Requirements of Identity Validation for RA

Version information		
Date	**Version**	**Changes**
19.04.2021	4.2	Requirements of Identity Validation for RA removed from SK ID Solutions AS - EID-Q SK Certification Practice Statement and published as separate requirements document in SK repository.
10.04.2018	4.1	References to the new versions of ETSI standards.
19.11.2017	4.0	Requirements for alternatives for four-eye control was added.
12.10.2017	3.0	Requirements for identity validation for revocation of certificates via Helpline was added.
23.02.2017	2.0	Requirements for identity validation for qualified certificate revocation was added (paragraph 2.).
22.01.2017	1.1	Removed reference to Smart-ID.
15.11.2016	1.0	Initial version.

1 Introduction

The aim of the current document is to describe requirements of identity validation for registration authorities (RA) providing services to SK ID Solutions.

SK ID SOLUTIONS

2 Identity validation requirements for qualified certificate issuance

Name of control	Controls for qualified certificate issuance (with qualified e-signature certificates and authentication certificates conformant to level HIGH)	Source reference	Requirement (from source)
Verification of subscriber by physical presence/or using methods with equivalent assurance	Subscriber shall be verified either: 1. by the physical presence (natural person); 2. authentication using high level electronic identitification means (for which issuance physical presence is necessary) national ID-card, mobile-ID certificates for authentication.	eIDAS regulation, article 24 clause 1 (requirements to trust service provider)	1. When issuing a qualified certificate for a trust service, a qualified trust service provider shall verify, by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate is issued. The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law: (a) by the physical presence of the natural person or of an authorised representative of the legal person; or (b) remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or (c) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or (d) by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.
		ETSI EN 319 411-2, 6.2.2 a/	6.2.2 Initial identity validation

		ETSI 319 411-1,v1.2.1 REG-6.2.2-02	a) [QCP-n] and [QCP-n-qscd] the identity of the natural person and, if applicable, any specific attributes of the person, shall be verified: i) by the physical presence of the natural person; or ii) using methods which provide equivalent assurance in terms of reliability to the physical presence and for which the TSP can prove the equivalence.	
Identity proofing and verification of natural person (distinguishing from other persons)	In case of verification of physical presence: 1. national identity document as evidence of identity and claimed identity shall be checked: 1. validity of national identity document 2. authenticity of national identity document (inspect primary security features) 2. susbscriber 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.	ETSI 319 411-1, 6.2.2 b ETSI 319 411-1,v1.2.1 REG-6.2.2-05	CONDITIONAL] [NCP]: If the subject is a natural person (i.e. physical person as opposed to legal person) evidence of the subject's identity (e.g. name) shall be checked against this natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence. NOTE 2: An example of the required indirect evidence of identity is one or more registration documents electronically signed by a person trusted to have checked the persons' identity in line with the requirements of this clause. Some other examples can be found in annexes B and C of the EVCG [4].	
		Commission implementing regulation (EU) 2015/1502 of 8 September	Level 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.

		2.1.2. Identity proofing and verification (natural person)		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.
			Level 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 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; 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.
			Level 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: 1. 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 2. 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 3. 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 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. 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.
Checking and collecting evidence about attributes to distinguish the person from others with the same name	1. The following data shall be collected: 1. Persons name (the current first and last name) and 2. personal identity code (EE, LV, LT) shall be collected. In case where personal identity code does not contain the date of birth, separately date of birth shall be collected. 2. The personal data (persons name and personal identiy code) from national	ETSI 319 411-1, 6.2.2 c/ ETSI 319 411-1,v1.2.1 REG-6.2.2-06 and REG-6.2.2-07	c) [CONDITIONAL]: If the subject is a natural person (i.e. physical personal as opposed to legal person), evidence shall be provided of: 1) full name (including surname and given names consistent with the national identification practices); and 2) date and place of birth, reference to a nationally recognized identity document, or other attributes which can be used to, as far as possible, distinguish the person from others with the same name. The place of birth should be given in accordance to national or other applicable conventions for registering births.	

	identity document shall match 100% with the name on the application.	Commission implementing regulation (EU) 2015/1502 of 8 September 2.1.1 Application and registration	Requirements same for all levels	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.
Collection of evidence or attestation of subjects identity and attributes	In case of verification of physical presence: 1. RA shall collect copy of national identity document. 2. If the subscribers national identity document is not containing respective personal identification code of EE, LV or LT, then additional evidence of issuance personal identification code shall be presented by subscriber.	ETSI 319 411-1, 6.2.2 a/ ETSI 319 411-1,v1.2.1 REG-6.2.2-02	a) The TSP shall collect either direct evidence or an attestation from an appropriate and authorized source, of the identity (e.g. name) and if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation (in both cases the RA shall validate their authenticity). Verification of the subject's identity shall be at time of registration by appropriate means.	
		ETSI 319 411-1, 6.2.2 l/ ETSI 319 411-1,v1.2.1 REG-6.2.2-18	l) The TSP shall record all the information necessary to verify the subject's identity and if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity.	
Four-eye control	In case of physical presence of subscriber national identity document as evidence of identity and claimed identity of subscriber during four-eye control shall be checked: 1. validity of national identity document	risk assessment	Two persons shall verify the identity of subscriber to minimize the risk of false identity.	

	2. authenticity of national identity document (inspect primary security features) 3. 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. Alternative controls in the case when subscriber cannot be physically present during the four-eye control, can be implemented: 1) 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 application. Also that document copy is copy of genuine identification document. 2) Four-eye control can be replaced by technical control, where person's biometrical data or identity document data are matched with persons or its identity document data from the authorized source (for example population registry, identity document registry etc) and the modification of the input or output data is technically restricted to second employee.		

	In case of electronic authentication using high level electronic identification means (for which issuance physical presence is necessary) national ID-card, mobile-ID certificates for authentication etc, four-eye control is not necessary.		

3 Identity validation requirements for qualified certificate revocation

Name of control	Controls for qualified certificate issuance (with qualified e-signature certificates and authentication certificates conformant to level HIGH)	Source reference	Requirement (from source)
Identity proofing and verification of natural person (distinguishing from other persons)	1. Verification of person in case person has national identity document: 1. national identity document as evidence of identity and claimed identity shall be checked: 1. validity of national identity document 2. authenticity of national identity document (inspect primary security features) 2. 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.	ETSI 319 411-1, 6.2.4	The TSP shall revoke certificates in a timely manner based on authorized and validated certificate revocation requests.

	2. Verification of person in case person has no national identity documents (lost, stolen etc) 1. persons identity is verified and claimed identity compared using historical data (in information system) about persons identity and physical characteristics. 3. verification of person if revocation is requested from Helpline 1. person has to present at least the following data: 1. Persons name (the current first and last name); 2. personal identity code (EE, LV, LT) or the date of birth; 3. if present contact information known to RA (address, phone number or an e-mail address); 4. in the case of suspicion the persons identity is verified and claimed identity compared using historical data (in information system) about persons identity or his/her transactions that is known to RA.		

Collection of evidence or attestation of subjects identity and attributes	1. In case of verification of person with national identity document: 1. RA shall collect copy of national identity document. 2. In case of verification of person with historical identity data: 1. evidence that such check took place and by whom, that for verification and identity comparison historical data was used and reference to data set which was used to verify and comparison of identity. 3. in case of verification of persons identity via Helpline: 1. RA shall maintain the call records according to the agreement.	ETSI 319 411-1, 6.2.2 a	a) The TSP shall collect either direct evidence or an attestation from an appropriate and authorized source, of the identity (e.g. name) and if applicable, any specific attributes of subjects to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation (in both cases the RA shall validate their authenticity). Verification of the subject's identity shall be at time of registration by appropriate means.
		ETSI 319 411-1, 6.2.2 l	l) The TSP shall record all the information necessary to verify the subject's identity and if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity.