, eIDAS secondary legislation - Commission

32 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910&from=EN#d1e736-73-1

Implementing Regulation 2015/1502 - sets out the requirements per assurance level.[33] According to the eIDAS framework, the security levels of authentication solutions are low, substantial and high.

One of the key requirements of eIDAS Regulation is the obligation to ensure that all EU residents have access to public e-services provided by the public sector on equal terms with their own residents. This means that if a citizen is required to provide an authentication solution when logging in to the e-service portal, authentication solutions with an equivalent level of security from other EU Member States, which have been officially notified by the Member States, must also be accepted. In practice, this means that if the portal accepts solutions with different levels of security (e.g. password card, ID card), all EU Member States' solutions must be accepted that are higher than the lowest that the portal requires from a resident, assuming that the national solution is described in the list of eID solutions in the EU Member States.

The eIDAS regulation leaves room for acceptance of low-level solutions. However, this does not mean that if, for example, a resident is required to have a low or high level of authentication, then only a high level can be required from an EU resident. In this case, authentication of EU residents with a substantial level of collateral must also be accepted.

To access an electronic public service provided by the public sector:

- Service/portal administrators must assess the threats and risks that may arise from implementing different levels of authentication;
- Service/portal administrators must define an access policy for their services that sets the conditions for authentication security levels to access the service. Also, risk mitigation measures set for the service when setting the conditions of access should be considered;
- The service access policy must be applied to all users - both economy and EU residents;
- When compiling the technical solution and architecture, the authentication normative must be established, and relevant information on security standards, where applicable, must be followed.
- In order to enable cross-border/boundary authentication, the SSO solution may be considered in the service/portal to make them more convenient to use.

On the Estonian example, the Estonian Information System Authority has provided the following guidelines for setting the level of authentication when ensuring access to e-services in the public sector:

1. If there are no personalised services in the portal and there is no benefit for the user, then the requirement for authentication should be avoided (authentication is not to satisfy the opinion of the service administrator/administrator/owner).
2. When logging in to the portal, the level of security of authentication solution required by the most demanding service provided by the portal (the minimum level of this service) must be required.
3. If the portal contains different services with different minimum levels of security for identification, and want to ensure access to different levels of solutions, then each must verify that the required level of security has been met when granting access to the service.
4. If the portal requires authentication for the collection of statistical data or for any other reason that does not process personal data or provide a service to a specific person, a low level of authentication shall be sufficient.

33 Sec 2.3 of Commission Implementing Regulation 2015/1502. It should be noted that international standard ISO/IEC 29115 has been taken into account for the specifications and procedures set out in referred eIDAS implementing act, as being the principle international standard available in the domain of assurance levels for electronic identification means.

5. Where a service is provided on the portal which provides a personalised service, but does not involve personalised benefits, substantial level is deemed to be sufficient.
6. If it is possible to access user's sensitive personal data on the portal, then a high level of authentication security should be required.
7. If personalised benefits can be obtained through the service provided on the portal, a high level of security must be required.
8. If the service provided on the portal is likely to cause economic or reputation damage to the person or to the service provider, a high level of security must be required by default.
9. When using a third-party authentication service, always validate the level before the service offered by the portal is opened to a person (trust, but control).[34]

5.2.2. Digital Signature Creation

Digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents and gives a recipient very strong reason to believe that the message was created by a known sender, and that the message was not altered in transit (integrity).[35] A digital signature corresponds to requirements for advanced electronic signature (AdES) and qualified electronic signature (QES) laid down in eIDAS Regulation, whereas a qualified electronic signature shall have the equivalent legal effect of a handwritten signature. Thus, a digital signature is a narrower concept than an electronic signature and falls within the latter.[36]

Digital signature should:

- Be applicable to all digital public services and where handwritten signature is required. Replacement of the physical visits to service centres will give significant cost savings for entire society. Remarkably, the Estonian Certification Centre conducted a cost-benefit analysis of digital signing, which demonstrated that it entails remarkable financial benefits, e.g. by replacing handwritten documents with digitally signed ones Estonia has saved over 200 million euros;[37]
- Be equal to the handwritten signature;
- Be legally accepted by all government entities;
- Be legally accepted by courts and other law enforcement entities;

34 Available: https://www.ria.ee/sites/default/files/content-editors/EID/eidas-autentimistasemed.pdf

35 https://en.wikipedia.org/wiki/Digital_signature. Importantly though, eIDAS Regulation does not recognise the term "digital signature", and defines "electronic signature" instead that means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign (art 3 (10) of eIDAS Regulation).

36 In Estonia, digital signature and qualified electronic signature are synonyms by nature. QES is an e-signature which is based on the qualified certificate (issued by qualified TSP) and is created by a qualified electronic signature creation device. Qualified certificate ensures that the certificate is issued to the person identified by physical presence. Qualified signature creation devices shall ensure that the private keys remain under sole control of the certificate holder.

37 http://www.eturundus.eu/digital-signature/ Digital document cost-profit calculator: www.eturundus.eu/digital-document

These calculators are helpful tools for institutions and companies which sign contracts with their clients, partners and suppliers or exchange other formal documents (subscriptions, acts, invoices, etc.). (Reference: www.sk.ee)

- Support signing different file formats not limited only to .pdf format.[38] Less limitations are better for implementation;
- Enable to add signature to already signed document or file;
- Enable to sign several documents or files at the time (more productive than physical signing procedures).

ETSI (European Telecommunication Standardisation Institute), which is mandated to establish the conditions for achieving the interoperability of eSignature at a European level, by defining and providing a rationalised European eSignature standardisation framework, has specified procedures for creation of AdES digital signatures in ETSI EN 319 102-1.[39] The referred standard introduces general principles, objects and functions relevant when creating or validating signatures based on signature creation and validation constraints and defines general classes of signatures that allow for verifiability over long periods.

5.2.3. Digital Signature Validation

Digital signature validation means the process of verifying and confirming that the digital signature or a seal is valid,[40] that the message was created by a known sender, and that the message was not altered in transit.

Digital signature validation is an organic and integral part of the digital signature management process and should:

- Provide signature validity information in a simple and understandable manner;
- Contain information of signatory, content authenticity and signature creation time;
- Provide other signature related relevant parameters:
  - Signatory's certificate issues;
  - Signatory's certificate;
  - Signature method;
  - Signature format;
  - Signature policy;
  - Signing time (timestamp);
  - Validity proof of the certificate used for signing (OCSP response).

38 Previous report of the project revealed that ID card related end-user software is currently available only for Microsoft Windows based desktop computers. Signature creation is possible only for .pdf format documents using Adobe Reader. No other format is supported for digital signing. Also, multiple documents can't be signed simultaneously (page 15 of the first report).

39 https://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf

40 Article 3(41) of eIDAS Regulation. There are varieties of ways to implement the signature validation procedures, such as:

running as (part of) an application software on a device like a PC with a graphical user interface; as a web service; a web application; a command-line tool; an integrated library or a middleware for other applications. (ETSI EN 319 102-1 V1.1.1).

In terms of requirements applicable to the validation of QES arising from eIDAS framework, Article 32 (1) of eIDAS Regulation stipulates that the process for validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature provided that:

- The certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I of the eIDAS Regulation;
- The qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;
- The signature validation data corresponds to the data provided to the relying party;
- The unique set of data representing the signatory in the certificate is correctly provided to the relying party;
- The use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;
- The electronic signature was created by a qualified electronic signature creation device;
- The integrity of the signed data has not been compromised;
- The requirements provided for in Article 26 of eIDAS Regulation were met at the time of signing.

Article 26 of eIDAS Regulation sets the requirements for advanced electronic signatures, which also constitute baseline requirements for QES and AdES/QC level signatures. Namely, advanced signature should meet the following requirements:

(a) It is uniquely linked to the signatory;

(b) It is capable of identifying the signatory;

(c) It is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

(d) It is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

Further, Article 28 and Annex I of eIDAS Regulation establish additional requirements for qualified certificates for electronic signatures.

5.2.4. Encryption/decryption

Sometimes sensitive information should be transferred via electronic channels. To increase the confidentiality during the information exchange some type of information or documents could be encrypted before using electronic communication channels.

For information encryption/decryption dedicated key-pair can be used, but to reduce the number of PIN codes to remember authentication key-pair can be used instead. From the information security point of view there is no difference if the same level of cryptography is used and according to the best practices it is rather recommended, because less PIN codes users should remember leads to the lower probability they start to write down their PIN codes onto insecure media such as notes or paper tags on the wallets.

It is highly recommended that encryption/decryption means related to the national eID are used solely for short term encryption purposes, like information exchange via electronic channels. For documents and

information that should be stored in encrypted format for longer periods, other technical solutions where back-up keys can be created should be used to avoid unexpected information loss.

6.

KEY COMPONENTS OF NATIONAL eID SYSTEM

This chapter introduces the primary components of North Macedonia eID system and outlines recommendations to consider in designing an eIDAS compliant solution corresponding to level 'high'. It gives a general description of each proposed component with relevant general requirements applicable. However, detailed technical requirements should be specified during the ToR preparation process.

The components addressed in the chapter are eID token (carrier), eID issuance process, tasks and role of the Certification Authority and user environments.

6.1. eID Carrier

eID carrier is one of the key components of the eID ecosystem. It is tightly related to the security, in particular, how to maintain personal data of the user under one's own control, and how to use different verified attributes to access a range of services as and when needed. Only information that needs to be shared should be exchanged, and the identity proofing using multiple pieces of personal information should only happen once. On the other hand, and in relation to user experience, the easy-to-use principle is important to facilitate maximum coverage in the use of eID.

Thus, those two features - security and easy-to-use - should both get maximum attention in the course of establishment of the national eID system.

Electronic identity and digital signature means can be installed onto various carriers like ID cards/smart cards, SIM cards, memory sticks, mobile applications, etc. or kept partly in a secure cloud environment. Currently, as described in Section 4, mainly ID cards and SIM cards are used for the economy level issued strong eID means, also some cloud and mobile application based solutions have been implemented.

6.1.1. Identity Document

Presently, eID schemes attached to the physical identity document can be considered most commonly known eID means. As a rule, electronic identity and digital signature credentials are integral part of the national identity management. However, some, like Germany, may handle digital signature credentials separately from the identity credentials. In case of eID means issued by the government, it forms a solid ground for a higher trust level, as it is the issuer's responsibility to ensure that the eID means are properly tied to the persons and used accordingly.

One of the advantages of ID card-based eID is that ID card as economy level identity document is well-perceived to be handled with care and usage principles are set by legislation. This approach expands also to the eID, and people are handling ID card-based eID means more carefully compared to memory stick, SIM-card or cloud based eID means. The negative side is that traditionally people do not use their ID card on daily basis and thus efforts may be required to change the habits and practices to foster the usage of eID. However, if PIN codes are handled with care and security systems are well developed it should not create major problems.

ID card-based eID means require additional physical hardware deployment (which will increase logistics concerns and costs). Thus, establishing ID card readers infrastructure is identified as one of the challenges to achieve eID massive usage. However, if ID cards have contact-chip, the readers are affordable for most population and can be even distributed free of charge along with the ID card. Also, they are small to carry and easy to use via standard USB interface.

ID card with contactless chip can give some advantage in durability if there is a need to use the chip several times per day. Yet, this solution does not have any other advantages. Moreover, contactless chip-readers

are way more expensive (50-150 euros) and are unlikely be subsidised to promote and support eID usage widely. Also, it can be argued that carrying the readers is likely to be considerably inconvenient - thus they can be installed in service offering points, as one option. Overall, this approach does not support widespread eID electronic usage that should be independent of time and location.

6.1.2. Mobile ID

Mobile communication has undergone tremendous development during the last decades and mobile devices, and smartphones in particular, have become commonly used devices amongst majority of the population, even in developing countries. In service development area, mobile environments are becoming the highest priority to ensure 24/7 availability. Mobile/smart phone is the last thing people forget to take with them and is the first one they notice is missing. In that regard, it is a natural development that the electronic identity and digital signature means should be easily and securely usable with mobile device. Mobile identity services are expected to be used across many sectors, from banking to public services. Mobile-based systems have the advantage of offering convenience and security.[41]

SIM-card based Mobile-ID solutions were first on the market more than a decade ago, as SIM-cards offered equivalent technical security components compared to the chip-based ID cards or tokens. Given that mobile devices with the e-SIM functionality are starting to take off, SIM-card based solutions should be considered rather old-fashioned ones, and thus implementing these in the national eID ecosystems may likely have negative impact on early adopters market segment.

Recommendations

> ***Mobile-based eID that is securely tied to the identity management on economy level can be considered to be the best option to ensure people can have easy-to-use and secure eID to access both public and private services.***
>
> ***Mobile-based solution should be designed in a manner to keep the private keys under the sole control of the user. The mobile devices do not need special purpose hardware (such as smart-card readers or Trusted Platform Module chips) and special purpose SIM-cards. The Smart-ID App works with regular devices and does not require extraordinary permissions. Shared-key solution, where part of the private key is kept in mobile device and another part in highly secure HSM module on back-end side, could be one option to ensure the user's maximum control over the private keys.***
>
> ***ID card-based solution can be planned as alternative to the mobile-based for those who do not want to use smartphone, or just prefer using national ID card-based eID solution.***

6.2. eID Issuance

eID issuance process forms an important and integral part to ensure desired assurance level of the eID means. To support the e-government development vision and to achieve North Macedonia's eID scheme to be accepted by other WB economies and also EU Member States in a longer run, it is highly recommended

41 eIDAS Compliant eID Solutions. ENISA 2020.

that the eID means should correspond to the assurance level 'high'. If eID issuance is tied to the identity management on economy level and is issued with high assurance level, corresponding electronic identification and digital signature certificates can be defined in the domestic legislation as electronic breeder documents and thus, it is easier to make them mandatory to be accepted by all public institutions. Government-issued easy-to-use eID with high assurance level would be very attractive for banking sector and will significantly support both public and private e-services development via increasing usage intensity.

National ID card, currently in use, does not have any eID scheme or electronic signature related capabilities, but Ministry of Interior (MOI) has started preparations to issue a new type of national ID card with eID and digital signature functionalities.

In terms of certification of identity providers issuing eID means, standards (against which certification is possible) could be followed by identity providers or third parties involved in the eID means management for compliance:

- ISO/IEC 27001:2013 for fulfilment of requirements on information security management, record keeping, facility and staff and technical controls;
- Relevant ETSI standards such as ETSI EN 319 401 and ETSI EN 319 411-1 and ETSI EN 319 411-2.

Those standards, if relevant, could eventually be referred to in the domestic legislation.

Recommendations

Economy level issued mobile-based eID could be one of the most cost-effective eIDAS compliant eID solution for North Macedonia, as importantly, there is no need to invest in relatively expensive, time-consuming ID card readers infrastructure inconvenient in everyday usage. To issue mobile-based eID means with high assurance level, a person's identity must be verified with high accuracy before the eID activation. It can be done over the counter in all MOI service centres following the procedures that are similar to the processes of issuing national ID cards and/or passports.

As another option, establishing self-service workplaces in all or selected MOI service centres could be considered. Persons' identities can be verified by using their ID cards and fingerprint biometrics stored in MOI database. This kind of self-service workplace does not require significant investments, since these would consist of a standard PC, basic ID card MRZ (machine-readable zone) reader and fingerprint reader. The software part does not require notable developments and 1:1 fingerprint biometrics verification is not complex either. Thus, fingerprints could be used to validate an identity enrolling to eID.

Also, well-proven solution is to use the biometric passports for mobile-based eID enrolment procedure. Facial biometrics stored in the biometric passport RFID chip is compared with online selfie photo, and validity of the passport issuer certificate is checked. When adding passport and personal numbers online verification then all high assurance level issuance requirements are met.

Recommended options are secure and cost-effective that can be applied not only for initial mobile-based eID credential activation, but also later for credential renewal, if necessary.

> ***eID issuance procedures should be designed in line with eIDAS framework requirements applicable to eID means with high assurance level.***
>
> ***When the new type of ID cards with eID and digital signature functionalities are being issued, it is recommended to consider to add the mobile-based eID issuance into the same procedure to save valuable time and increase perceived importance of the mobile-based eID.***

6.3. Certification Authority

Certification authority (CA) is a functional part of a TSP, an entity that issues digital certificates and is a central trusted body of the PKI based trust network. In electronic communication, third parties can rely on presented digital certificates persons are the ones they claim to be reliable.

Summing up the best practices, the main services offered by CA consist of:

- Certificate issuance;
- Certificate validity verification;
- Activation of certificates (termination of suspension);
- Suspension of certificates;
- Revocation of certificates.

In addition to certificate lifecycle management related services, Certification Authority's trust services portfolio may contain:

- Time-Stamping Service, which certifies the existence of specific data at a certain point of time. It is, therefore, widely used in digital signing or archiving documents. Time-Stamping Service is protected by digital signature to ensure that no one is able to change the data once it is recorded and confirmed with trust service provider's time stamp. It shall be noted that Time-Stamping Service could be provided by separate Trust Service Provider who is not dealing with CA functions at all.
- e-Seal certificate issuance/management to certify digital documents/content and can be used by legal persons acting both in the public or private interests. It proves that electronically transferred documents or information originates from the sending institution. e-Seal ensures that the respective institution is associated with the specific document and the document has not been altered in the meantime. e-Seal can be used both with or without digital signature. Using the certificate for e-Seal along with the person's digital signature one can be certain that the person who signed the document/content is authorised to sign documents/content on behalf of the respective institution.
- Certificate for Authentication for identifying legal persons or for ensuring the originality and completeness of electronic data. The certificate is used for authenticating clients on websites, in e-mail exchange systems or other data processing systems.

Recommendations

> ***CA issuing certificates to the eID means should be eIDAS certified as qualified trust service provider in accordance with the requirements laid down, inter alia, in Article 24 of eIDAS Regulation.***

To facilitate eID usage, the CA should offer full set of main services listed above.

CA as a trust service provider should draft and publish several documents such as Certification Hierarchy, Trust Services Practice Statement, Certification Practice Statement, Certificate Policies, etc. to demonstrate how the chain of trust is built up and how the trust services are offered. Requirements are laid down in General Policy Requirements for Trust Service Providers of the ETSI EN 319 401 standard.

CA could be the government entity, private entity, or set up based on PPP-model. It is crucial that the entity has motivation and necessary resources to build proper organisational routines, technical infrastructure and service portfolio described above. Simply put, the qualified trust service provider should be trusted in all means, starting from fulfilling all regulatory requirements up to exemplary service quality.

CA operational model should be decided during the eID Strategic Positioning phase.

6.4. eID Usage Environments

User environments form a critical part of the technological infrastructure. Currently, the End User Software and API solutions for service providers to authenticate and create/validate electronic signatures are not well-developed. User software of one QTSP is not able to validate QES created by means of other QTSP. Lack of easy-to-get and easy-to-use User Software and API solution components can be considered as serious obstacle for e-services take-off and eID schemes and electronic signature usage in service offering processes.

To promote the eID usage, it is highly recommended that all operations described in chapter Main Use Cases could be performed in desktop environments supporting Microsoft and macOS operating systems, and in web environments using most usable web browsers (Chrome, Edge, IE, Safari). Operations in mobile environments can be considered that mobile devices are able to function as the (qualified) signature creation devices.

6.4.1. Desktop

Desktop environment as the main working environment is the most suitable for personal use to create/validate digital signatures and encrypt/decrypt documents. In case of desktop environments, the processed content does not leave the perimeter fully controlled by the user and therefore any content including the documents with confidential nature can be processed with great certainty that nobody can have access to this information (for example system administrator of the web environment might have access to the content in certain circumstances like violating the rules of the process).

When signing content in the desktop environment, software installed onto the desktop creates a unique hash[42] from the content and the hash is signed and timestamped. Hash can be processed outside the desktop perimeter as it is completely impossible to derive any hints about the content it belongs to.

It is highly recommended to use open source software for desktop applications to avoid vendor lock-in.

6.4.2. Web

Web environment is convenient to use when non-confidential content is processed and several parties have to sign the content within the same timeframe. Also, in cases where the user does not have one's

42 https://en.wikipedia.org/wiki/Hash_function

personal desktop environment, but has a tablet-type computer with mobile operating systems, the web environments can be used.

When using web environment, the content to be processed will be loaded into the web environment and corresponding actions (signing/signature validation, encryption/decryption) can then be performed.

There are many service providers on the market (Dokobit, signNOW, Docusign, etc.) offering such environments. For personal and low-volume usage (couple of signatures per months), the service could be free of charge. For large volumes and data storage, there are volume-based paid packages available. As a starting point, it is important to understand whether the preferred environment supports electronic identity and digital signature means, and also required signature formats. As a rule, the trust service provider who has issued the eID should give a list of proper web signing environments.

6.4.3. Mobile

Mobile environments (smartphones, tablets) can be also used for digital signature creation/validation and content encryption/decryption. However, the screen size limitations should be considered for content processing. Mobile environments are good to use when eID means are related to the mobile device while a smartphone can be used as a smart-card reader for smart-card based eID carriers.

It is also highly recommended to use open source software for mobile applications to avoid vendor lock-in.

6.4.4. APIs for Service Providers

To facilitate eID usage in various service environments, easy-to-integrate and well-documented APIs should be available to all service providers - both public and private. This facilitates integration of eID to their service environments. It concerns primarily authentication, digital signature creation and validation services.

Recommendations

User environments form a critical part of the technological infrastructure. To support innovation and ensure vendor and technology neutrality, open source based user environments are highly recommended. There are several successfully implemented solutions where source codes are available and could be adjusted and customised to North Macedonia's ecosystem.

Implementation of desktop environments for the main use cases and APIs for service providers should have the highest priority, while mobile environment can be introduced in second phase. Web environment for digital signature creation/validation and file encryption/decryption can be selected and customised from the existing ones on the market.

Besides the technology neutrality principle, the user environments should correspond to the following criteria:

- ***easy-to-get and easy-to-use. No special technical skills should be required to install and use the eID software;***
- ***supporting main use cases described in Section 5.2;***
- ***supporting digital signing and encryption/decryption of all file formats;***

- *multiple files regardless of the file type can be signed simultaneously;*
- *no limits for the number of signatories.*

There should be well-documented and ready-to-use components for service providers in order to integrate national eID means to the service environments for authentication and digital signature creation.

Private sector involvement in the active eID usage, in particular the involvement of the financial sector, is crucial for accelerating eID usage. According to the best practices, and as per studies, the financial sector accounts for over 80% of the total eID transaction volumes and shapes the eID usage habits among the end-users. To attract the financial sector, the eID must comply with the legal obligations in the fields of know-your-customer (KYC), Anti-Money Laundering (as per the 4th Anti-Money Laundering Directive, 4AMLD), and strong authentication of parties (as per the Payment Services Directive 2, PSD2), and should be easy and convenient to use for end-users.

Also, public sector trust in the eID plays an important role.

7.

ORGANISATIONAL AND BUSINESS MODEL

7.1. Business Model

Economy-wide accepted North Macedonia eID can be considered one of the main building blocks of a contemporary e-Governance, and by-default element for simplifying the use of e-services to remove the borders/boundaries between the WB economies and EU member states. It should be handled as a significant government supported infrastructure component rather than a profitable stand-alone business project. Gainfulness of such infrastructure should be estimated based on the overall benefit from processes automatisation and increase in effectiveness rather than direct income from electronic identity and digital signature related services.

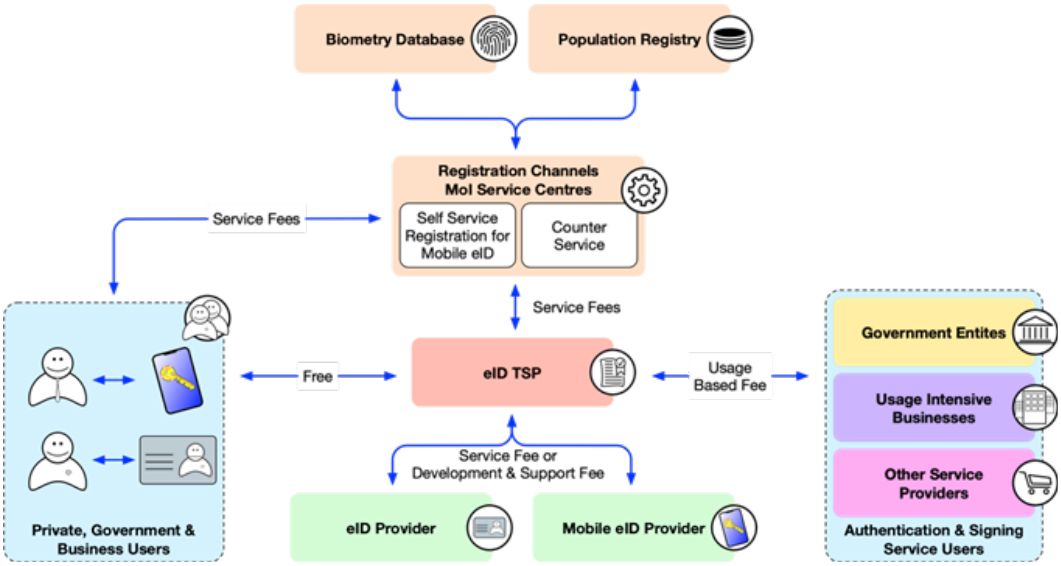

Figure 7. Proposed Business Model

The key requirements/recommendations regarding the business model are as follows:

- eID issuance and management should be government-controlled. Government and economy level issued and guaranteed electronic identity solution has a stronger position to gain overall trust;
- eID should be handled as a crucial e-services infrastructure component (not as a stand-alone profitable business project);
- eID should be available to all citizens and residents;
- eID should be strongly tied to physical identity – be an integral part of the identity management on economy level;
- eID and its usage should be free of charge for users;
- Service providers, both public and private, should contribute by paying for validation services based on transaction volumes. Service providers gain from e-services effectiveness and they could cover eID (both mobile and ID card based eID) infrastructure and service related costs;
- Fast roll-out is critical to speed up North Macedonia e-transformation and private sector entities, specially the financial sector onboarding. For fast roll out the service-based business model could be used where mobile-based eID solution is brought in as a service under government control. But

business model may change over time, and service infrastructure components and corresponding competences could be transferred under government created or controlled Trusted Service Provider organisation.

Proposed business model is illustrated in Figure 7:

- It is assumed that both mobile-based eID and ID card based eID will be implemented to cover all user segments and have secure fall-back/alternative solution;
- Both mobile-based eID and ID card based eID usage should be free of charge for users;
- eID registration services should also be free of charge for users; however if registration service provider set registration (support) fee, this could be covered by North Macedonia government or eID TSP;
- To ensure eID recognition by the North Macedonia government with assurance level 'high' it is recommended to use MOI as Registration Authority;
- Service providers could pay for validation services based on authentication and digital signature transaction volumes;
- North Macedonia eID TSP should be handled as an infrastructure component to support the e-transformation. It can take at least 5 to 7 years for TSP to reach operational profitability;
- Development and support fees could be paid to mobile-based eID and ID card based eID solution technology providers in accordance with the agreed business models;
- Depending on the technical solution there could be other technical component providers currently not indicated in Figure 7.

7.2. Organisational Model

Successful implementation of the eID solution is a prerequisite for creating a trusted electronic identity and easy-to-use electronic identity related service environments. Organisational model and service offering processes are playing an important role in building broadly trusted infrastructure services.

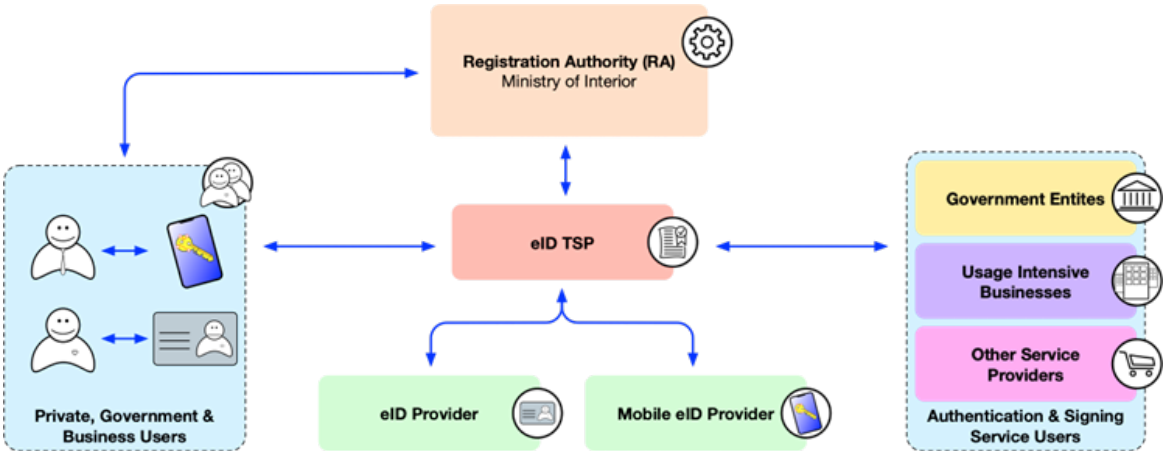

Figure 8. Organisation Model

As government entities have high reputation in North Macedonia's society it is wise to set up the Trusted Service Provider organisation as government organisation. It will significantly help stimulate the use of mobile-based eID and/or ID card based eID internally by all government entities and also create trust and acceptance by service providers (to use government guaranteed electronic identity solutions).

The proposed organisational model is following the business model and is presented in Figure 8.

7.2.1. TSP Ownership

The trust services can be provided by a public or private entity or also in combination of both. There are some risks in both cases to be considered. The following matrix could provide an overview of the potential scenarios for both models. The main issue lies with trust. In order to truly digitalise, the trust is the first issue to be dealt with. The end users and relying parties must be able to have the confidence in electronic transactions both public or private. It is important to keep in mind that the experience is driven by the private sector, especially the commercial banks.

Based on the Estonian example, the average person communicates with the state about two times a year on average while checking if salary has been deposited several times in an hour.

Risk	Description	Remedy	Public TSP	Private TSP
Trust issues	The general public or the relying parties are not able to trust the trust service provider due to organisational, political or historical reasons.	Economy level supervisory body overviewing the trust services provision within the economy territory; TSP is to be audited by a private independent auditor; audit reports must be published in full extent; public policies and procedures including practice statements; liability insurances for both organisational and technical misusage of the tokens and key materials; clear and open communication with the public.	The trust lies with the government as a whole and therefore the services provided fall under the same concept of trust. Supervisory body as part of the government does not improve the trust level for the public.	A dedicated entity has all means to establish its own reputation and trustability. The trust defines its financial outlook and therefore the sustainability of the business as such.
Stagnation	The TSP is able to fulfil the minimum requirements but does not develop additional services. For example, the APIs run out of date using ancient technology which in return could create serious issues for relying party integrations.	Long-term vision including strategic goals to provide best possible service to the end users and relying parties. The supervisory body has to have the mandate to force TSP to improve the quality of services provided.	Bare minimum is sufficient to sustain the service.	The private entity has a business interest to gain additional usage using new service channels and solutions.

Risk	Description	Remedy	Public TSP	Private TSP
Reliability	The quality of service is directly connected to the quality of the whole chain of trust starting from registration authority taking care of the whole lifecycle of an eID.	Reliability and availability of the service provided are crucial elements for both end users and relying parties. The ultimate goal is to provide a secure authentication and digital signature creation tool that is always available and reliable. The aim is to make the government provided eID an industry standard for both authentication and digital signature. It could be achieved only if the trust services provided are always available and reliable enough. There should be a strong motivation mechanism in place to avoid any issues related to reliability and/or availability.	The operator does the best it can given its capabilities. In case of the public sector entity it is rather difficult to find the methods to enforce underperformance in those areas.	Private entity has the risk of reputational damage which has a financial impact on the services provided. Based on the risk, the entity is well motivated to maintain the highest level of reliability and availability. The integration with the relying parties should be under strict SLAs which must include the requirements for the service availability and financial penalties.
Availability	As the relying parties start to integrate with the trust service, it becomes a critical part of the infrastructure. The downtime of the validity or time stamping service means that they are unable to serve their customers. If the solution provided by the government is not reliable enough, they will not adopt it in their systems and therefore the electronic usage of the national eID will not increase.			
Business model	Creation of a money machine out of the trust services that eventually kills the usage and may render national eID's electronic functionality useless as the users and relying parties will not abandon the existing solutions and start searching for cheaper alternatives.	The provision of trust services can be a lucrative business for a private sector entity. At the same time, in order to support the usage of electronic services and digitalisation in general, the price tags should be kept on a reasonable level just to sustain the service provision. It is reasonable and expected that the provision of trust services is free of charge for the end users and the reliable party takes care of the transaction fees based on the business model proposed.	A public sector provided TSP has no business interest and follows the duties and limits provided by regulations.	Private entity shall be dependent on the issuance and transaction fees. The latter makes the operator financially interested to promote the usage of eID based electronic services.

Either way, the recommendation is to create a dedicated entity for trust service provision. This makes it easier to handle and manage trusted services if the TSP is a dedicated unit.

There are several options how to position the main roles organisationally:

- North Macedonia eID Trusted Service Provider (TSP):
  - In principle, as stated earlier in the study, the TSP could be the government entity, private entity, or an entity set up on a PPP-model. It is crucial that the entity has motivation and necessary resources to build proper organisational routines, technical infrastructure and service portfolio described above. Simply put, the qualified trust service provider should be trusted in all means, starting from fulfilling all regulatory requirements up to exemplary service quality. Certificate issuance and lifecycle management for government issued and granted eID means should be under strict control of the corresponding government institution.
  - To consider existing situation we recommend the to set up the government controlled TSP because:
    - Government structure is better positioned for infrastructure components;
    - Certificates (aka electronic documents) issued by the government entity are easier to make mandatory for all government entities to accept;
    - It is wise to have the same TSP for mobile-based eID and ID card based eID to gain cost and resource efficiency.
- Registration Authority (RA):
  - Based on the proposed eID positioning described in Sections 5 and 6 we recommend the Ministry of Interior (MOI) or its structure currently issuing national ID cards to operate as RA, because:
    - Both mobile eID and ID card based eID is recommended to have government recognised assurance level 'high';
    - MOI is responsible for national identity management. eID related authentication and digital signature certificates as electronic documents are recommended to tie the identity management on economy level;
    - eID means (tokens) as electronic documents carriers issued by the government entity are easier to make mandatory for all government entities to accept;
    - Cost and resource efficiency as some of the resources and procedures implemented for national ID card issuance can be also used for eID issuance;
    - Self-service workplaces require access to biometry database and most probably can be set up only in MOI (or its substructure) perimeter.

7.2.2. Qualified Certificates

Qualified certificate is defined only in the context of electronic signatures (not applicable in authentication certificates). The requirements are defined in Annex I of eIDAS Regulation. The requirements for qualified

electronic signature creation devices (QSCD) are defined in Annex II. The detailed technical requirements are defined by ETSI EN 319 412 part 1[43] and 2[44].

According to eIDAS, to be considered a qualified digital certificate, the certificate must meet the requirements provided in Annex I of eIDAS Regulation, including, but not limited to:

- Identification that the certificate is a qualified certificate for electronic signature;
- Identification of the qualified trust service provider whcih issued the qualified certificate, including such information;
- Corresponding electronic signature validation data and electronic signature creation data;
- Indication of the certificate's period of validity;
- Unique certificate identity code of the trust service provider;
- Qualified trust service provider's advanced electronic signature or electronic seal.

The compatibility with the eIDAS regulation can be achieved through relevant ETSI standards.

7.2.3. Root Certificate Ownership

Contemporary trust model is based on trust lists so trust is inherited from a signed trust list and not from a root certificate. The usage of root certificate is a technical legacy and is being used mostly for web server certificate validation.

The mechanism for distributing authorised trust list signers in EU is LOTL. As a non-EU economy, the local regulation must be developed to define how the trust lists are populated and signed. Normally on an economy level, the signer and the distributor of the trust list is the supervisory body.

The national trust list for trust services has an important role in establishing the first link in the chain of trust for the national electronic identity documents. The economy level supervisory body is the one signing all the underlying trust service instances within the scheme.

By the original concept, the root certification authority is used only to certify the intermediate instances. In case of an intermediate compromise, it could be also used for issuing an updated certificate revocation list. Otherwise the root CA should be an offline instance only to be used for certifying the intermediate authorities.

Considering the contemporary approach, the CA certificate issuing national ID certificates could be also self-signed if it is going to be included in the national trust list. Therefore there is no need to create a root certification authority.

The root certification authority must exist for technical reasons. It should remain under the control of TSP and used to sign intermediate certification authorities; however if the trust list is being the selected approach, there is no need to create a national root certification authority.

Our recommendation is to follow the contemporary practice and start using trust lists instead of establishing national root certification authorities.

43 ETSI EN 319 412-1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

44 ETSI EN 319 412-2 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

7.2.4. With or Without a Chip

Throughout the Western Balkans region, there are several examples of ISO/IEC 7810[45] compatible national ID card implementation. Some of them follow the German model provided by German plastic manufacturers but there is no good example to follow in terms of electronic usage of the functionality of the card.

Simplicity is the key. The electronic functionality of an ISO/IEC 7816[46] compatible eID should be limited to two distinct functions - authentication and digital signature creation. Due to the nature of X.509 certificates used, it will have the functionality of data encryption/decryption using the authentication certificate. Having more than two pairs of keys and more than two X.509 certificates on eID does not help the user experience.

Both of the functions should have a separate PIN codes in order to distinguish the operations for the end user. PIN 1 for authentication (and data decryption) and PIN 2 for digital signature creation.

As the digital signature is equal to the handwritten signature and has a legal value, it must be clearly communicated so that the user is fully aware of the possible consequences of the operation. This is also a security feature in order to protect the user from possible phishing sites which instead of authentication could lure the user to sign something digitally without showing the user its true intentions.

While the ISO/IEC 14443[47] compatible contactless interface is more durable and fancier it also renders the price tag of the card reader out of reach for a normal user while the contact chip readers are cheap enough to be subsidised by the relying parties such as commercial banks which will benefit the most from having a government provided authentication tool.

Even though the eID chip on the card is technically able to host a large number of applets with different functionalities, it should be kept as simple as possible. The eID should serve as a key to services instead of building the services on the card.

The basic functions should be authentication and digital signature creation. Only the information printed on the card, should be stored on the personal data file of the chip. In order to support mobile devices it is recommended to use a hybrid solution providing similar functionality over contact and also contactless interface with the exception of security operations such as PIN code change and unblocking which should not be available over contactless interface.

As an optional component, if the eID is also to be used as a travel document, it could contain a separate MRTD chip for Supplemental Access Control (SAC) following the example of biometric passports already being used in most of the world. The recommendation is to implement a solution compatible with ICAO Doc 9303[48].

Using a QR or barcode on the card does not provide any electronic functions to the end user and therefore does not support digitalisation on the economy level if there are no features to provide users with strong authentication and digital signature creation mechanisms.

45 ISO/IEC 7810 - Identification cards - Physical characteristics

46 ISO/IEC 7816 - Identification cards - Integrated circuit cards

47 ISO/IEC 14443 - Identification cards - Contactless integrated circuit cards

48 ICAO Doc 9303, Machine Readable Travel Documents, Part 1: Machine Readable Passports, Volume 2: Specifications for Electronically Enabled Passports with Biometric Identification Capability

8.

APPLICABLE SOLUTION OPTIONS

Implementation of well-functioning eIDAS compliant and economy level accepted eID ecosystem is a complex task and should not be handled as technology project. It is highly recommended to handle the national eID ecosystem as one of the key infrastructure components for e-transformation and the focus should be placed on strategic positioning, policy, organisational and business model development. If this approach is followed there should be no big issues with organisational and technical implementation.

To create economy level accepted and cross-border/boundary interoperable eID ecosystem the following areas should be in focus:

- Strategic Positioning and Key Requirements of the national eID to cover the main principles the eIDAS compliant eID system should meet;
- Legal and Policy Framework Adjustments to handle questions to be solved in relation to implementing the eID Strategic Positioning;
- Business and Organisational Model to cover topics related to the eID and trust services organisational activities to set up well-functioning organisation and customer support activities;
- Key Components of National eID System to handle questions related to eID carrier or carriers, eID issuance, setting up Certification Authority as a Qualified Trust Service Provider, and eID Usage Environments.

Main recommendations for all those areas based on global best practices and considering the existing situation in North Macedonia are shortly described in Sections 5-7. In addition, Section 9“Implementation Timeline gives a structured and concentrated view on all the above mentioned areas.

As one of our main recommendation on eID Strategic Positioning is that it should be handled as an integral part of the identity management on economy level, the current section addresses various applicable options for eID carriers and correspondingly eID issuance. All other recommendations for other eID ecosystem areas listed above are applicable to all eID carriers in the same manner.

8.1. National ID card based eID

As described above in Section 6, eID schemes attached to the physical identity document, especially to the National ID card, can be considered most commonly known eID means. One of the advantages of ID card-based eID is that ID card as economy level identity document is well-perceived to be handled with care and usage principles are set by legislation. This approach expands also to the eID, and people are handling ID card-based eID means more carefully compared to memory stick, SIM-card or cloud based eID means. The negative side is that traditionally people do not use their ID card on daily basis and thus efforts may be required to change the habits and practices to foster the usage of eID. However, if PIN codes are handled with care and security systems are well developed it should not create major problems.

The identity card of North Macedonia is a compulsory identity document from age 16 and is issued by the Ministry of Interior. Currently, it has no eID scheme or digital signature related capabilities but there is an ongoing initiative to add those functionalities to the new version of the national ID card.

Using national ID card for eID carrier is a secure and well-proven approach. It is well positioned to carry foundational electronic documents (certificates for electronic authentication and digital signature creation) issued as integral part of identity management on economy level. Also, as an identity document, ID

card is well-perceived to be handled with care and is well-suited to carry private keys and ensure those are under the sole control of the user.

ID card-based eID means require additional physical hardware deployment (which will increase logistics concerns and costs). Thus, establishing ID card readers infrastructure is identified as one of the challenges to achieve eID massive usage. However, if ID cards have contact-chip, the readers are affordable (2-3 euros per item) for most population and can be even distributed free of charge along with the ID card. Also, they are small to carry and easy to use via standard USB interface.

To avoid card-readers related (mass) usage blockers and to maximise National ID card based eID carrier benefits the following additional recommendations are provided to those described above:

- Design and issue the national ID card as travel document according to the ICAO standards Doc 9303. Adding biometric information on the ID card significantly expands the ID card usage potential and convenience to the holder, such as the possibility of use in automated boarder control or check in to air flights, just to mention some examples. From eID scheme perspective it creates possibility for highly secure online onboarding and renewal of secondary eIDs such as mobile-based eIDs which are most convenient for everyday mass usage and attractive to private sector to integrate into their service offering processes;
- On ID card electronic side, avoid using RFID technology only as it leads to significant investments into readers infrastructure and inconvenience for daily use-cases;
- Use hybrid chip technology instead of combining contact-chip and RFID technologies. Clear rulesets can define what technologies can be used with what applications/use-cases. As explained earlier, contact-chip technology will facilitate the use of ID card based eID for secure authentication and digital signature creation as readers are cheap and easy-to-use compared to the RFID card readers.

8.1.1. National ID card based eID components

The following Figure 9 describes the components of a smart card based eID ecosystem. This illustration covers the whole system including the TSP on a very high level. In this case, the smart card contains the private keys which are under the sole control of the end user.

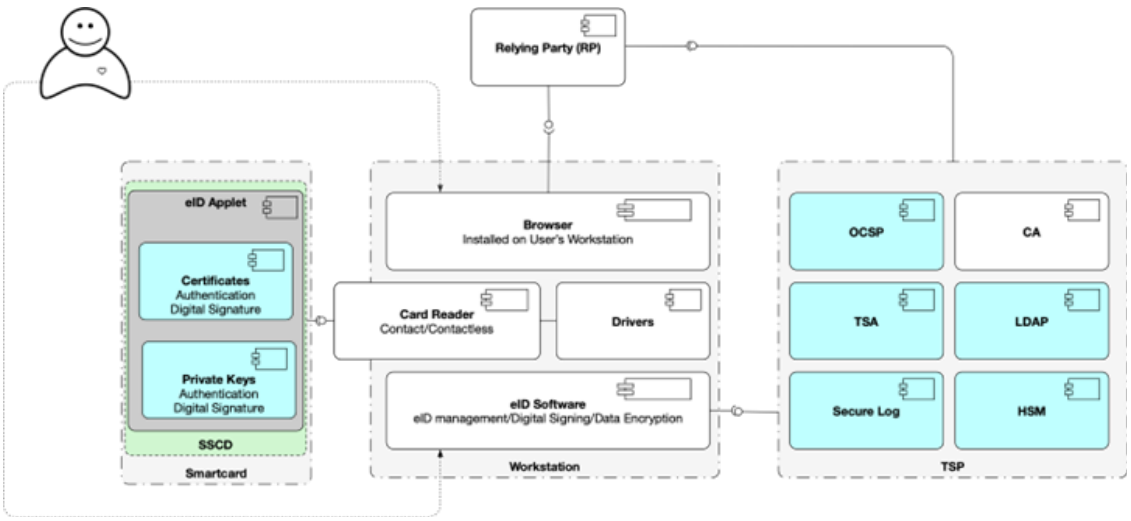

Figure 9. National ID card based eID components

8.1.2. National ID card based eID issuance

National ID card based eID issuance can be done by using almost the same procedures currently used for issuing the existing ID cards and biometric passports. Electronic components for authentication and digital signature creation (key-pairs and corresponding certificates) are prepared during the ID card personalisation process, and the ID card is ready for usage when issued together with the PIN codes envelope.

Section 8.4 below gives a comparative overview of the National ID card based on eID and other applicable solutions according to the most relevant criteria for implementation and use.

8.2. SIM card based Mobile eID

As described in Section 6 above, mobile environments are becoming the highest priority to ensure 24/7 availability in various service offering areas both in public and private sector. Mobile/smart phone is the last thing people forget to take with them and is the first one they notice missing. In that regard, it is a natural development that the electronic identity and digital signature means should be easily and securely usable with mobile device.

SIM-card based Mobile-ID solutions were first on the market more than a decade ago, as SIM-cards offered equivalent technical security components compared to the chip-based ID cards or tokens. Currently, all mobile phones are able to house a SIM card and that means all mobile phones, including the simplest and cheapest ones, can be used as a secure eID carrier for electronic authentication and digital signature creation.

Given that various mobile devices with the e-SIM functionality are starting to take off, SIM-card based solutions should be considered rather old-fashioned ones, and thus implementing these in the national eID ecosystems may likely have negative impact on early adopters market segment.

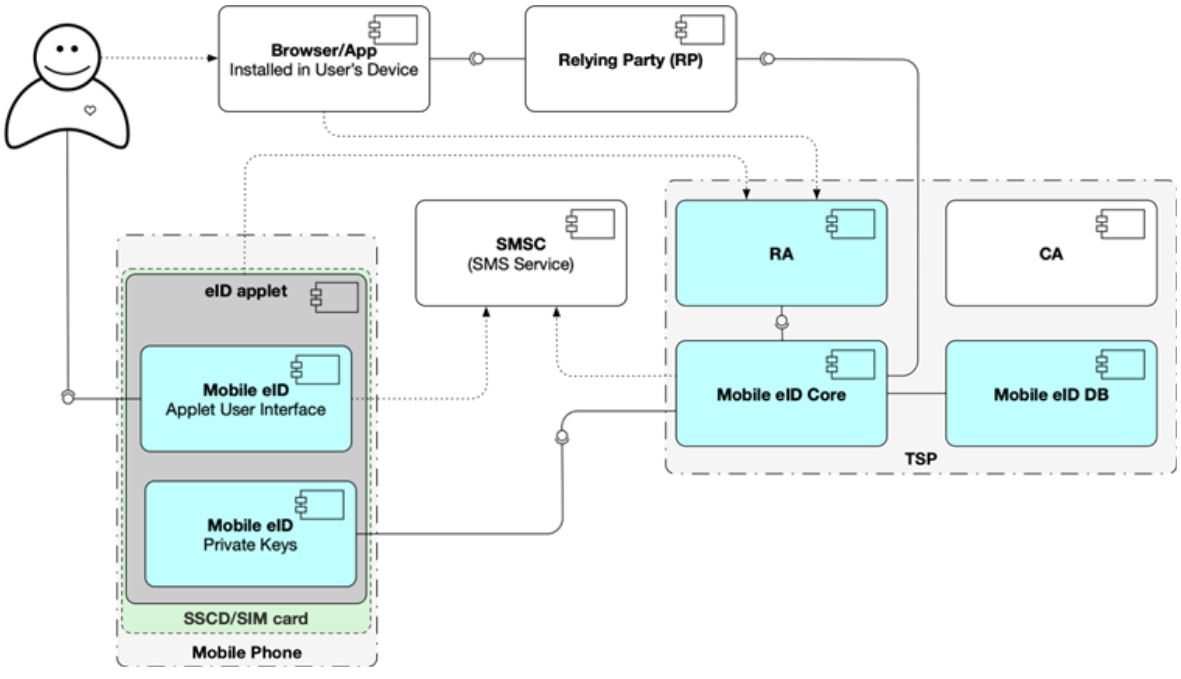

Figure 10. SIM card based eID components

8.2.1. SIM card based Mobile eID issuance

SIM card based Mobile eID issuance requires replacement of the existing SIM cards with the ones with PKI capability. This means all domestic mobile operators should be involved in both technical implementation and eID issuance procedures. Technical implementation from the mobile operators side covers establishment and management of communication channels between mobile phone (as eID carrier) and Certification Authority (CA). In eID issuance procedures mobile operators are responsible for ordering, distribution and activation of SIM cards with agreed set of cryptographic key-pairs (usually for authentication and digital signature creation). At this point SIM card is active in mobile operator's network, but cryptographic key-pairs still need to be activated and corresponding certificates (electronic documents) should be issued and tied to the person's identity management on economy level.

To issue SIM card based Mobile eID with high assurance level, a person's identity must be verified with high accuracy before the eID activation. It can be done over the counter in all MOI service centres following the procedures that are similar to the process of issuing national ID cards and/or passports.

Establishing self-service workplaces in all or selected MOI service centres could be considered as another option. Persons' identities can be verified by using their ID card details and fingerprint biometrics stored in MOI database. This kind of self-service workplace does not require significant investments, since these would consist of a standard PC, basic ID card MRZ and fingerprint reader. The software part does not require notable developments and 1:1 fingerprint biometrics verification is not complex either. Thus, fingerprints could be used to validate an identity enrolling to eID.

Recommended options are secure and cost-effective, and can be applied not only for initial mobile-based eID credential activation, but also later for credential renewal, if necessary.

Section 8.4 below provides a comparative overview of SIM card based on Mobile eID and other applicable solutions according to the most relevant criteria for implementation and use.

8.3. Mobile application based Mobile eID

During the past couple of years several mobile application based solutions have been introduced, and some of them such as Belgian *itsme®* (described in more details in Section 4.3 above) and Portuguese Digital Mobile Key have even passed eID scheme notification process under eIDAS regulation. Those eID schemes use technical specifications for cloud-based digital signatures (ETSI TS 119 431-1, ETSI TS 119 431-2, ETSI TS 119 432, EN 419241-1:2018 and EN 419241-2:2019) and general principle is that private keys are stored at qualified trust service provider environments. According to the specifications, the provider of the remote digital signature service has to apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, but still it can be argued that it is not technically excluded the private keys can be used without the consent of the owner. Also, despite the usage of secure communication channels, in case of server signing solutions, the content leaves user-controlled perimeter and can affect the use of the solution in case of sensitive materials.

The mobile application based Mobile eID solution is described below where it is technically excluded that a corrupt system administrator of the trusted service provider has access to the user's private keys. The core functionality of proposed solution comes from Smart-ID - the new generation electronic ID solution developed in Estonia. It takes advantage of the capabilities of today's smart devices to offer a high level of

security to end-users. No special SIM card nor a card reader is necessary to be used by a proposed smart phone based eID (Mobile eID), the only thing required is a smartphone with an active internet connection.

Smart ID solution has been successfully launched in Estonia, Latvia and Lithuania in 2017 and currently it has accounts for over 3.1 million users with more than 3 million daily transactions.

The solution handles the protection of user's private key by using the results from the threshold crypto-system.[49] Threshold cryptography studies such systems, where, in order to decrypt an encrypted message (or to sign a message), several parties must cooperate in the decryption protocol (or signature computation protocol). Threshold cryptography provides the benefit in that the compromise of a single party (or revealing the share of a single party) does not result in the compromise of the whole system. Historically, this technique is used in the highly critical systems, where the two-man rule[50] must be enforced. For example, the key for decryption may be shared between independent members of the management team and executing some critical function requires that all key holders are present.

Advances in the threshold cryptography and increase of the computing power inside the mobile devices allows us to use similar techniques for securing the private key, which is used in public key encryption algorithms. In the proposed application based Mobile eID solution, the separate and independent parties which hold the shares of the private keys are the following:

- User's mobile device;
- Mobile eID backend systems (qualified trust service provider).

With the Mobile eID solution, the private key of the user is never generated or combined in a single place or location. Instead, the distributed generation protocol is used and the shares of the private key in the user's mobile device and in the Mobile eID service side (backend) are generated. The shares of the private key are generated, processed, stored and protected in the separate physical locations and never combined into single private key. This approach makes the solution more resilient for various cyber attack vectors.

8.3.1. Application based Mobile eID components

Main components of the proposed mobile application based Mobile eID are presented in Figure 11.

The components described in the illustration have the following functions:

- Mobile eID App Lib – The component handles all the cryptography, account management and server communication related tasks inside the SIM-less Mobile eID app;
- Mobile eID App UI - This handles the UI and user interactions;
- Mobile eID App - The Android/IOS application, which the user installs on his/her mobile device in order to register for the Mobile eID account and to authenticate himself/herself to the relying party (RP) services and to give digital signature;
- GCM/APN - The push notification platform, such as Firebase Cloud Messaging (FCM) and Apple Push Notification, relays the notifications from Mobile eID Core to the Mobile eID App instances;

49 https://en.wikipedia.org/wiki/Threshold_cryptosystem

50 https://en.wikipedia.org/wiki/Two-man_rule

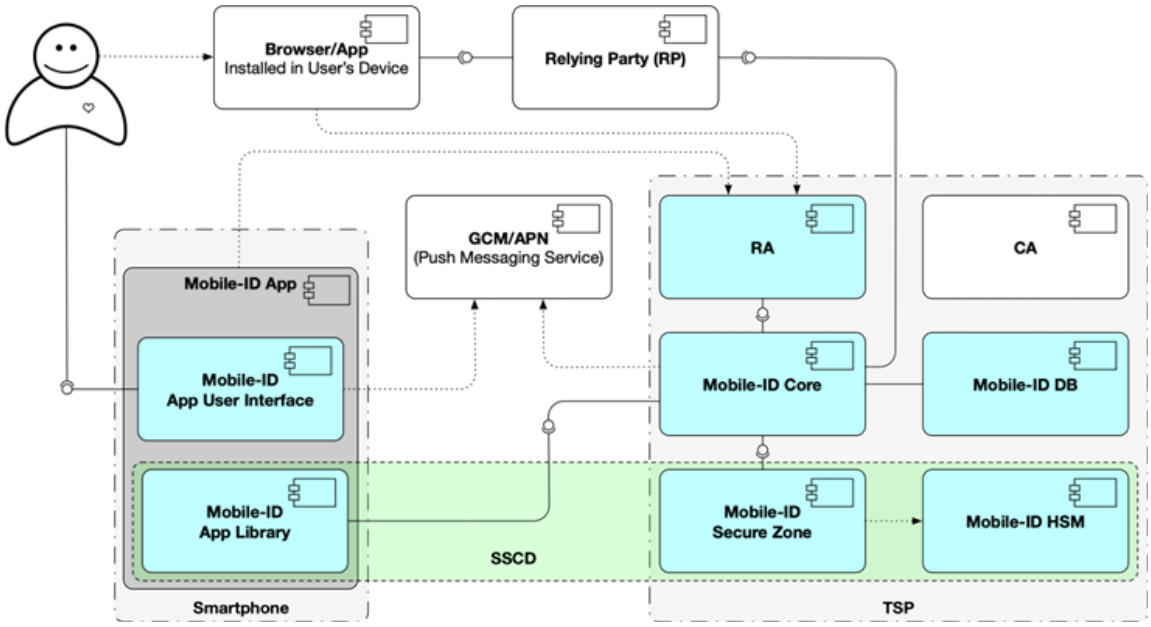

Figure 11. Application based Mobile eID solution components

- Mobile eID Core - This component implements the business logic, manages the database and provides APIs to the mobile devices, RPs and Registration Authority (RA). It also mediates the messages between the Mobile eID App Lib and Mobile eID SecureZone components.
- Mobile eID SecureZone - This is the component which is handling the cryptography tasks and key pair generation on the server side. The SecureZone also requests the cryptographic operations from Mobile eID HSM.
- RA - Registration Authority. This is the component which implements the registration processes and performs the Registration Authority duties. There are multiple RAs to correspond to different registration process variants, for example, on-site registration with human employees, identity proofing, and self-service registration desk/portals which use third-party authentication services.
- CA - Certification Authority, which is issuing X.509 certificates for authentication and signature key pairs.
- SSCD - Secure Signature Creation Device is the logical component, consisting of the Mobile eID App Lib and Mobile eID SecureZone and Mobile eID HSM components.

Mobile eID application is the eID carrier and easy-to-use transaction device for the user. The application has the following functionalities:

- Registration, supports registration in RA (MOI) offices and at self-service desks;
- Transaction notifications;
- PIN entry for authentication and digital signing;
- Account info;
- Revocation of Mobile eID account.

Mobile eID application will be available for Android and iOS platforms. Users can download Mobile eID application from Play Store and Apple Store accordingly and, as suggested in our business model proposal, it should be free of charge.

8.3.2. Mobile application based Mobile eID issuance

Mobile application based Mobile eID registration process starts with downloading the Mobile eID Application. After opening the application, the user will be notified about the registration options. As an example, there could be the following registration options:

- Registering in RA (MOI) office with the help of RA officer;
- Registering in self-service desk (at MOI office as proposed);
- Registering online using valid biometric passport.

For the registration in RA office or in self-service desk the user has to bring the device on which the Mobile eID application has been installed, as the registration process, secure key generation and certificate issuance expect collaboration with the installed app. After completing the registration, a new electronic identity (with authentication and digital signature certificates) will be issued and linked with the user.

As another option, establishing self-service workplaces in all or selected MOI service centres could be considered. Persons' identities can be verified by using their ID card details and fingerprint biometrics stored in MOI database. This kind of self-service workplace does not require significant investments, since these would consist of a standard PC, basic ID card MRZ and fingerprint reader. The software part does not require notable developments and 1:1 fingerprint biometrics verification is not complex either. Thus, fingerprints could be used to validate an identity enrolling to eID.

Also, there is a well-proven solution to use the biometric passports during the mobile-based eID enrolment procedure. Facial biometrics stored in the biometric passport RFID chip is compared with online selfie photo, and validity of the passport issuer certificate is checked. When adding passport and personal numbers online verification then all high assurance level issuance requirements are met.

Section 8.4 below gives a comparative overview of the mobile application based on Mobile eID and other applicable solutions according to the most relevant criteria for implementation and use.

8.4. Comparison of Applicable eID carriers

The following table gives a short comparison of the above described applicable eID carriers according to the most relevant criteria for implementation and use.

Criteria		eID carrier			Comments
		ID card	SIM card	Mobile App	
1	Secure, recognised as QSCD under eIDAS framework	+	+	+	All described eID carriers can be implemented as QSCD under eIDAS regulation

Criteria		eID carrier			Comments
		ID card	SIM card	Mobile App	
2	Private keys are under sole control of the user	+	+	+	If private keys are stored in cloud environment the qualified trust service provider internal attack vector towards the private keys is not fully mitigated by technical means
3	Maximum penetration among North Macedonia residents	+	+/-	+/-	National ID card as mandatory identity document has the potential to ensure best penetration for eID due to the regulation. Mobile eID solution penetration is driven by usage capabilities (availability of useful services and easy-to-use)
4	Easy-to-get	+/-	-	+	Involvement of mobile operators makes the SIM card based solution less convenient to activate as part of the identity management on economy level
5	Easy-to-use in various environments	-	+	+	Mobile eID solutions do not need card readers and are better positioned to use in mobile service environments
6	Supporting mobile initiatives	-	+	+	ID card based eID is complex for adoption in mobile service environments
7	Attractive for private sector, especially for banks	+/-	+	+	Mobile-based eID issued on economy level is attractive for private sector, especially banks, to implement.

8.5. Conclusions

Considering the currently perceived need to replace the existing national ID card with a new version with electronic capabilities, accelerating growth in e-services development and increasing the need for secure eID means for electronic transactions, we recommend North Macedonia to consider implementation of both National ID card based and mobile application based Mobile eID.

As described above, Strategic Positioning, Legal and Policy Adjustments, Organisational and Business Models and majority of Key Components are exactly the same for both eID carrier solutions. National ID card with eID functionality will establish default economy-wide eID coverage and will allow secure online onboarding of mobile application based Mobile eID. Based on best practices the Mobile eID will be very attractive for the private sector, especially for the banking sector and will drive the usage experience.

National ID card based eID can be an alternative to the Mobile eID for those who do not want to use smartphones, or just prefer using National ID card based eID solution. Also, as importance of electronic transactions in our everyday lives is growing exponentially, it is always good to have alternative solution as a fallback.

To avoid card-readers related (mass) usage blockers and to maximise National ID card based eID carrier benefits the National ID card should be designed and issued as travel document according to the ICAO standards Doc 9303. Adding biometric information on the ID card significantly expands the ID card usage potential and convenience to the holder, such as the possibility of use in automated boarder control or check in to air flights, just to mention some examples. From eID scheme perspective it creates capability for highly secure online onboarding and renewal of secondary eIDs like mobile-based eIDs which are the most convenient for everyday mass usage and attractive to private sector to integrate into their service offering processes.

On ID card electronic side, avoid using RFID technology only as it leads to significant investments into readers infrastructure and inconvenience for daily use-cases.

Use hybrid chip technology instead of combining contact-chip and RFID technologies. Clear rulesets can define what technologies can be used with what applications/use-cases. As explained earlier, contact-chip technology will facilitate the use of ID card based eID for secure authentication and digital signature creation as readers are cheap and easy-to-use compared to the RFID card readers.

It is highly recommended to implement both solutions in parallel or at least under the same project framework to avoid duplication and interoperability issues. Also, we recommend to add national ID card visual presentation and its validity online check functionalities into the application based Mobile eID. National ID card visual presentation in Mobile eID application without online validation capability is not recommended because it can be attractive for fraudsters.

Taking into account the speed of mobile communication technology development and usage trends we do not recommend introducing SIM card based Mobile eID as part of national eID ecosystem.

9.

IMPLEMENTATION TIMELINE

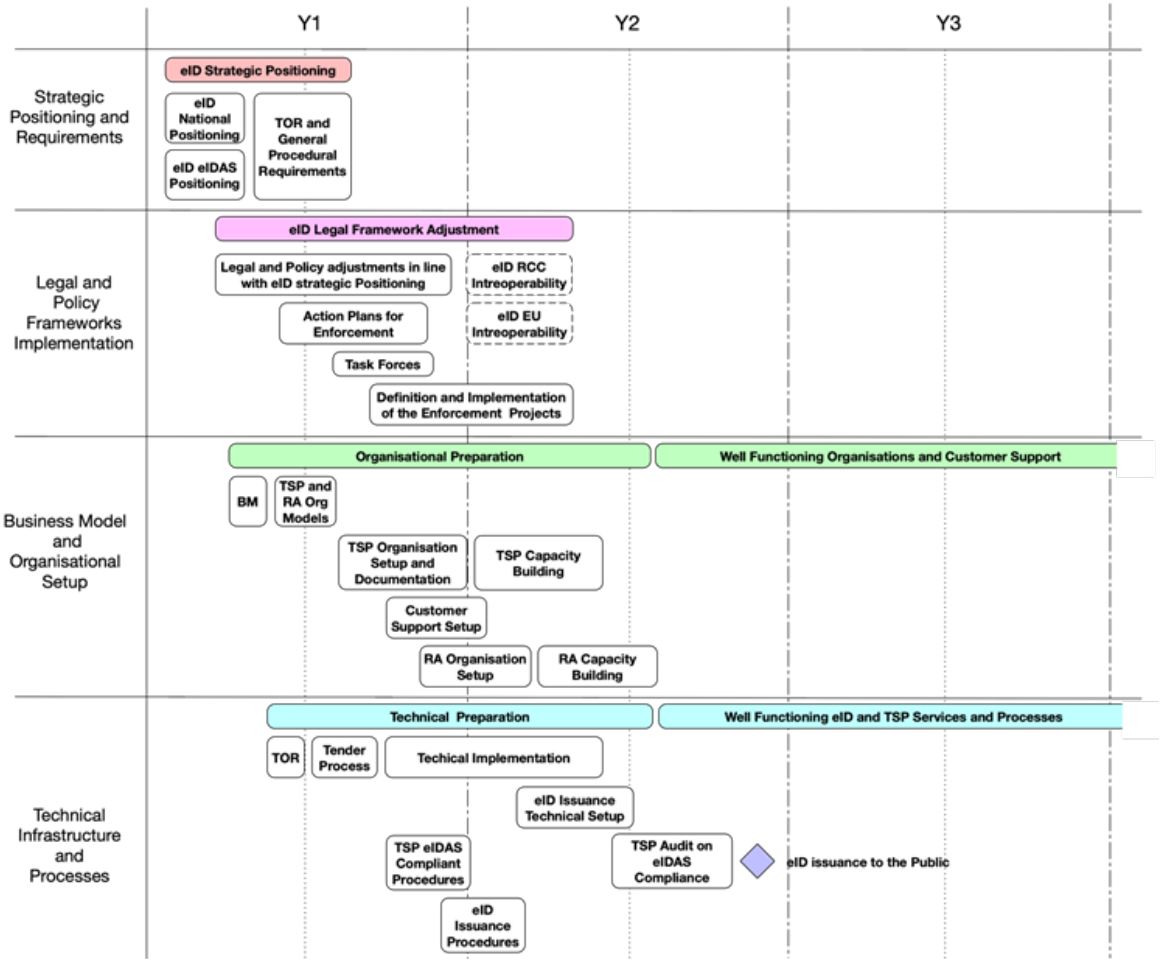

Figure 12. Estimated implementation timeline

Estimated implementation timeline is based on the project structure illustrated in Figure 12.

Activities on the implementation timeline are divided into four sections:

- Strategic Positioning and Requirements section covers the main principles the eIDAS compliant eID system should correspond to;
- Legal and Policy Frameworks Adjustments section handles questions to be solved in relation to implementing the eID Strategic Positioning;
- Business Model and Organisational Setup section covers topics related to the eID and trust services organisational activities to set up well-functioning organisation and customer support activities;
- Technical Infrastructure and Processes section handles the main activities related to technical and procedural preparation to insure well-functioning eID issuance and TSP services.

9.1. Strategic Positioning and Requirements

9.1.1. eID National Positioning

eID National Positioning covers the main principles the new eID solution and entire eID ecosystem should correspond to and how it is positioned on economy and international scale. Based on the best practices and current situation analysis (see also recommendations in Section 5 above) we recommend the following:

- Authentication and digital signature certificates should be an integral part of the identity management on economy level;
- eID should be issued on economy level;
- Digital signature created with eID means is equal to the handwritten signature;
- eID (electronic authentication and digital signature) should be mandatory to accept for all government institutions;
- eID should have economy-level and cross-border/boundary acceptance.

Other recommendations are described in detail in Sections 5 and 6.

Based on the recommendations, other information sources and political ambitions, the main eID National Positioning principles should be defined, coordinated and accepted at the highest possible level during the eID National Positioning activity.

The current activity should be handled in line with eID eIDAS positioning activity.

eID National and eIDAS positioning principles form a playground for the entire eID ecosystem.

9.1.2. eID eIDAS Positioning

eIDAS regulation is handling electronic authentication and trust services (including electronic/digital signature) related activities inside the EU, but eIDAS framework can be implemented also outside the EU. Based on the best practices and current situations analysis we recommend the following:

- To choose eID scheme witch will be recognised by the North Macedonia Government as eID with high level of assurance;
- To choose digital signature solution corresponding to eIDAS Qualified Electronic Signature requirements;
- To create Trust Service Provider corresponding to eIDAS Qualified Trust Service Provider requirements.

Other recommendations are described in detail in Sections 5 and 6.

Based on the recommendations, other information sources and political ambitions, the main eID National Positioning principles should be defined, coordinated and accepted at the highest possible level during the eID National Positioning activity.

The current activity should be handled in line with eID national positioning activity.

eID national and eIDAS positioning principles form a playground for the entire eID ecosystem.

9.1.3. General TOR and Procedural Requirements

Based on the accepted eID national and eIDAS sositioning principles and our recommendation for the Key Components of the National eID System, described in Section 6, General TOR and Procedural Requirements should be specified.

General TOR and Procedural Requirements form a basis for organisational and technological preparation. It is recommended to coordinate those requirements with key stakeholders of the eID implementation.

9.2. Legal and Policy Frameworks Adjustments

Legal and policy frameworks form a basis for acceptance and trust of the eID system. It should be noted that eID implementation is an important building block of the e-Transformation (or e-Governance) and for successful eID implementation it should be handled in line with e-Transformation initiatives. Current implementation timeline does not cover implementation principles and recommendations outside the eID implementation scope.

North Macedonia has fully eIDAS compliant economy level regulation and all relevant EU standards related to eID and Trust Services are transposed. Legal and Policy Frameworks might need eID Strategic Positioning related adjustments.

9.2.1. Legal and Policy Adjustments

eID Strategic Positioning principles might need adjustments of the current legal and policy documents regulating electronic records, electronic transactions, identity documents, data protection, data exchange between government entities, etc. Based on the approved eID Strategic Principles, legal and policy framework assessment should be done to identify the required adjustments. Following, adjustments should be drafted, coordinated and passed to be ready for enforcement.

It is recommended that adjustments should be prepared, coordinated and passed before or in line with the TSP and RA Organisation Setup activities to avoid legislative misinterpretations. As TSP is subject to eIDAS compliance audit, all procedures and corresponding organisational routines should be developed in proper legal framework.

To speed up preparation of the required adjustments it is recommended to involve experts with hands-on experience from economies with well-developed eID usage and e-Governance as they are able to consider the whole legal environment for successful e-Transformation.

9.2.2. Action Plans for Enforcement

Most of the identified and planned adjustments need to be enforced. In line with the preparation, coordination and passing processes, Action Plans for Enforcement should be prepared for every significant legal and policy adjustment.

This approach will speed up the law enforcement and operational readiness for eID implementation.

Preparation of the Action Plans should be coordinated by the institution(s) responsible for the enforcement of corresponding adjustments.

9.2.3. Task Forces

Implementation Task Forces should involve those stakeholders which are significantly affected by the activities or processes regarding those adjustments and corresponding Action Plans.

9.2.4. Enforcement Projects

Task Forces will be responsible for defining the detailed activities for each adjustment, and should also implement the planned activities.

9.2.5. WB economies and EU Interoperability

Coordinated by the RCC, WB economies have developed an ambitious vision of Interoperable Western Balkans - the first fully interoperable region. In line with the prepared Action Plan, there will be series of complex and coordinated activities to achieve economy level issued eID schemes, and trust services mutual recognition and interoperability between WB economies. When following the principles stated in eIDAS regulation and implemented on the EU level, the notified eID schemes and trust services mutually recognised between WB economies will be in principle ready to be recognised by the EU.

To act in the forefront of the WB and EU interoperability activities it is highly recommended, as already stated earlier, for North Macedonia to:

- Choose eID scheme witch will be recognised by the North Macedonia Government as eID with high level of assurance;
- Choose digital signature solution corresponding to eIDAS Qualified Electronic Signature requirements;
- Create Trust Service Provider corresponding to eIDAS Qualified Trust Service Provider requirements.

9.3. Business Model and Organisational Setup

9.3.1. Business Model

eID is an important building block of the e-Transformation (or e-Governance) and has significant impact on the e-Transformation success. Business Model should be set up in a way to support eID usage in public and private sector. Based on our experience and many use-cases/trials around the world, most important recommendations are:

- Electronic authentication and digital signature services via national eID means should be free of charge for physical residents;
- eID should be easy-to-get and easy-to-use;
- Service providers, both public and private could contribute by paying for validation services based on transaction volumes;
- eID solution must get banking sector acceptance and wide usage.

Our recommendation for the Business Model is given in Section 7.1 Business Model of this study.

Based on our recommendation, the Business Model should be prepared, coordinated and decided on the level of the responsible organisation. At least TSP and RA organisation stakeholders should be involved.

9.3.2. TSP and RA Organisational Models

TSP and RA organisations have critical roles in the eID ecosystem. It is crucial that TSP has motivation and necessary resources to build proper organisational routines, technical infrastructure and service portfolio described is Section 6. Simply put, the qualified trust service provider should be trusted in all means, starting from fulfilling all regulatory requirements up to exemplary service quality.

Also, it is highly recommended to have the same TSP issuing certificates and related trust services for mobile-based eID and ID card based eID.

Economy level CA/TSP should be handled as an infrastructure component rather than a profitable business model. It can take 5-7 years to reach operational profitability.

Our recommendations for the Organisational Model are given in Section 7.2.

Based on our recommendations, the Organisation Model should be prepared, coordinated and decided as soon as possible following the Business Model decision because building eIDAS certified TSP requires significant amount of time and resources. TSP is also responsible for development of proper eID issuance procedures corresponding to agreed/decided eIDAS qualification level.

9.3.3. TSP Organisation Setup and Documents

TSP plays one of the key roles in national eID ecosystem. TSP organisation setup, eIDAS compliant procedures development and implementation and mandatory documents preparation requires high level competences, time and experience. It is recommended to involve the existing competences as much as possible.

To speed up the organisation setup, eIDAS compliant procedures development and implementation, and mandatory documents preparation, it is recommended to use competent consultants who have a proven track record in setting up and operating TSP corresponding eIDAS level - qualified trust service provider.

9.3.4. RA Organisation Setup

RA is responsible for following the established and certified eID issuance procedures. As according to our recommendations RA is also responsible for tying the eID to the identity management on economy level it is also responsible for eID lifecycle management.

It is recommended that TSP involves RA personnel into eIDAS required eID issuance procedures development from the initial phases.

9.3.5. Customer Support Setup

Well-functioning customer support is an integral part of the secure and trusted eID ecosystem. Proper customer support routines should be set in cooperation by TSP and RA. One of them can also take operational responsibility for the customer support activities.

9.3.6. TSP and RA Capacity Building

Capacity building is an operational activity to ensure and onboard all competences needed for well-functioning operations.

It is recommended to involve competent consultants in the TSP organisational setup phase who have a proven track record in setting up and operating TSP corresponding eIDAS level (qualified trust service provider). They can assist in preparing proper competence profiles and workload estimations.

9.4. Technical Infrastructure and Processes

9.4.1. TOR and Tender Process

Based on General TOR and Procedural Requirements, the principal technical solution for the eID should be selected and corresponding Business and System Requirements should be specified.

It is recommended to involve competent consultants who have a proven track record in setting up and operating similar solution(s) with corresponding eIDAS levels. They can assist in preparing proper Business and System Requirements for the RFP documents and also provide support in the tender evaluation process.

9.4.2. Technical Implementation

Technical setup of the solution consists of the following components:

- Selected eID solution;
- CA/TSP as eIDAS qualified trust service provider offering full set of main services;
- User environments/APIs (middleware) facilitating usage of eIDs of both carriers;
- eIDAS node to validate the cross-border/boundary usage of nationally accepted eID means.

To speed up the solution implementation process it is recommended to involve competent consultants who have a proven track record in setting up and operating similar solution(s) with corresponding eIDAS levels.

9.4.3. eID Issuance Procedures

eID issuance procedures should be developed based on:

- Selected onboarding methods;
- Requirements of the identity management on economy level;
- eIDAS requirements to the selected electronic authentication scheme.

It is recommended to involve competent consultants who have a proven track record in setting up and operating TSP/RA corresponding eIDAS level (qualified trust service provider).

9.4.4. eID Issuance Technical Setup

eID issuance technical solution should support eID issuance procedures and eID lifecycle management.

eID issuance technical solution specification can be prepared after the eID user onboarding procedures are approved. Depending on the specification complexity, it can be decided whether the separate tender process is required or the solution can be developed using internal resources.

9.4.5. TSP eIDAS Compliant Procedures

TSP should prepare a set of compulsory documents. According to ETSI standards (ETSI EN 319 411-1 and 319 401) the documents must cover facility, management and operational controls used in TSP organisation.

For the operational activities the TSP should prepare a set of required documents and implemented operational routines in compliance with eIDAS Regulation requirements for Qualified Trust Service Provider.

To speed up the preparation of eIDAS compliant procedures and corresponding mandatory documents it is recommended to use competent consultants who have a proven track record in setting up and operating TSP corresponding eIDAS level - qualified trust service provider.

9.4.6. TSP Audit on eIDAS Compliance

TSP services offered must be audited according to ETSI 319 411-2 or similar by an accredited third party auditor.

RegionalCooperationCouncil

Regional Cooperation Council Secretariat
Trg Bosne I Hercegovine 1/V
71000 Sarajevo, Bosnia and Herzegovina
T: + 387 33 561 700
www.rcc.int/balkanbarometer

good.better.regional.


@rccint

RegionalCooperationCouncil

RCCSec


regionalcooperationcouncil_rcc


Regional Cooperation Council


rcc.int