Requirements to Secondary Subscriber Authentication Providers

Version information		
Valid from	**Version**	**Changes**
19.04.2021	1.0	Initial version

1 Introduction

The aim of the current document is to describe requirements for Secondary Subscriber Authentication and its providers as mandated in SK ID Solutions AS - EID-Q SK Certification Practice Statement (https://www.skidsolutions.eu/en/repository/CPS/).

2 Terminology and abbreviations

Term	Definitions
Authoritative source	Source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity.
eIDAS	Regulation (EU) No 910/2014 [8] 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.
Electronic identification means	A material and/or immaterial unit containing person identification data and which is used for authentication for an online service in a context of this document when its necessary, it can be interpreted as electronic identification channel.
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).
Secondary Subscriber Authentication	A process that ensures Subscriber awareness about on-going 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 means. Secondary Subscriber Authentication provides definite and integral connection to information stating creation of a new Smart-ID account for Subscriber.

Term	Definitions
Secondary Subscriber Authentication Provider	An organisation, which facilitates or performs Secondary Subscriber Authentication during enrollment 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 Service Providers.
SK	SK ID Solutions AS
Subscriber	A natural person to whom the certificates are issued.

3 Organisational reliability and compliance

	Requirement
3.1.	The Secondary Subscriber Authentication Provider shall be reliable: • it is following all requirements stipulated in this Contract annex; • it has concluded and follows Code of Conduct of SK.
3.2.	The Secondary Subscriber Authentication Provider is responsible for the subcontractors activity and shall have a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.
3.3.	The Secondary Subscriber Authentication Provider is data controller according to GDPR regarding contact data.
3.4.	The Secondary Subscriber Authentication Provider is compliant to GDPR requirements.

4 Requirements for delivering authentication messages

Applicable only to Secondary Subscriber Authentication Provider delivering authentication messages.

4.1 Contact data enrollment and renewal, modification and replacement

	Requirement
4.1.1.	Secondary Subscriber Authentication Provider has verified Subscriber in either following ways during contact data enrollment: 1) face-to-face physically or equally comparable and accepted procedure (e.g video identification for anti-money laundering (AML) or know-your-customer (KYC) processes, remote onboarding according to eIDAS art 24 point 1 d) based on comparison of one or more physical characteristics of the Subscriber according to valid authoritative source (as for example national identity documents); 2) by Electronic Identification mean which is issued to the customer using face-to-face identity verification method comparable to Electronic identification scheme under which electronic identification means are issued conforms to the assurance level substantial or high.
4.1.2.	The Secondary Subscriber Authentication Provider has enrolled sufficient identity data to identify unique person, at least: • persons surname(s) and given name(s); • unique identificator: national level personal identity number or identity card number or passport number.
4.1.3.	The Secondary Subscriber Authentication Provider has collected Subscriber's contact data, either • e-mail address or • mobile phone number or • persons's physical address.
4.1.4.	The Secondary Subscriber Authentication Provider has enrolled contact data of contact data subject based on his/her consent in written or in other way reproducable form as on the paper or electronically signed application or person has consented in information system to which person has authenticated with its electronic identification mean. The Secondary Subscriber Authentication Provider ensures that the Subscriber is aware of the current terms and conditions related to the use of the contact data.
4.1.5.	The Secondary Subscriber Authentication Provider has used enrolled contact data at least once for own legal proceedings or transactions and The Secondary Subscriber Authentication Provider depends on contact data quality.
4.1.6.	Contact data shall be refreshed at least once in three years and evidences as audit logs, signed applications etc about consent of contact data subject and contact data enrollment or renewal, modification and replacement must be maintained and presented if needed to SK.
4.1.7.	Contact data renewal, modification or replacement needs to meet the same requirements as for initial contact data enrollment.

	Requirement
4.1.8.	The Electronic Identification means in clause 4.1.1. shall be: 1) compliant to best security practices and it utilises at least on two factor authentication factors from different categories; 2) designed so that it can be assumed to be used only if under the control or possession of the person to whom it belongs.

4.2 Requirements for secure channel and OTP for delivering authentication messages

	Requirement
4.2.1	The Secondary Subscriber Authentication Provider is able during Subscriber onboarding process to send message through personalized channel (SMS, App push, e-mail, etc.) to Subscriber about the transaction context and forward one-time password request calculated and initiated by SK.
4.2.2	Electronic communication channels used to exchange one-time password requests and information processed are protected according to requirements stipulated in this document, clause 6.4.

5 Requirements for performing Secondary Subscriber Authentication with electronic identification means

Applicable only to Secondary Subscriber Authentication Provider performing authentication.

	Requirement
5.1.	The Secondary Subscriber Authentication is performed by Secondary Subscriber Authentication Provider ~~who's~~ with electronic identification scheme complies with one of the following requirements: • Electronic identification scheme under which electronic identification means are issued has been notified according to the eIDAS Article 9(1) or evaluated by member state on the assurance level substantial or high. Evaluation of electronic identification scheme must be publicly available; • Electronic identification scheme under which electronic identification means are issued conforms to the assurance level substantial or high. Evaluation of electronic identification scheme is performed by SK or third party assessment body; • Electronic identification scheme under which electronic identification means are issued has already granted by SK status of Identity Provider according to SK Requirements for Identity Provider (https://www.skidsolutions.eu/en/repository/requirements-by-sk/requirements-for-identity-providers/). Secondary Subscriber Authentication Provider can carry out authentication only with identity mean that is accepted by SK. SK has given acceptance for the authentication based on concrete electronic identification scheme before the Secondary Subscriber Authentication Provider can start Seconday Subscriber Authentication.
5.2.	Subscriber awareness about on-going Smart-ID registration will be verified by authentication process, which has connection to information stating creation of a new Smart-ID account for Subscriber. The information displayed during authentication process to Subscriber shall be approved and verified by SK before Secondary Subscriber Authentication Provider can start with Secondary Subscriber Authentication.
5.3.	Secondary Subscriber Authentication Provider ensures that identity mean used for authentication is valid at the time of issuance of Smart-ID.
5.4.	Secondary Subscriber Authentication Provider ensures and records the response about the success of authentication, authentication time, name, personal identification number or other unique identifier (national identity document number) of authenticated person and information about identification mean as the name of identification mean what was used, identifier of the identification mean and autentication session's UID.

6 General security requirements

6.1 Information security management

	Requirement
6.1.1.	There is an effective information security management system for the management and control of information security risks.

	Requirement
6.1.2.	The information security management system adheres to proven standards or principles for the management and control of information security risks.

6.2 Record keeping

	Requirement
6.2.1.	Recording and maintenance of relevant information is made using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention.
6.2.2.	Retain records, as far as it is permitted by national law or other national administrative arrangement, but not less than 3 years.

6.3 Facilities and staff

	Requirement
6.3.1.	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 fulfill.
6.3.2.	Facilities used for providing the service are continuously monitored for, and protect against, unauthorised access and other factors that may impact the security of the service.
6.3.3.	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.

6.4 Technical controls

	Requirement
6.4.1.	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.
6.4.2.	Electronic communication channels used to exchange personal or sensitive information are protected against manipulation according to best security practices.
6.4.3.	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.
6.4.4.	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.

	Requirement
6.4.5.	All media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.
6.4.6.	Sensitive cryptographic material, if used for issuing electronic identification means and authentication is protected from tampering.

6.5 Compliance and audit

Applicable only to Secondary Subscriber Authentication Provider delivering authentication messages.

	Requirement
6.5.1.	The existence of periodical independent internal or external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy and requirements described in the current document (*explanation: financial audits do not cover the audit object*). Audits according to this requirement has to carried out at least over 3 years. In separate agreement with SK, SK may perform above-mentioned audit.
6.5.2.	SK right to ask and see above-mentioned audit reports.
6.5.3.	SK right to control/audit service on the request within reasonable time.