eID level of assurance mapping for Smart-ID according to Article 8 (3) of Regulation (EU) No. 910/2014

Version 3.1

Version History			
Date	**Version**	**Version info**	**Author**
19.10.2021	3.1	Added Secondary Subscriber Authentication and SSAP role for Automated Biometric Identity Verification onboarding method.	SK ID Solutions
15.07.2021	3.0	Amended biometric identification registration method and added Smart-ID for Electronic identification	SK ID Solutions

26.05.2020	2.1	Improved description based on expert committee questions	SK ID Solutions
01.04.2020	2.0	Added biometric identification as a new registration method.	SK ID Solutions
26.08.2019	1.0	Public version	SK ID Solutions

1. Introduction

The current document maps the characteristics of Qualified Smart-ID solution used in Estonia (issued to owners of Estonian national identity document) to the requirements of eIDAS levels of assurance, defined in the COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 pursuant to article 8 (3) of the eIDAS regulation (EU) 910/2014.

The scope of this evaluation is Qualified Smart-ID solution used in Estonia.

The developer of Smart-ID – SK ID Solutions AS has been audited by relevant authorities and the audit (see latest and valid eIDAS certificate for creation EID-SK qualified electronic signature certificates from: https://www.skidsolutions.eu/en/repository/audit/) certifies Qualified Smart-ID as a qualified signature, the highest eIDAS level for signatures. Since same CA procedures are used for authentication certificates, then this certification applies for authentication as well.

According to audit carried out by KPMG in 2017 Smart-ID solution is considered as a suitable solution for strong authentication. Smart-ID meets the Regulatory Technical Standards (RTS) and is capable of guaranteeing the high security of the electronic authentication. SK's information systems, organisation, processes and work methods comply with PSD2, other technical requirements and the online payment legislative requirements of Estonia, Latvia and Lithuania.

SK ID Solutions AS has evaluated based on table below that the Qualified Smart-ID used in Estonia, security level corresponds to the authentication assurance level "HIGH", as defined in the Implementing regulation.

2. Terminology

Term	Definition
ABIV	Automated Biometric Identity Verification. Verification of the Subscriber's identity performed based upon face matching and liveness detection through a deep learning algorithm. In the course of ABIV, comparison is made between a snapshot taken from a selfie video stream against the image of the person read from the eMRTD chip.
CA	Certificate Authority
CSR	Certificate Signing Request
eMRTD	Electronic Machine Readable Travel Document
eMRZ	Electronic Machine Readable Zone
MRZ	Machine Readable Zone
NFC	Near-Field Communication
oMRZ	Optical Machine Readable Zone
Registration Authority	Entity that is responsible for identification and authentication of subjects of certificates. Additionally, the Registration Authority may accept certificate applications, check the applications and/or forward the applications to the Certificate Authority.
SK	SK ID Solutions AS
Secondary Subscriber Authentication	A process that ensures Subscriber awareness about ongoing Smart-ID registration. The authentication method for verifying Subscriber awareness is either delivery of authentication message to Subscriber or requesting Subscriber to perform authentication with electronic identification mean. Secondary Subscriber Authentication provides definite and integral connection to information stating creation of a new Smart-ID account for Subscriber.
SSAP	Secondary Subscriber Authentication Provider. An organisation, which facilitates or performs Secondary Subscriber Authentication during enrolment process for assurance of Subscriber awareness. Secondary Subscriber Authentication Provider is responsible for delivering authentication messages to Subscriber or for performing Secondary Subscriber Authentication with electronic identification mean. Secondary Subscriber Authentication Provider has been verified by Smart-ID Provider to follow the Requirements for Secondary Subscriber Authentication Providers *[24]*.
Smart-ID or also used Qualified Smart-ID	Smart-ID which contains one pair of certificates consisting of the authentication certificate and the qualified electronic signature certificate and their corresponding private keys.

Smart-ID account	Subscriber has to register a Smart-ID account to use services provided by the Smart-ID system. Smart-ID account binds Smart-ID App instance to a Subscriber's identity in the Smart-ID system. In the course of Smart-ID account creation and registration, the identity of the Smart-ID account owner (Subscriber) is proofed by a Registration Authority and the relation between the identity and a key pair is certified by a Certificate Authority. Smart-ID Account has an Advanced or Qualified Electronic Signature key and an Authentication key.
Smart-ID App	A technical component of the Smart-ID system. A Smart-ID App instance installed on a Subscriber's mobile device that provides access to Smart-ID service.
Smart-ID system	A technical and organisational environment which enables electronic authentication and electronic signatures in an electronic environment. The Smart-ID system provides services that allow Subscribers to authenticate themselves to services, to give electronic signatures requested by e-service providers, and to manage their Smart-ID accounts
Subscriber	A natural person to whom the Smart-ID certificates are issued.

3. Mapping of technical specifications and procedures

	Level of Assurance	Requirements	Explanation how requirements are met
3.1. Enrolment			
3.1.1. Application and registration	HIGH (same with LOW and SUBSTANTIAL)	1. Ensure the applicant is aware of the terms and conditions related to the use of the electronic identification means. 2. Ensure the applicant is aware of recommended security precautions related to the electronic identification means. 3. Collect the relevant identity data required for identity proofing and verification.	1. Upon submitting an application for Smart-ID, the Subscriber confirms familiarisation and agreement to the terms and conditions. If the Subscriber applies for Smart-ID via ABIV, then additionally to the terms and conditions, the Subscriber also confirms that he/she agrees with Consent to process personal data via ABIV *[21].* Only adult Subscriber can apply using ABIV. In case of a minor, both the minor and his/her legal representative confirm familiarisation and agreement to the terms and condition upon submitting an application for Smart-ID. Terms and conditions are publicly available at SK website and accessible for Subscriber via Smart-ID self-service web portal. *Source: SK ID Solutions AS - EID-SK Certification Practice Statement [2], clause 4.1.2.1.1, 4.1.2.1.2 and 4.1.2.1.3.* 2. The obligations of the Subscriber are described in terms and conditions document which is

			accepted by Subscriber on request of the certificates. The Subscriber is obligated to: • ensure that he/she no longer uses his/her private key, in the case of being informed that his/her certificate has been revoked or that the issuing CA has been compromised; • ensure that his/her private key is used under his/her control; • immediately inform SK of a possibility of unauthorised use of his/her private key and revoke his/her certificates; • immediately revoke his/her certificates if his/her private key has gone out of his/her possession. *Source: Terms and Conditions for Use of Certificates of Qualified Smart-ID [3], clauses 5.2.7, 5.2.8, 5.2.11 and 5.2.12 respectively.* 3. The Subscriber can be identified either electronically, face to face (in a customer service point) or via ABIV. Electronic identification is possible when the application is signed with a Qualified Electronic Signature compliant with eIDAS Regulation. In that case, SK relies on identification data provided in the signature of the application, which in turn has to be previously verified by the CA that has issued the certificate used for signature. SK also verifies that the CA that issued the

			certificate used for signature, has physically identified the Subscriber before issuing the certificate to him/her. The requirement for Qualified Electronic Signature implies acceptable identification and authentication level required to issue Qualified Certificates. *Source: SK ID Solutions AS - EID-SK Certification Practice Statement [2], clause 3.2.3.1* Physical identity validation is carried out by an employee of customer service point in accordance with the Requirements of Identity Validation for RA *[2]*. In case of verification of physical presence: national identity document as evidence of identity and claimed identity shall be checked: validity of national identity document and authenticity of national identity document (inspect primary security features). Physical identity validation for Smart-ID registration in customer service point is based on physical national identity documents issued based on the national identity document act. In Estonia following documents are accepted: 1) an Identity card; 2) a residence permit; 3) an Estonian citizen passport; 4) a diplomatic passport; 5) a seafarer's discharge book; 6) an alien's passport; 7) a travel document for a refugee;

			8) a certificate of record of service on ships. Smart-ID is not issued based on the documents that has temporary function for returning or temporary use (like temporary travel document, a certificate of return, a permit of return), or documents which do not represent the physical identity e.g. do not contain at least facial image. *Source: SK ID Solutions AS - Requirements of Identity Validation for RA [23], Identity validation requirements for qualified certificate issuance*. ABIV. Identity validation for Smart-ID is based on physical national identity documents issued based on the national identity document act. In Estonia following documents are accepted: 1) an Estonian citizen passport; 2) a diplomatic passport;* 3) a seafarer's discharge book; 4) an alien's passport; 5) a temporary travel document; 6) a travel document for a refugee. *shall be accepted in the future. All the listed national identity documents also serve as biometric documents and as such, follow the requirements from the European Council Regulation (EC) No 2252/2004 of 13 December

			2004 on standards for security features and biometrics in passports and travel documents issued by Member States and the Regulation (EC) No 444/2009 of the European Parliament and of the Council of 28 May 2009 amending Council Regulation (EC) No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States. The regulation is aimed at establishing secure link between the document and its holder by storing on the document its holder's biometric features (including facial image). To guarantee trustworthiness and safety of the solution, biometric data are collected on the document in a way that integrity, authenticity and confidentiality of the data is warranted. The requirements stemming from the respective regulation provide automatic check of the authenticity of the document and identity verification of its holder. All the listed national identity documents also serve as eMRTD. Authenticity check of an eMRTD is described in sub-clause 3.1.2. ABIV consists of the following steps. The Subscriber's identity is verified based on his/her personal information read from the chip on eMRTD presented by the Subscriber for identity validation. Authenticity of the eMRTD chip is verified based on authentication and security mechanisms supported by the chip. Validity check of eMRTD is performed based on document validity checking service offered by the eMRTD

			issuing country[1]. Biometric verification of the Subscriber is based on the facial image retrieved from data on the eMRTD chip with NFC technology and the facial image captured in the liveness session during registration via Smart-ID app. During the identity verification session, liveness of the Subscriber's facial image is verified. *Source: SK ID Solutions AS - EID-SK Certification Practice Statement [2], clause 3.2.3.1* Each registration method risk assessment based additional measures are applied to increase applicant awareness. For example, for Smart-ID registration with Mobile-ID we are sending additional notification and one-time password to the Subscriber's Mobile-ID phone number. For Smart-ID registration via ABIV, Secondary Subscriber Authentication is performed in order to ensure Subscriber awareness about ongoing Smart-ID registration. The Secondary Subscriber Authentication is facilitated or performed by Secondary Subscriber Authentication Provider using with following method: • delivering authentication message (one-time password) to Subscriber with unique secret generated by Smart-ID System, that Subscriber has to represent through Smart-ID app to Smart-ID System during

[1] For Estonian eMRTDs validity is checked against X-road 'itdak' service (EE/GOV/70008747/itdak)

			registration process and Smart-ID system will verify the unique secret's correctness; or • authenticating Subscriber with electronic identification mean that corresponds minimal to assurance level substantial. *Source: SK ID Solutions AS - EID-SK Certification Practice Statement [2], clause 4.1.2.1.3* As a universal risk mitigation measure notifications about the creation of a new Smart-ID account are sent to the existing contacts.
3.1.2. Identity proofing and verification (natural person)	LOW	1. The person can be assumed to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity. 2. The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid. 3. It is known by an authoritative source that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.	1. N/A, because the identity of the applicant is always verified, not assumed. 2. N/A, because the evidence of identity of the applicant is always verified, not assumed. 3. N/A, identity existence is always verified, not assumed.

	SUBSTANTIAL	Level low, plus one of the alternatives listed in points 1 to 4 has to be met: 1. The person has been verified to be in possession of evidence recognised by the Member State in which the application for the electronic identity means is being made and representing the claimed identity and the evidence is checked to determine that it is genuine; or, according to an authoritative source, it is known to exist and relates to a real person and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired evidence; or 2. An identity document is presented during a registration process in the	Physical identification. Physical identity validation is carried out by an employee of customer service point in accordance with the Requirements of Identity Validation for RA *[2]*. National identity document as evidence of identity and claimed identity shall be checked: • validity of national identity document from Police and Border Guard Board public service[2] • authenticity of national identity document (inspect primary security features) Subscriber is identified as the claimed identity through comparison of one or more physical characteristic of the person with national identity document, including verification that document presented is representing claimed identity. Two persons shall verify the identity of subscriber to minimize the risk of false identity. This four-eye control is implemented in customer service point or as a back-office procedure. For four-eye control in the back-office the second employee has to check and compare the match of the person's data and identity document data from copy of identification document with data on the

[2] https://www.politsei.ee/en/inquiries/document-validity-check

		Member State where the document was issued and the document appears to relate to the person presenting it and steps have been taken to minimise the risk that the person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents; or 3. Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level substantial, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 of the European Parliament and of the Council (1) or by an equivalent body;	application. Also, that document copy is copy of genuine identification document. *Source: SK ID Solutions AS - Requirements of Identity Validation for RA [23], Identity validation requirements for qualified certificate issuance*. Electronic identification. Electronic identification is possible when the application is signed with a Qualified Electronic Signature compliant with eIDAS Regulation using national ID-card, mobile-ID or Smart-ID certificates for signing. Subscriber is identified with high level electronic identification means (for which issuance physical presence is necessary) national ID-card, Mobile-ID certificates for authentication. ABIV. eMRTD as evidence of identity and claimed identity is checked as follows: • an eMRTD is checked via the oMRZ and from the eMRZ. • The oMRZ data is checked for integrity and plausibility and used to calculate the card access number required to read the eMRZ and facial image from eMRTD chip. The electronic read out procedure comprises the digital verification of the electronic security mechanism provided by the eMRTD. The process is recognized as electronic identification and includes the verification of the integrity and

		or 4. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the electronic identification means serving as the basis has not been notified, the assurance level substantial or high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body.	authenticity of the eMRZ and facial image data through recalculating and verifying the certificate chain up to the official ID document issuing countries CA (Country Signing CA). In details the eMRTD authenticity and integrity is verified using mechanisms that particular eMRTD supports: 1) chip clone detection mechanisms: a) AA - Active Authentication, or b) CA - Chip Authentication 2) PA - Passive Authentication a) verifying CSCA against trusted CSCA list[3], b) verifying certificate chain (CSCA, DS certs), c) validating DS signature over Document Security Object (SOD), d) recalculating hashes of Data Groups and validating against hashes retrieved from SOD.

[3] Trusted CSCA list is compiled based on BSI CSCA Master List (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekAusweise/CSCA/GermanMasterList.html). Trusted CSCA list is updated against BSI CSCA Master List on monthly basis, and quarterly audited by SK.

			• Furthermore the oMRZ and the eMRZ data are verified against each other. It is checked that the attempts for registration with the same eMRTD do not exceed given limit. • On top the detailed checks with regard to the ID document authenticity, the validity of ID document is verified using respective service offered by the eMRTD issuing country[4]. SK's conformity assessment body has rated controls performed with regard to the evaluation of national identity document validity, authenticity and integrity to be stronger than the controls provided by a typical average human based face2face identification. The verification of the Subscriber's identity is performed based upon face matching through a deep learning algorithm based on comparison of a snapshot taken from a selfie video stream against the ICAO compliant picture of the person read via NFC from the eMRTD (means: the reference picture material is of a defined quality as specified by ICAO). Presentation attack detection (PAD) and face matching are the two capabilities of biometric technology. Deployed technologies address various presentation attacks (e.g. still or video

[4] For Estonian eMRTDs validity is checked against Police and Boarder Guard Board registry over X-road

			imagery submission, usage of high quality masks, replay of a previous video capture). System is continually monitored and reacting to evolving threats. Face matching algorithm uses the latest advances in deep neural networks, to deliver matching performance with highest level of assurance. It is optimized for 'selfies' taken on smartphones and PCs in a huge variety of lighting conditions, poses and facial features. The key risks from False Accepts are managed and mitigated with the following framework: 1) It is assumed that smart device and its software have been fully compromised. 2) It is assumed that information received from the device cannot necessarily be trusted. 3) Physical impersonation is a non-scalable threat because on a large scale expensive and impractical to undertake. 4) Forgery is a low-cost and scalable threat as faces are publicly available credentials. 5) Replay is a major and scalable threat as video imagery can become available to an attacker. 6) Server penetration resilience, as any server directly exposed to the internet will be subject for potential penetration and compromise.

			In terms of risks very high assurance profile has been deployed with False Accept Rate (FAR) 0.0001 and Combined Attack Presentation Classification Error Rate (CAPCER) 0.0002. All algorithms developed are evaluated thoroughly before deployment. Evaluation of biometric matching systems is governed by ISO/IEC 19795-1:2006. Evaluation of biometric security is partially governed by ISO/IEC 30107-3:2017. Whist certain many forms of attack, such as direct injection replay attacks and doctored imagery attacks, are not included in the scope of this standard, the biometric verification service provider has extended the testing methodology to cover wider forms of biometric attacks. The NPL, the official national UK research lab, specialized and recognized for evaluation of biometric methods, consider that the methodology for testing and reporting (error rates specified, etc.) biometric verification performance conforms to the relevant requirements of ISO/IEC 19795-1:2006, and that the methodologies for testing and reporting presentation attack detection sufficiently conform to ISO/IEC 30107-3:2017 to support the iProov performance claims. iProov is SK's partner for providing facial recognition service. SK's conformity assessment body has rated controls performed in the course of the Subscriber's identity verification to be stronger

			than the controls provided by a typical average human based face2face identity verification. *Source: Audit Reports [22]*
	HIGH	Requirements of either point 1 or 2 have to be met: 1. Level substantial, plus one of the alternatives listed in points (a) to (c) has to be met: (a) Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source; and the applicant is identified as the claimed identity through comparison of one or more physical characteristic of the person with an authoritative source; or	Physical identification. Subscriber is identified as the claimed identity through comparison of one or more physical characteristic of the person with national identity document, including verification that document presented is representing claimed identity. *Source: SK ID Solutions AS - EID-SK Certification Practice Statement [2]* Electronic identification. Electronic identification is possible when the application is signed with a Qualified Electronic Signature compliant with eIDAS Regulation using national ID-card, mobile-ID or Smart-ID certificates for signing. Subscriber is identified with high level electronic identification means (for which issuance physical presence is necessary) national ID-card, mobile-ID or Smart-ID certificates for authentication. In that case, SK relies on identification data provided in the signature of the application, which in turn has to be previously verified by the CA that has issued the certificate used for signature. SK also verifies that the CA that issued the Certificate used for signature, has physically identified the Subscriber before issuing the Certificate to him/her. The requirement for Qualified Electronic Signature implies acceptable identification and

		(b) Where procedures used previously by a public or private entity in the same Member State for a purpose other than the issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.2 for the assurance level high, then the entity responsible for registration need not to repeat those earlier procedures, provided that such equivalent assurance is confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of the earlier procedures remain valid; or (c) Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level high, and taking into account the risks of a change in the person identification data, it is not required to repeat the identity proofing and verification processes. Where the	authentication level required to issue Qualified Certificates. *Source: SK ID Solutions AS - EID-SK Certification Practice Statement [2], clause 3.2.3.1* The validity (non-revocation) of previously issued national ID-card, Mobile-ID or Smart-ID certificates are checked via OCSP service. The validity of Qualified Electronic Signature in Smart-ID application is validated by using signature validation service. ABIV consists of the following steps. The Subscriber's identity is verified based on his/her personal information read from the chip of eMRTD presented by the Subscriber for identity validation. Person identification data read from eMRTD chip (excl. facial image) is validated against Population Registry. Authenticity of the eMRTD chip is verified based on authentication and security mechanism supported by the chip. Validity check of eMRTD is performed based on document validity checking service offered by the eMRTD issuing country. Biometric verification of the Subscriber is based on the facial image retrieved from data on eMRTD chip with NFC technology and the facial image captured in the liveness session during registration via Smart-ID App. During the identity verification session, liveness of the Subscriber's facial image is verified.

		electronic identification means serving as the basis has not been notified, the assurance level high must be confirmed by a conformity assessment body referred to in Article 2(13) of Regulation (EC) No 765/2008 or by an equivalent body and steps are taken to demonstrate that the results of this previous issuance procedure of a notified electronic identification means remain valid. OR 2. Where the applicant does not present any recognised photo or biometric identification evidence, the very same procedures used at the national level in the Member State of the entity responsible for registration to obtain such recognised photo or biometric identification evidence are applied.	*Source: SK ID Solutions AS - EID-SK Certification Practice Statement [2], clause 3.2.3.1*
3.1.3. Identity proofing and verification (legal person	N/A, Smart-ID is used only for identification of natural person.		
3.1.4. Binding between the	N/A, Smart-ID is used only for identification of natural person.		

electronic identification means of natural and legal persons			
3.2. Electronic identification means management			
3.2.1. Electronic identification means characteristics and design	LOW	1. The electronic identification means utilises at least one authentication factor. 2. The electronic identification means is designed so that the issuer takes reasonable steps to check that it is used only under the control or possession of the person to whom it belongs.	N/A
	SUBSTANTIAL	1. The electronic identification means utilises at least two authentication factors from different categories. 2. The electronic identification means is designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.	1. Smart-ID utilises two authentication factors: possession-based and knowledge-based. The possession based factor is the mobile device owned by the Subscriber. In order to prove that the mobile device is in possession of the Subscriber and the Subscriber is in control of the device, a one-time password (OTP) has to be presented by the Smart-ID App over the secure channel in case of each transaction. The knowledge-based factor is in the form of the signature share computed from the data to be signed by using the Subscriber's PIN code, presented by the Subscriber and the Smart-ID App over the secure channel.

			2. Smart-ID can be used for electronic identification only after the successful authentication and access control procedure of the Subscriber, performed on the Smart-ID server. The procedure includes validation of both the possession-based and the knowledge-based authentication factors. This assures that the Smart-ID is used under the control and in the possession of the person to whom it belongs. *Source: SK ID Solutions AS - EID-SK Certification Practice Statement [2], clause 6.2.8.1.2.*
	HIGH	Level substantial, plus: 1. The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential 2. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.	1. Smart-ID system protects the electronic identification function against duplication by detecting the usage of incorrect possession-based factor (the one-time password). This situation indicates that Subscriber's local environment has been cloned. Smart-ID server system (the SercureZone component) shall initiate the revocation of the Subscriber's certificate and destroy the respective key pair after detecting such situation. The Smart-ID server side component SecureZone which is responsible for executing the clone detection mechanism is additionally Common Criteria certified and compliant with level EAL4 augmented with AVA_VAN.5 (Advanced methodical vulnerability analysis). This means that Smart-ID SecureZone is resistant to attacks performed by an attacker possessing High attack potential.

			Smart-ID server-side system is deployed in a dedicated tamper-proof environment according to the requirements laid down in standards ETSI EN 319 401 *[17]* , ETSI EN 319 411-1 *[18]* and ETSI EN 319 411-2 *[19]* . This means that requirements on security management procedures, asset management, physical and environmental security, human resources, network security, etc. are followed in the course of operating the Smart-ID system. The Smart-ID operational environment has been audited by independent auditors who have assured compliance with the requirements. Also, the development life-cycle procedures as well as the development environment of Smart-ID Common Criteria evaluated components are designed to be protected against tampering, i.e. it is ensured that the content and modifications of the developed component are controlled by trusted personnel and only the content that is relevant and is of adequate quality will be incorporated in the Smart-ID. The development processes and development environment have been evaluated in the course of the Smart-ID Common Criteria evaluation and are in compliance with the requirements of Common Criteria for Information Technology Security Evaluation Part 3, Version 3.1 Revision 5, section 15.4 "Development security (ALC_DVS)" *[8]*.

			Additionally, the Subscriber's part of the private key is protected from tampering in the Subscriber's environment while at rest. The private key is encrypted with the key derived from the Subscriber's entered PIN code, the key is decrypted with PIN for each transaction. 2. Smart-ID utilizes a number of security mechanisms that allow the Subscriber to reliably protect it against use by others: • The cryptographic threshold signature protocol used in the Smart-ID system for electronic identification (as well as for electronic signature creation) has been developed to disperse the risk and responsibility of securing the private key. The responsibility has been divided between multiple system components which enables to add an extra level of security. The Subscriber's private key is generated in shares (one in the Subscriber's environment, i.e. the mobile device; the other in the tamper-proof Smart-ID server environment). In order to use the private key, the shares are never combined in a single physical location. Instead, the individual shares are used to create the shares of the cryptogram. Only when all shares of the cryptogram are combined, the compound cryptographic result is achieved.

			With the usage of such kind of protocol, it is impossible for the privileged users (administrators with access to the server-side operational environment of Smart-ID system) to perform any electronic identification operations on behalf of the Subscriber as the Smart-ID server alone doesn't create the whole cryptogram on behalf of the Subscriber, but they both participate in the cryptographic protocol. • Before inserting the PIN code, the Subscriber has to verify, if he is agreeing with the authentication request on the Smart-ID App. The e-service where the electronic identification session is initiated computes the verification code based on the challenge that the Subscriber is to sign. The verification code is displayed on the site of the e-service and also in the Subscriber's Smart-ID App, along with the name of the service. Only after verifying that the verification codes match and that the context of the operation is agreed, the Subscriber is to enter the PIN code. • In order for the Subscriber to use the Smart-ID for electronic identification, the validation of both of the authentication factors (knowledge-based and possession-based) must succeed. The Subscriber is responsible for not disclosing the PIN code and for using the smart device according to the best security practices. The Smart-ID system itself additionally

			protects the PIN code by not storing the PIN anywhere and by not providing any reference points for the attacker to conduct off-line brute force attack and to check, which PIN is correct and which is not. After a number of unsuccessful PIN insertions the Smart-ID system closes the account, initiates the revocation of the Subscriber's certificates and deletes the private keys. The possession-based factor is protected by clone detection mechanism, as described in point 1 of the current section. • The Smart-ID system uses trusted path (encryption) to communicate between the Smart-ID App in the Subscriber's environment and the backend server system. This ensures that the authentication session is not disclosed to others. *Source:* • *Smart-ID certificate for eIDAS compliant QSCD [4]* • *Smart-ID SecureZone Common Criteria certificate [5]* • *Smart-ID SecureZone Common Criteria certification report [6]* • *Common Criteria for Information Technology Security Evaluation Part 3, Version 3.1 Revision 5 [8]*

			• *Smart-ID SecureZone Security Target [9]*
3.2.2. Issuance, delivery and activation	LOW	After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed to reach only the intended person.	N/A
	SUBSTANTIAL	After issuance, the electronic identification means is delivered via a mechanism by which it can be assumed that it is delivered only into the possession of the person to whom it belongs.	N/A
	HIGH	The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.	After a Smart-ID App instance installation on a Subscriber's mobile device, account registration must be completed to start using Smart-ID. From the Subscriber's perspective, the registration process may have some differences depending as an example on the authentication method used or the age (under age of 18 users have special registering flow[5]) of the Subscriber. The options include the ID-card, Mobile-ID, Smart-ID, on-site registration or ABIV. Depending on the particular technology, the authentication may take place in the mobile device itself (for example, in case of Mobile-ID) or the Subscriber may be instructed to open up the desktop browser session (for example, in case of ID-card) or the Subscriber may be instructed to visit the on-site registration office. Registration via ABIV includes steps, where the Subscriber has to present eMRTD to smart device

[5] Excluding registration via ABIV

			and capture selfie-video, whereas authentication process will be performed in Smart-ID backend servers. In addition, during ABIV registration, Secondary Subscriber Authentication is performed in order to ensure Subscriber awareness about ongoing Smart-ID registration. The Secondary Subscriber Authentication is facilitated or performed by Secondary Subscriber Authentication Provider using with following method: • delivering authentication message to Subscriber with unique secret generated by Smart-ID System, that Subscriber has to represent through Smart-ID app to Smart-ID System during registration process and Smart-ID system will verify the unique secret's correctness; or • authenticating Subscriber with electronic identification mean that corresponds minimal to assurance level substantial. The overall process follows same basic steps: Smart-ID App begins to generate the shares of the authentication and signature key pairs. Subscriber sets PINs for the shares of the key pairs. During registration Smart-ID App initiates the registration session with the Smart-ID system and requests for the time-limited registration nonce computes the registration token and displays the token to the Subscriber.

			Subscriber enters the registration token to the identity proofing process in the desktop browser or shows the registration token to the on-site registration office employee. This binds together the fresh key material generated inside the Smart-ID App instance and the identity proofing session inside the Subscriber's browser or on-site registration office. The identity proofing process takes place inside the registration authority component and when finished, sends the confirmed Subscriber's identity details and the registration token to the Smart-ID system. Smart-ID system verifies the registration nonce, asks the Smart-ID SecureZone to generate its own shares of the key pairs and computes the composite public keys and generates the CSRs with the Subscriber's identity for issuing the certificates to the authentication key pair and signature key pair. Smart-ID App receives the CSRs and asks Subscriber to confirm the identity details and to enter the PIN1 and PIN2 to sign the CSRs. Subscriber confirms the identity details and enters the PIN1 and PIN2. Smart-ID App uses the shares of the corresponding key pairs to compute the share of the signature of CSRs and sends the result to the Smart-ID system. Smart-ID system forwards the signature completion request to the Smart-ID SecureZone. Smart-ID SecureZone completes the CSR

			signature generation steps with the shares of the key pairs and returns the composite signatures to the Smart-ID system. Smart-ID system sends the certificate issuing request to the Smart-ID CA along with the CSRs, Subscriber identity details and other verification data. Smart-ID CA issues the certificates. Smart-ID system activates the Subscriber's account. During the Subscriber registration process, the clone detection mechanism is already in force, which additionally enables to ensure that the user remains in possession of the device during the whole registration process. *Source:* • *SK ID Solutions AS - EID-SK Certification Practice Statement [2], 6.2.8.1.1 respectively* • *Smart-ID technical overview [7], "Registration Service" section.*
3.2.3. Suspension, revocation and reactivation	HIGH (same with LOW and SUBSTANTIAL)	1. It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner. 2. The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation. 3. Reactivation shall take place only if the same assurance	1. Suspension of Smart-ID certificates is not available. The Subscriber can request revocation of Smart-ID certificates via the help line or customer service point help line. The operator of the help line verifies the Subscriber by using the identification data in the Subscriber's application. After the Subscriber's identity and legality to request revocation is verified, the

		requirements as established before the suspension or revocation continue to be met.	operator of the help line revokes the Smart-ID certificates. If the operator of the customer service point help line is unable to verify the Subscriber's identity, the Subscriber can be directed to request revocation via the help line. Revocation request submitted via the help line or the customer service point help line is recorded. Alternatively, the Subscriber can request revocation of Smart-ID via Smart-ID self-service web portal, where the Subscriber is authenticated using verified electronic authentication. The Subscriber has to confirm the application there. The Smart-ID self-service web portal or Smart-ID App sends the request for revocation to SK. The Subscriber can also request revocation of Smart-ID certificates by deleting his/her Smart-ID account in Smart-ID App. In this case, revocation of the certificates is possible only from the Smart-ID App instance that the Subscriber used for registering his/her Smart-ID account. The Subscriber can also submit a signed application for revocation of the certificates to customer service point or SK customer service point. In case of a signed application, the identity of the person is verified based on the identity document by an employee of customer service point or SK customer service point.

			After SK has received an application for revocation of the certificate, the procedure for processing the request is the following: • the revocation application is registered by an employee of Customer Service Point or SK Customer Service Point; • the person filing an application for revocation is verified; • the compliance of the application for revocation with the CP for Smart-ID is verified in SK's information system; • the documentation on which the application for revocation was based is archived; • the Subscriber is notified of revocation of the Certificates. After SK has received an application for revocation, SK processes it immediately. The revocation of the certificate is recorded in the certificate database of SK. The Subscriber has a possibility to verify from the Smart-ID system that the certificate has been revoked. *Source: SK ID Solutions AS - EID-SK Certification Practice Statement [2], clause 4.9.3.1* 2. Please refer to the relevant description under point 1.

			3. Smart-ID reactivation is not available. After revoking certificates subscriber can apply a new Smart-ID based on initial registration process.
3.2.4. Renewal and replacement	LOW (same with SUBSTANTIAL)	Taking into account the risks of a change in the person identification data, renewal or replacement needs to meet the same assurance requirements as initial identity proofing and verification or is based on a valid electronic identification means of the same, or higher, assurance level.	A separate renewal and replacement procedure is not available. The new enrolment procedure must be completed.
	HIGH	Level low, plus: Where renewal or replacement is based on valid electronic identification means, the identity data is verified with an authoritative source.	N/A
3.3. Authentication			
3.3.1. Authentication mechanism	LOW	1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity. 2. Where person identification data is stored as part of the authentication mechanism, that information is secured in order to protect against loss and against	1. Please refer to the relevant description under Substantial level. 2. The integrity and confidentiality of the Subscriber's identification data is protected by using secure encrypted communication channel between the Smart-ID server and the e-service provider, as well as between the Smart-ID server and the Smart-ID App. Sensitive data is always stored in encrypted form. There are no reference points stored for the attacker to conduct off-line brute force

		compromise, including analysis offline. 3. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms.	attack to derive the private key of the Subscriber. 3. Please refer to the relevant description under High level. *Source: Smart-ID RP API documentation [10]*
	SUBSTANTIAL	Level low, plus: 1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication. 2. The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential	1. The dynamic authentication prior to releasing the Subscriber's identification data to the e-service provider (relying party) is carried out on several levels. • Firstly, the e-service provider to whom the Subscriber's identification data is released shall use secure encrypted HTTPS connection with the Smart-ID server which ensures confidentiality of the data exchanged over the communication channel. Additionally, the Smart-ID server shall authenticate and authorize the e-service based on its IP address and the service name. • Secondly, the Subscriber's shall dynamically verify the authenticity of the electronic identification session. The e-service computes the verification code

		can subvert the authentication mechanisms.	based on the one-time challenge that the Subscriber is to sign. The verification code is displayed on the site of the e-service and also in the Subscriber's Smart-ID App, along with the name of the e-service. Only after checking that the verification codes match and that the context of the operation is agreed, the Subscriber is to enter the PIN code. Before sending the verification code to the Subscriber's device, the Smart-ID server checks the correctness and validity of the Subscriber's Smart-ID account. If the Subscriber does not have a proper account available for the transaction then the transaction is not carried out and an error is returned to the e-service provider. • Thirdly, the Smart-ID authentication mechanism in essence is based on dynamic challenge-response algorithm by using digital signatures. In the course of the authentication session, the Subscriber shall use his part of the private key to sign a dynamic one-time challenge generated by the e-service which initiates the session. The validity of the signed challenge shall be reliably verified by the Smart-ID backend server before adding the server's signature share (according to Threshold Signature Scheme Protocol, TSSP) and returning the composite signature to the e-service provider. Additionally, the e-service provider shall also verify the correctness of the signed challenge by

			using the Subscriber's public key certificate. 2. Please refer to the relevant description under High level. *Source:* • *Smart-ID SecureZone Security Target [9]* • *Smart-ID RP API documentation [10]*
	HIGH	Level substantial, plus: The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.	The following security mechanisms are used against guessing, eavesdropping, replay and manipulation of communication: • Guessing the PIN code is mitigated by: o Utilising PIN complexity and length requirements and thus ensuring that the PIN code which is chosen by the Subscriber is not easily guessed. o Not storing the PIN anywhere and not providing any reference points for the attacker to conduct off-line brute force attack and to check, which PIN is correct and which is not. After a number of unsuccessful PIN insertions the Smart-ID system closes the account, initiates the revocation of the Subscriber's certificates and deletes the private keys.

			○ Utilising PIN counter mechanism in the Smart-ID server to restrict the unsuccessful signer authentication by locking their key pair for a defined time after a number of incorrect PIN entries have been detected. After the total limit of incorrect PIN validations is reached, the account is permanently closed, the certificates revoked and the private keys deleted. • Guessing the private key is mitigated by using well-known cryptographic algorithms for generating the key pairs and a secure source for the randomness. The Smart-ID App also checks the quality of the random number provided by the environment's random number generator and quits the key generation procedure, if the quality tests are not passed. • Eavesdropping, replay and manipulation of communication is mitigated by using encrypted and trusted channel to communicate between the Smart-ID App in the Subscriber's environment and the backend Smart-ID server system. The secure channel is implemented on several layers: HTTPS communication channel is used to communicate with the Smart-ID Core system component. The Smart-ID App is authenticating the Smart-ID system with the X.509 certificate pinning. Additionally, an asymmetric RSA key

			pair (the Key Transport Key) is used in order to encrypt specific sensitive data, which is meant to be delivered directly to the Smart-ID SecureZone component. Also, a symmetric AES key (the Transport Encryption Key) is used to encrypt and decrypt the messages between the specific instance of the Smart-ID App and the Smart-ID SecureZone component. The Smart-ID is Common Criteria certified and compliant with level EAL4 augmented with AVA_VAN.5 (Advanced methodical vulnerability analysis). This means that the system is designed to be resistant to attacks performed by an attacker possessing High attack potential. *Source:* • *Smart-ID certificate for eIDAS compliant QSCD [4]* • *Smart-ID SecureZone Common Criteria certificate [5]* • *Smart-ID SecureZone Common Criteria certification report [6]* • *Smart-ID SecureZone Security Target [9]*
3.4. Management and organisation			
3.4.1. General provisions	HIGH (same with LOW and SUBSTANTIAL)	1. Providers delivering any operational service covered by this Regulation are a public authority or a legal entity recognised as such by national	1. Smart-ID is operated by SK ID Solutions AS. SK ID Solutions AS is private company, a legal person, created according to the Estonian Commercial Law and acting upon Estonian law. Smart-ID service is included into Trusted

		law of a Member State, with an established organisation and fully operational in all parts relevant for the provision of the services. 2. Providers comply with any legal requirements incumbent on them in connection with operation and delivery of the service, including the types of information that may be sought, how identity proofing is conducted, what information may be retained and for how long. 3. Providers are able to demonstrate their ability to assume the risk of liability for damages, as well as their having sufficient financial resources for continued operations and providing of the services. 4. Providers are responsible for the fulfilment of any of the commitments outsourced to another entity, and compliance with the scheme policy, as if the providers themselves had performed the duties. 5. Electronic identification schemes not constituted by national law shall have in place an effective termination plan. Such a plan shall include orderly discontinuations of service or	List of Estonia (for issuing EID-SK qualified e-signature certificates) and SK ID Solution is qualified trust service provider. Subcontractors involved into service provision are also private entities, legal persons registered and acting upon Estonian law. SK as qualified trust service provider carries overall responsibility for conformance with the procedures and requirements for service provision defined according to regulation and standards. SK has a documented agreements and contracts with its subcontracting and outsourcing parties provisioning services. SK has defined in these agreements and contracts the liability, relevant requirements and right to audit subcontracting and outsourcing parties to be ensured that they are bound to implement any requirements and controls necessary for adequate service provision. The fulfilment of this requirement is checked during the eIDAS conformity assessment audit. 2. The SK ID Solutions AS - EID-SK Certification Practice Statement *[2]* is including the description how SK as qualified trust service provider is operating and delivering the service according to the

		continuation by another provider, the way in which relevant authorities and end users are informed, as well as details on how records are to be protected, retained and destroyed in compliance with the scheme policy.	requirements, also including what type of information is recorded, how identity proofing is conducted and which information is retained and for how long. The fulfilment of these requirements is checked during the eIDAS conformity assessment audit. 3. The ability to carry liability to damages is mitigated by Professional Indemnity Insurance. In accordance with the relevant legislation, SK publishes the terms of the compulsory insurance policy on its website https://www.sk.ee/en/repository/insurance/. SK has the financial stability and resources required to operate in conformity with its policies and practice statements. The fulfilment of these requirements is checked during the eIDAS conformity assessment audit. 4. Please refer to the relevant description under point 1. 5. SK ID Solutions AS - SK Trust Services Practice Statement *[11],* clause 5.8 is including publicly available termination plan for customers and relying parties. The more specific and internal termination plan is approved by CEO.

			The fulfilment of these requirements is checked during the eIDAS conformity assessment audit. *Source:* • *SK ID Solutions AS - SK Trust Services Practice Statement* [11] • *SK ID Solutions AS - EID-SK Certification Practice Statement [2]* • *eIDAS certificate for creation EID-SK qualified e-signature certificates [12]* • *Terms and Conditions for Use of Certificates of Qualified Smart-ID [3]*
3.4.2. Published notices and user information	HIGH (same with LOW and SUBSTANTIAL)	1. The existence of a published service definition that includes all applicable terms, conditions, and fees, including any limitations of its usage. The service definition shall include a privacy policy. 2. Appropriate policy and procedures are to be put in place in order to ensure that users of the service are informed in a timely and reliable fashion of any changes to the service definition and to any applicable terms, conditions, and privacy policy for the specified service. 3. Appropriate policies and procedures are to be put in place that provide for full and correct	1. Terms and Conditions *[3]* is document that describes obligations and responsibilities of the Subscriber while using certificates. SK guarantees the availability and access in a public data communications network to this document. Terms and Conditions *[3]* describe main policies and practices followed by SK and provided in Certificate Policy for Qualified Smart-ID *[1]*, EID-SK Certification Practice Statement *[2]* and SK ID Solutions AS - SK Trust Services Practice Statement *[11]* (e.g. Disclosure Statement), including: certificate acceptance; certificate type, validation procedures and usage; reliance limits; Subscriber's rights and obligations; SK rights and obligations; certificate status checking obligations of

		responses to requests for information.	relying parties; limited warranty and disclaimer/limitation of liability; applicable agreements, CPS, CP; privacy policy and confidentiality; refund policy; applicable law, complaints and dispute resolution; SK and repository licences, trust Marks and audit; contact information. Terms and Conditions *[3]* is following the structure of disclosure statement and subscriber agreement according to clause 6.3.4 of standard ETSI EN 319 411-1 *[18]*. In case of biometric verification, the rights and obligations of the Subscriber and SK are also described in Consent to process personal data via Automated Biometric Identity Verification *[21]*. 2. Upon submitting an application for Smart-ID, the Subscriber confirms familiarisation and agreement to the Terms and Conditions *[3]*. Terms and Conditions *[3]* together with the enforcement dates are published on SK's website no less than 30 days prior to taking effect. The Subscriber’s individual notices are communicated via the Subscriber’s email address or mobile phone number provided in registration form for Smart-ID account.

			As enrolment procedure for Smart-ID via ABIV comprises of collecting and processing the Subscriber's biometric data that fall under special category of personal data, the Subscriber is obligated to agree with Consent to process personal data via Automated Biometric Identity Verification *[21].* It includes the contact for information requests. 3. The section 13 of Terms and Conditions *[3]* describe the procedure and provide the contact for information requests and disputes. Consent to process personal data via Automated Biometric Identity Verification *[21]* includes the contact for information requests.
3.4.3. Information security management	LOW	There is an effective information security management system for the management and control of information security risks.	Please refer to the relevant description under High level.
	HIGH (same as SUBSTANTIAL)	Level low, plus: The information security management system adheres to proven standards or principles for the management and control of information security risks.	In the field of security management, SK guides itself by the generally recognised standards, e.g. ISO/IEC 27001: 2013 "Information technology. Security techniques. Information security management systems." *[20]*, and other standards required by regulations and law. SK's services meet specific industry security standards as ETSI EN 319 401 *[17]*, ETSI EN 319 411-1 *[18]*, ETSI EN 319 411-2 *[19]*. SK's security management policy documents include the security controls and operating

			procedures for SK facilities, systems and information assets providing the services. SK carries out and revises risk assessment regularly in order to evaluate business risks and determine the necessary security requirements and operational procedures. SK management approves risk assessment and accepts the residual risks identified. SK management establishes the security policy, which forms a basis for consistency and completeness of information security and management support. SK Chief Executive Officer approves policies and practices related to information security for the overall SK services. SK management communicates information security policies and procedures to employees and relevant external parties who are impacted by it. In addition, SK management sets out SK approach to manage information security objectives for Trust Services, including auditable procedures for internal control. SK has achieved ISO/IEC 27001: 2013 certification. Certificates of conformity and audit reports for SK and SK services are available at SK website: • eIDAS certificate for creation EID-SK qualified e-signature certificates *[12]*

			• ISO/IEC 27001: 2013 certificate *[13]*
3.4.4. Record keeping	HIGH (same with LOW and SUBSTANTIAL)	1. Record and maintain relevant information using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention. 2. Retain, as far as it is permitted by national law or other national administrative arrangement, and protect records for as long as they are required for the purpose of auditing and investigation of security breaches, and retention, after which the records shall be securely destroyed.	1. SK secures confidential information, personal data and information intended for internal use from compromise and refrains from disclosing it to third parties by implementing different security controls described in more detailed way in SK ID Solutions AS - EID-SK Certification Practice Statement *[2]* and SK ID Solutions AS - SK Trust Services Practice Statement *[11]*, in sections 5 and 6. SK is following GDPR *[16]*, eIDAS regulation *[14]*, Electronic Identification and Trust Services for Electronic Transactions Act *[15]* and ETSI standards *[17, 18, 19]* for protecting its data records, logs and archives. The data recording and retention, also data protection controls are checked during the eIDAS audit. 2. SK ensures that all relevant information concerning the operation of the Smart-ID services is recorded for providing evidence for the purpose of legal proceedings. This information includes the archive records that are required for proving the validity of certificates and the audit log of the trust service operation and transactions. According to the Electronic Identification and Trust Services for Electronic Transactions Act

			[15], SK and its registration authorities retain physical or digital archive records about certificate applications, signed Subscriber agreements, registration information (including evidences of Subscriber identity verification) and requests or applications for revocation are retained at least for 10 years after validity of relevant certificate and audit logs kept for 10 years after logging event. Although Electronic Identification and Trust Services for Electronic Transactions Act *[15]* is directly applicable to qualified certificates for electronic signatures, the same requirements are applied to the certificate for authentication as these certificates are issued together and are issued under similar certificate policy (certificates for authentication under NCP+ and qualified certificates for electronic signature QCP-n-qscd according to ETSI EN 319 411-1 and -2 *[18, 19]*). The retention of data is checked during the eIDAS conformity assessment.
3.4.5. Facilities and staff	HIGH (same with LOW and SUBSTANTIAL)	1. The existence of procedures that ensure that staff and subcontractors are sufficiently trained, qualified and experienced in the skills needed to execute the roles they fulfil. 2. The existence of sufficient staff and subcontractors to adequately	1. The employees of SK and its subcontractors have received adequate training and have all the necessary experience for carrying out the duties specified in the employment contract and job description before they perform any operational or security functions. The more specific procedural and personnel controls are described in SK ID Solutions AS - EID-SK

		operate and resource the service according to its policies and procedures. 3. Facilities used for providing the service are continuously monitored for, and protect against, damage caused by environmental events, unauthorised access and other factors that may impact the security of the service. 4. Facilities used for providing the service ensure that access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors.	Certification Practice Statement *[2]*, clause 5.2 and 5.3. The fulfilment of this requirement is checked during the eIDAS conformity assessment audits and ISO/IEC 27001 certification. 2. The existence of sufficient staff and subcontractors adequately operate and resource the service according to its policies and procedures are checked during the eIDAS conformity assessment audits. SK takes warranty to carry overall responsibility for conformance with the procedures defined in SK ID Solutions AS - SK Trust Services Practice Statement *[11]* (clause 9.6.1) and service-based policies and practices statements. SK gives warranty that SK has the financial stability and resources required. Also SK has a documented agreements and contracts with its subcontracting and outsourcing parties provisioning services. SK has defined in these agreements and contracts the liability, relevant requirements and right to audit subcontracting and outsourcing parties to be ensured that they are bound to implement any requirements and controls required by SK. The fulfilment of this requirement is checked during the eIDAS conformity assessment audits and ISO/IEC 27001 certification.

			3. Facilities used for the service provision are monitored and protected on the necessary security level. The more specific physical controls are described in SK ID Solutions AS - SK Trust Services Practice Statement *[11]*, clause 5.1. The fulfilment of this requirement is checked during the eIDAS conformity assessment audits and ISO/IEC 27001 certification. 4. Logical and organisational access is limited to authorised staff or subcontractors. The more specific description of implemented controls is included into SK ID Solutions AS - SK Trust Services Practice Statement *[11]*, clause 6.5. The fulfilment of this requirement is checked during the eIDAS conformity assessment audits and ISO/IEC 27001 certification.
3.4.6. Technical controls	LOW	1. The existence of proportionate technical controls to manage the risks posed to the security of the services, protecting the confidentiality, integrity and availability of the information processed. 2. Electronic communication channels used to exchange personal or sensitive information are protected against	1. Technical controls to manage risks posed to the security of the services, protecting of the confidentiality, integrity and availability of the information processed are defined and described in the S*K ID Solutions AS - EID-SK Certification Practice Statement [2]* and SK ID Solutions AS - SK Trust Services Practice Statement *[11]*, in both respective under clause 6. Technical controls are defined for key management, computer security controls, life-cycle of technical controls for operations, network security, etc.

		eavesdropping, manipulation and replay. 3. Access to sensitive cryptographic material, if used for issuing electronic identification means and authentication, is restricted to the roles and applications strictly requiring access. It shall be ensured that such material is never persistently stored in plain text. 4. Procedures exist to ensure that security is maintained over time and that there is an ability to respond to changes in risk levels, incidents and security breaches. 5. All media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.	The fulfilment of these requirements is checked during the eIDAS conformity assessment audit and also during ISO/IEC 27001 certification audit. 2. Please refer to p 3.3.1, description under High level. 3. Access to sensitive cryptographic material is allowed only to the trusted administrators under dual control. The administrators are responsible for creating and deleting cryptographic key material which is used for secure encryption of the communication channel, secure encryption of the sensitive data in the database as well as generation of the server-side key shares of the Smart-ID Subscriber. The sensitive cryptographic material in the Smart-ID server is never persistently stored in plain text. For secure storage of sensitive data in database, we are encrypting the data with a symmetric AES key. The key which is used for encryption is, in turn, stored in and protected by the Hardware Security Module (HSM). Additionally, we are using a symmetric key HMAC key for authenticated encryption for encrypting the key material in the database, in order to identify the accidental corruption or malicious changes in the stored data. The sensitive cryptographic material in the

			Smart-ID App (i.e. the App's part of the private key) is stored in encrypted form in the mobile device's secure storage area. The private key is encrypted with the AES key derived from the Subscriber entered PIN code. 4. In the field of security management, SK guides itself by the generally recognised standards, e.g. ISO/IEC 27001 and other industry standards required by regulations and law. SK's security management policy documents include the security controls and operating procedures for SK facilities, systems and information assets providing the services. SK carries out and revises risk assessment regularly in order to evaluate business risks and determine the necessary security requirements and operational procedures. SK management approves risk assessment and accepts the residual risks identified. SK has implemented a business continuity management framework, which covers procedures of risk assessment (including changes in risk levels), incident handling (includes a response to incidents and disasters), recovery and recovery exercises. The procedures for the handling of information security incidents, emergency situations and critical vulnerabilities are documented in SK Internal Crisis Management Regulation. The

			objective of that regulation is the immediate response and recovery of availability and the continuous protection of SK services. The response times to vulnerabilities, security incidents and communication to public authorities (CERT, Data Protection Inspectorate, etc.) is describe in this internal procedure, but also in the public documentation SK ID Solutions AS - SK Trust Services Practice Statement *[11]*, clause 5.7. The fulfilment of these requirements is checked during the eIDAS conformity assessment audit and also during ISO/IEC 27001 certification audit. 5. All media containing production environment software and data, audit, archive, or backup information are stored within SK with appropriate physical and logical access controls designed to limit access to authorised personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic). Media management procedures and backup of records and data to different media types protects against obsolescence and deterioration of media within the period of time that records are required to be retained. Media containing Sensitive Information are securely disposed of when no longer required. All removable media are used only for the intended period of the user (either by time or by number of uses).

			Media containing sensitive information are securely disposed of when no longer required. Paper documents and materials with sensitive information are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Any media with sensitive information removed from use (removable media, hard disks etc.) are sanitised when decommissioned or recycled for other use, to prevent data leaks. The fulfilment of these requirements is checked during the eIDAS conformity assessment audit and also during ISO/IEC 27001 certification audit.
	HIGH (same as SUBSTANTIAL)	Same as level low, plus: Sensitive cryptographic material, if used for issuing electronic identification means and authentication is protected from tampering.	Please refer to p.3.2.1, under High level, point 1.
3.4.7. Compliance and audit	LOW	The existence of periodical internal audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.	N/A
	SUBSTANTIAL	The existence of periodical independent internal or external audits scoped to include all parts	N/A

		relevant to the supply of the provided services to ensure compliance with relevant policy.	
	HIGH	1. The existence of periodical independent external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy. 2. Where a scheme is directly managed by a government body, it is audited in accordance with the national law.	eIDAS conformity assessment and certification of Smart-ID qualified certificates for electronic signature (under trust service EID-SK for issuing qualified certificates of electronic signatures) is performed by accredited certification body (initial conformity assessment by TÜV Informationstechnik GmbH accredited by DAkkS Deutsche Akkreditierungsstelle GmbH, currently valid conformity assessment is carried out by TÜV AUSTRIA CERT GMBH accredited by Akkreditierung Austria) according to the eIDAS regulation, implementation acts, the Electronic Identification and Trust Services for Electronic Transactions Act of Estonia and ETSI relevant standards. For major changes of trust service, for example new identification methods, e.g. certification of change is carried out and appendix to the conformity assessment report and certificate is added. Supervisiory Body have included the qualified service into the Estonian Trusted List. The SK as qualified trust service provider and its qualified services and activities are under supervision, Information System Authority (until 31.12.2018 under Estonian Technical Regulatory Authority). Also SK has achieved ISO/IEC 27001: 2013 certification, the Smart-ID service and parts that

			are relevant to the supply of the service, belongs to the certification scope. 2. N/A

4. References

[1] SK ID Solutions AS - Certificate Policy for Qualified Smart-ID, https://www.skidsolutions.eu/upload/files/SK-CP-QUALIFIED SMART-ID-EN-v7_0-20210512.pdf

[2] SK ID Solutions AS - EID-SK Certification Practice Statement, https://www.skidsolutions.eu/upload/files/SK-CPS-EID-SK-EN-CURRENT.pdf

[3] Terms and Conditions for Use of Certificates of Qualified Smart-ID, https://www.skidsolutions.eu/upload/files/SK-TCU-QUALIFIED-SMART-ID-EN-CURRENT.pdf

[4] Smart-ID certificate for eIDAS compliant QSCD, https://www.tuvit.de/fileadmin/Content/TUV_IT/zertifikate/de/9801UE_s.pdf

[5] Smart-ID SecureZone Common Criteria certificate, https://www.tuvit.de/fileadmin/Content/TUV_IT/zertifikate/en/9263UE_s.pdf

[6] Smart-ID SecureZone Common Criteria certification report, https://www.tuvit.de/fileadmin/Content/TUV_IT/zertifikate/de/9263BE_s.pdf

[7] Smart-ID technical overview, https://github.com/SK-EID/smart-id-documentation/wiki/Technical-overview

[8] Common Criteria for Information Technology Security Evaluation Part 3, Version 3.1 Revision 5, https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

[9] Smart-ID SecureZone Security Target, version 2.7.0, https://github.com/SK-EID/smart-id-documentation/blob/master/files/Smart_ID_SecureZone_Security_Target.pdf

[10] Smart-ID RP API documentation, https://github.com/SK-EID/smart-id-documentation/blob/master/README.md

[11] SK ID Solutions AS - SK Trust Services Practice Statement, available at https://www.sk.ee/en/repository/sk-ps/

[12] eIDAS certificate for creation EID-SK qualified e-signature certificates, https://www.sk.ee/en/repository/audit/

[13] ISO/IEC 27001: 2013 certificate, https://www.sk.ee/en/repository/audit/

[14] 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910

[15] Electronic Identification and Trust Services for Electronic Transactions Act, RT I, 25.10.2016, 1, https://www.riigiteataja.ee/en/eli/511012019010/consolide

[16] GDPR - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

[17] ETSI EN 319 401 General Policy Requirements for Trust Service Providers, https://www.etsi.org

[18] ETSI EN 319 411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements, https://www.etsi.org

[19] ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, https://www.etsi.org

[20] ISO/IEC 27001: 2013 Information technology. Security techniques. Information security management systems

[21] Consent to process personal data via Automated Biometric Identity Verification, https://www.skidsolutions.eu/en/repository/data-protection/

[22] Audit Reports. Information contained in the conformity assessment reports is intended for internal use only. Public information about conformity assessments (including ABIV) is available eIDAS certificate for creation EID-SK qualified e-signature certificates, published at SK repository: https://www.skidsolutions.eu/en/repository/audit/

[23] SK ID Solutions AS - Requirements of Identity Validation for RA, https://www.skidsolutions.eu/en/repository/requirements-by-sk/requirements-of-identity-validation-RA/

[24] Requirements for Secondary Subscriber Authentication Provider, https://www.skidsolutions.eu/en/repository/requirements-by-sk/requirements-for-SSAP/