FILE NUMBER: 2022-0941
CLASSIFICATION ID: 3.2.3

The Trust Framework

for Swedish E-Identification

Version 2022-10-04

1. Background and purpose

The Trust Framework for Swedish E-Identification aims to establish common requirements for issuers of electronic IDs reviewed and approved by the Swedish Agency for Digital Government (DIGG). The requirements are divided into different levels of protection – known as assurance levels – which correspond to different degrees of technical and operational security on the part of the issuer and different degrees of verification that the person to whom an electronic identification document is issued is indeed who he or she purports to be.

The requirements of this trust framework apply to assurance levels 2 to 4, with level 4 corresponding to the highest level of protection.

Compliance shall be interpreted in the following way:

(a) where the assurance level is not specified, the requirement shall be met at all levels, and

(b) where the assurance level is specified, compliance shall be ensured at least at the relevant level.

Requirements set for a lower level than the relevant one shall be disregarded.

2. Organisation and governance

Overall operational requirements

K2.1 Issuers of Swedish eIDs that are not public bodies shall operate as registered legal entities and take out and maintain the insurance required for the business.

K2.2 Issuers of Swedish eIDs must have an established business, be fully operational in all parts specified in this document, and be well versed in the legal requirements placed on them as issuers of Swedish eIDs.

K2.3 Issuers of Swedish eIDs must have the capacity to bear the risk of liability for damages and possess sufficient financial resources to conduct their operations for at least one year.

Information security

K2.4 Issuers of Swedish eIDs shall have established an information security management system (ISMS) for the parts of their activities affected by the trust framework, which is based, where applicable, on ISO/IEC 27001 or equivalent principles for the management and control of information security work, including the following:

(a) All safety-critical administrative and technical processes must be documented and based on a formal foundation, where roles, responsibilities and powers are clearly defined.

(b) Issuers of Swedish eIDs shall ensure that they have sufficient human resources at all times to fulfil their obligations.

(c) Issuers of Swedish eIDs shall establish a risk management process that, in an appropriate manner, continuously or at least every 12 months, analyses threats and vulnerabilities in the business, and that, through the introduction of security measures, balances the risks to acceptable levels.

(d) Issuers of Swedish eIDs shall establish an incident management process that systematically ensures the quality of the service, forms of onward reporting, and that appropriate reactive and preventive measures are taken to mitigate or prevent damage resulting from such events.

(e) Issuers of Swedish eIDs shall establish and regularly test a continuity plan that meets the accessibility requirements of the business through an ability to restore critical processes in the event of a crisis or serious incidents.

(f) Issuers of Swedish eIDs shall regularly evaluate the information security work and introduce improvement measures in the management system.

K2.5 Scope and maturity of the management system:

Level 4: The information security management system shall comply with SS-ISO/IEC 27001:2017 or equivalent subsequent or international versions of the standard, and within the scope of this include all requirements imposed on Issuers of Swedish eIDs.

Subcontracting conditions

K2.6 An Issuer of Swedish eIDs who has outsourced the performance of one or more security-critical processes to another party shall define by contract which critical processes the subcontractor is responsible for and which requirements are applicable to these, and clarify the contractual relationship in the issuer declaration.

Traceability, deletion and storage of documents

K2.7 Issuers of Swedish eIDs shall store:

(a) application documents and documents relating to the issuing, receiving or blocking of eIDs;

(b) contracts, policy documents and issuer declarations; and

(c) processing history and other such documentation as is required to prove compliance with the requirements imposed on Issuers of Swedish eIDs and which enables follow-up that demonstrates that the security-critical processes and controls are in place and effective.

K2.8 The storage period shall not be less than five years and material shall be capable of being produced in a legible form throughout this period, unless a requirement for deletion is necessitated from the point of view of privacy and is supported by law or other regulation.

Review and follow-up

K2.9 Issuers of Swedish eIDs shall establish an internal audit function that periodically reviews the issuing activities. The internal auditor shall be independent in the performance of his or her duties in a manner that ensures objective and impartial review and shall have the competence and experience required for the performance of his or her duties. The internal auditor shall independently plan the conduct of the audit and document this in an audit plan covering a period of three years. Audit elements shall be selected on the basis of a risk and materiality analysis and shall be based on the descriptions of operations submitted by the Issuer to the Agency for Digital Government.

Levels 3 and 4: Internal auditing shall be carried out on the basis of accepted auditing standards.

3. Physical, administrative and person-oriented security

K3.1 The central parts of the operation shall be physically protected against damage as a result of environmental events, unauthorised access or other external disturbances. Access control shall be applied in such a way that access to sensitive areas is restricted to authorised personnel, information-carrying media are stored and disposed of securely, and access to these protected areas is continuously monitored.

K3.2 Before a person assumes any of the roles identified in accordance with K2.4(a), and which are of particular importance for security, the Issuer of Swedish eIDs shall have carried out background checks in order to ensure that the person can be considered reliable and that the person has the qualifications and training required to safely and securely perform the tasks resulting from the role.

K3.3 Issuers shall have procedures in place to ensure that only specifically authorised staff have access to the data collected and retained in accordance with K2.7.

K3.4 **Levels 3 and 4:** Issuers shall ensure throughout the chain of the issuing process that separation of duties is applied in such a way that no single person is able to obtain an eID in the name of another person.

4. Technical security

K4.1 Issuers of Swedish eIDs shall ensure that the technical controls in place are sufficient to achieve the level of protection deemed necessary with regard to the nature, scope and other circumstances of the business, and that these controls function and are effective.

K4.2 Electronic means of communication used in the transmission of sensitive data shall be protected against interception, manipulation and replay.

K4.3 Sensitive cryptographic keying material used to issue eIDs, identify holders and issue identity certificates shall be protected in such a way that:

(a) access is limited, logically and physically, to the roles and applications that are strictly necessary;

(b) the keying material is never stored in plain text on persistent storage media;

(c) the keying material is protected by the use of a cryptographic hardware module with active security mechanisms that counteract both physical and logical attempts to compromise the keying material;

(d) security mechanisms for the protection of keying material are transparent and based on recognised and well-established standards; and

(e) **Levels 3 and 4:** activation data for keying material protection is managed through multi-person control.

K4.4 Issuers shall have documented procedures in place to ensure that the required level of protection in the relevant IT environment can be maintained over time and in connection with changes, including regular vulnerability assessments and appropriate preparedness to meet changing risk levels and incidents that occur.

5. Application, identification and registration

Information on conditions

K5.1 Issuers of Swedish eIDs shall provide information about contracts, terms and conditions, as well as related information and any restrictions on the use of the service, to connected users, e-service providers, and others who may rely on the issuer's service.

K5.2 An Issuer of Swedish eIDs shall clearly refer to the terms and conditions and design the procedures so that the terms and conditions are provided to the applicant in the issuing process.

K5.3 Issuers of Swedish eIDs shall provide an issuer declaration that includes:

(a) the identity and contact details of the issuer;

(b) brief descriptions of the services and solutions provided by the issuer, including applied methods for application, issuing and blocking;

(c) conditions associated with the service provided, including the user's obligations to protect their electronic ID, the issuer's obligations and responsibilities, any guarantees given and promised availability;

(d) information on the processing of personal data and the manner in which it is carried out; and

(e) arrangements for amending the terms or other conditions of the service provided, including the steps to be taken to discontinue the service in a controlled manner.

K5.4 **Levels 3 and 4:** Issuers of Swedish eIDs shall, upon request by the Agency for Digital Government (DIGG) or another contracting party that relies on services provided by the issuer, provide information on how the business is owned and managed.

K5.5 An Issuer of Swedish eIDs who ceases its activities shall follow a pre-established plan for discontinuing the service. The plan shall include informing all users of the service and DIGG. The issuer shall further keep archived material available in accordance with K2.7 and K2.8 after discontinuation.

Application

K5.6 A Swedish eID may only be issued at the request of the applicant or through another equivalent acceptance procedure, and only after the applicant has been made aware of the conditions under which it is issued and the responsibility that will be placed on him or her.

However, the issuing of an eID that replaces or supplements a valid or recently blocked eID document previously issued by the same issuer may take place without any prior application procedure.

K5.7 An application for a Swedish eID shall be linked to a personal identity number or coordination number, as well as the information that is otherwise necessary for the issuer to provide such eID.

Determination of the applicant's identity

K5.8 Issuers of Swedish eIDs must verify that the information linked to the application is complete and corresponds to information registered in an official register.

K5.9 Where information to be checked in an official register is marked as confidential ('protected identity'), the necessary checks may be carried out by other equivalent means.

K5.10 Identification of the applicant during a face-to-face visit:

Issuers of Swedish eIDs may verify the applicant's identity during a face-to-face visit, in the same manner as when issuing a standard identity document.

K5.11 Remote identification of the applicant in the existingrelationship:

Level 3: Issuers of Swedish eIDs who have already identified the applicant in a relationship involving economically or legally significant transactions, and where the applicant can be identified remotely by other reliable means equivalent to the level 3 requirements of the Swedish eID quality mark, may use this method to establish the applicant's identity.

Level 4: Not applicable.

K5.12 Identification through Swedish eID:

An Issuer of Swedish eIDs may identify the applicant remotely by means of an existing valid Swedish eID of at least the same assurance level as the one to be issued, if it can, without contractual obstacles, use such identification as a basis for issuing a new eID.

Level 4: The validity period of the newly issued eID shall be limited to not extending beyond the validity period of the existing eID.

K5.13 Remote identification of the applicant:

Level 2: Issuers of Swedish eIDs may use reliable image recordings of a valid standard identity document and the applicant's facial image as a basis for establishing the applicant's identity remotely if the comparison does not give rise to doubts as to the applicant's true identity.

Level 3: Issuers of Swedish eIDs may, by means of a secure reading of a valid standard identity document containing electronically stored biometric data, establish the applicant's identity remotely on the basis of those data if the corresponding biometric data of the person to be identified can be collected in a sufficiently secure manner so that a comparison can be made with equivalent reliability as in the case of a face-to-face visit, and where the comparison does not give rise to doubts as to the applicant's true identity.

Level 4: Not applicable.

Registration

K5.14 Issuers of Swedish eIDs shall, taking into account the applicable rules on personal data protection, keep a register of connected users and the allocated electronic identification documents, and keep this register up to date.

6. Issuing and blocking of eID

Design of technical means

K6.1 Technical means:

Levels 2 and 3: Technical means for electronic identification through eID with the Swedish eID quality mark shall be designed according to a two-factor principle, whereby one part consists of electronically stored information that the user shall hold, and the other part consists of what the user shall use to activate the eID.

Level 4: Technical means for electronic identification through eID with the Swedish eID quality mark shall be designed according to a two-factor principle, whereby one part consists of a personal security module that the user shall possess, and the other part consists of what the user shall use to activate the security module.

K6.2 The activation mechanism and personalized code shall be designed in such a way that it is unlikely for third parties to breach the protection, even by mechanical means.

Levels 3 and 4: The protection shall include mechanisms to prevent copying and manipulation of the electronic identification document.

K6.3 Users of eID with the Swedish eID quality mark shall be able, on their own initiative, within the period of validity of the eID, free of charge, and without significant inconvenience, to exchange or request a new personal code and, through guidance or automatic production, be helped to maintain the requirements of K6.2.

If the eID is designed in such a way that a personalized code cannot be exchanged, the user should instead, under the same conditions, promptly be able to obtain a new eID with a new personalized code that replaces the previous one via a blocking procedure.

K6.4 Issuers of Swedish eIDs shall ensure that the data registered for electronic identification of holders uniquely represents the applicant and is attributed to the person in question when issuing the eID document.

K6.5 The period of validity of issued eIDs shall be limited taking into account the security features of the eID document and the risks of misuse. The maximum period of validity of the eID shall be five years.

Provision of eID document

K6.6 Remote provision:

Level 2: An Issuer of Swedish eIDs shall provide the e-ID document in a way that confirms contact details kept in the official register or such information recorded in connection with the electronic procedure according to K5.13 Level 2.

Level 3: An Issuer of Swedish eIDs who provides an eID via electronic procedure that is in accordance with K5.11 Level 3, K5.12 Level 3 or K5.13 Level 3 shall, when newly issued, separately and independently from the provision in terms of security, ensure that the user is informed that such e-ID document has been handed over, or by other measures ensure an equivalent degree of control that the person is alerted to the risk of identity theft in connection with the provision.

Level 4: An Issuer of Swedish eIDs that provides an eID via an electronic procedure compliant with K5.12 Level 4 shall, when newly issued, separately and independently from the provision in terms of security, ensure that the user is informed that such eID document has been handed over.

K6.7 Provision during a face-to-face visit:

An Issuer of Swedish eIDs shall, during a face-to-face visit and after an identity check in accordance with K5.10, provide the electronic identification document against signed receipt, and shall further provide the part that the user shall use to activate the eID separately and independently from the provision of the eID document in terms of security, on the basis of contact details kept in an official register or other information of equivalent credibility.

Blocking service

K6.8 Issuers of Swedish eIDs shall provide a blocking service with good accessibility for the user to be able to block their eID.

K6.9 Issuers of Swedish eIDs shall promptly and securely process and effect requests of blocking, and take measures to prevent systematic misuse of the blocking service or other intentional actionsthat lead to the widespread blocking of electronic identification documents, ensuring that users' eIDs are available when needed

7. Verification of holders' electronic identities

K7.1 Issuers of Swedish eIDs shall ensure that, when verifying the identity of the holder, reliable checks are carried out on the authenticity and validity of the eID document.

K7.2 Issuers of Swedish eIDs shall ensure that technical security controls have been implemented when verifying the electronic identities of holders, so that it is unlikely that third parties, through guessing, eavesdropping, replaying or manipulation of the process can breach the protection mechanisms.

8. Issue of identity certificates

Issuers of Swedish eIDs that provide a service for issuing identity certificates to relying e-services shall also comply with the provisions of this Section.

K8.1 Issuers of Swedish eIDs shall ensure that the service for issuing identity certificates has good accessibility and that the issuance of identity certificates is preceded by reliable identification in accordance with the provisions of Section 7.

Level 4: Certificates shall include a reference to cryptographic keying material verified by the issuer as being in the sole possession of the holder.

K8.2 Submitted identity certificates shall be valid only for as long as is necessary to allow the user access to the requested e-service, and be protected so that the information can only be read by the intended recipient and that the authenticity of the certificates can be verified by the recipients of the certificates.

K8.3 Issuers of Swedish eIDs shall, taking into account the risks of misuse of the certification service, limit the period of time within which several consecutive identity certificates may be issued to a particular holder before the holder is re-identified in accordance with the provisions of Section 7.