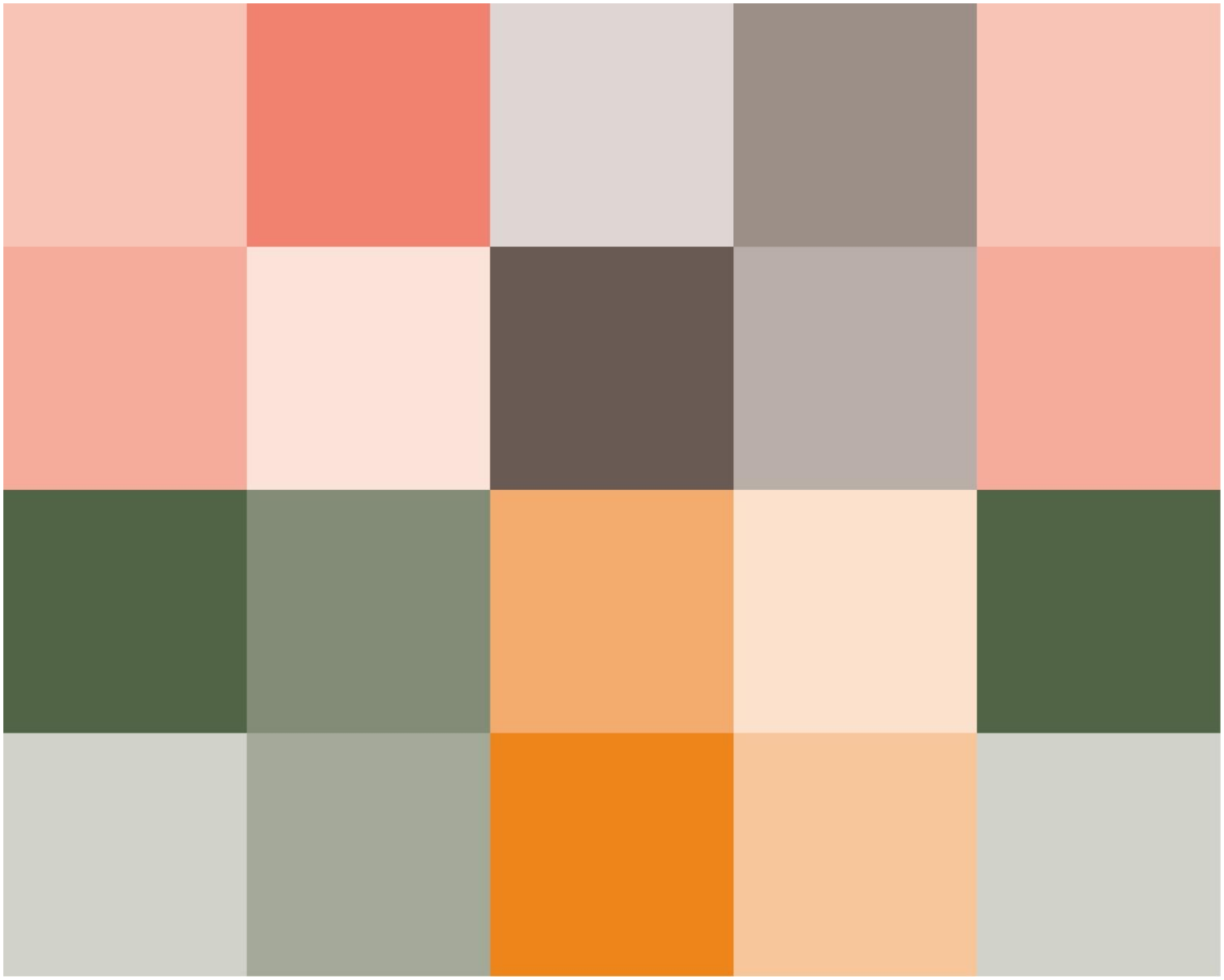

LoA Mapping

The Swedish Trust Framework

2021-01-14

Dnr: 2020-1972

MYNDIGHETEN FÖR
DIGITAL FÖRVALTNING
Agency for Digital Government

Purpose of this document

This document maps the provisions of the Swedish Trust Framework to the requirements of the eIDAS implementing regulation (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of the eIDAS regulation (EU) 910/2014.

Table of contents

1 Introduction

This document provides an overview of how the Swedish Trust Framework meets the requirements of the eIDAS implementing regulation (EU) 2015/1502, and how the provisions of the Swedish Trust Framework are applied to the providers of eID means within the Swedish eID ecosystem.

The document includes the guidance given to providers of eID means in the Swedish Trust Framework. This same guidance is used for the compliance audit of those providers. Finally, a summary of the audit criteria are also included which is used to demonstrate how compliance with each requirement of the Swedish Trust Framework should be verified.

As appendices to the document, each of the current Issuers of eID means' compliance with the requirements is included.

The audit process for Issuers of eID means is described in the "Swedish eID White Paper".

1.1 The Swedish Trust Framework

The Swedish Trust Framework establishes a common set of requirements for Issuers of Swedish eIDs. The requirements are based on international standards and recognised and established principles, and are divided into three different classes, known as assurance levels. The assurance levels each corresponds to different degrees of technical and operational controls of the issuer and the confidence that the identity of a person being assigned an electronic identification means is that of the claimed identity.

The requirements are structured according to a generally accepted model for electronic identification, where the management of the eID means is divided into three different phases:

1. enrolment,
2. credential management and
3. authentication

In each of these phases, certain security measures and controls are required to maintain the specified level of assurance. In addition, there are requirements aimed at the Issuer's management and organisation.

The assurance levels are based on an impact-based model for risk assessment which defines 6 different risk areas. The model's impact levels are divided into *limited*, *moderate*, *substantial* and *high*.

It is the service providers' obligation to select the appropriate assurance level required to access their service based on their risk profile and the potential consequences of an incorrect authentication.

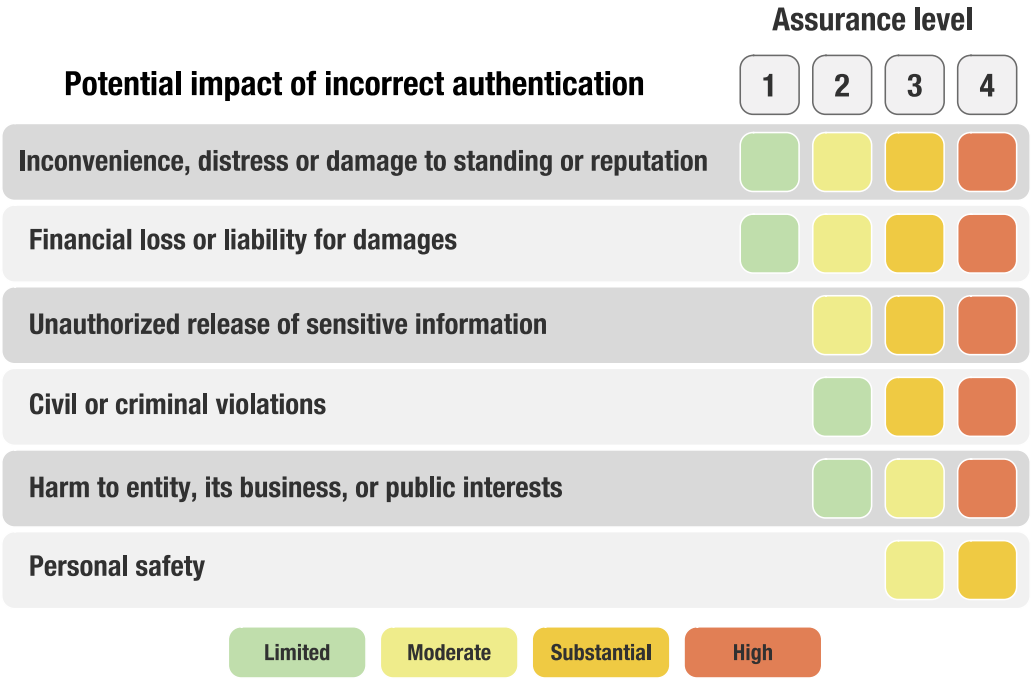

Figure 1

The impact-based risk model sets out a number of areas of risk with a recommended assurance level to use depending on the level of risk in that area.

If an incorrect identification may lead to negative consequences in several areas it is the most severe consequence that determines the level of assurance required. The existence of several risks in different areas is generally not considered to be cumulative.

The impact categories are defined by the Swedish Civil Contingencies Agency (MSB) in the publication *Model for classification of information*[1], however this model only has three impact levels and does not include the level of *limited*. The Swedish Trust Framework introduces this lower level in order to be fully in line with the international definition of assurance levels[2]. For the same reason, there is an assurance level 1 in the model that corresponds to an electronic identification where the user's real identity is not verified. Assurance level 1 is currently not defined in the Swedish Trust Framework.

Currently only assurance level 3 is in wide-spread use. The intention for assurance level 3 is that it should provide an equivalent level of assurance as a traditional photo-identification document, but at the same time allow for such an eID to be issued and provided remotely in an as efficient manner as possible.

For services with lower risk, assurance level 2 can be used. The assurance provided at level 2 roughly corresponds to that of a one-time personal code conveyed via regular mail.

[1] https://rib.msb.se/filer/pdf/25602.pdf
[2] ISO/IEC 29115, section 6.

A two-factor authentication token is still required, but the proofing requirements are less strict.

Assurance level 4 is intended to meet the highest assurance needs. For this level, issuance, delivery and renewal is required to be done in-person, and there are particularly stringent requirements for the issuer's risk management and internal controls. For level 4, only hardware tokens are allowed.

The Swedish assurance levels 2, 3 and 4 each fulfil the requirements of the eIDAS assurance levels low, substantial and high respectively.

2 LoA mapping

2.1 Enrolment

2.1.1 Application and registration

LOW

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.

The provisions of section 2.1.1 paragraph 1 and 2 corresponds to K5.6 of the Swedish Trust Framework:

> K5.6 Swedish eID may be issued only at the request of the applicant, and only after the applicant is made aware of the conditions under which the issuance occurs and what responsibility will lie with the applicant.
>
> Issuance of eID that replace or supplement one of the same issuer's previously provided valid or recently revoked eID, may be made without an application procedure.

The provisions of paragraph 3 correspond to K5.7 of the Swedish Trust Framework:

> K5.7 An application for a Swedish eID shall be associated with a personal identity number or a verified co-ordination number, and all other information otherwise necessary for the issuer to be able to provide the eID.

Applicable guidance

The application procedure may look different depending on whether the application is made remotely or in-person. It is common for the application to take the form of a request from the user to obtain an eID through their on-line banking service. For eIDs issued in-person the applicant may fill out an application form with their personal information which is signed and submitted to the issuer.

The provision of K5.6 aims to ensure that an eID is only issued on the request by the user. The users must be made aware that an eID is provided to them, on what conditions this takes place and what responsibility will rest with the user.

The purpose is to prevent situations where users are automatically assigned an eID, perhaps without the situation being completely clear to the user that this has occurred. Such a situation could arise if the eID included in another service, such as a telephony

subscription, not realising the phone (or SIM card) is also an identity document. It is important that it must be clear to the user if an eID is bundled in this way.

Issuance for the purpose of replacing, for example, a revoked eID, or to provide a new bearer of an eID, is not intended to require such an application procedure, and can be carried out on the issuer's initiative.

Audit criteria

1. Verify that the issuers declaration of practices includes a description of the application procedures.
2. Make a conformance assessment of the application procedure based on provided guidance.
3. Verify that the application procedures described ensure that the terms and conditions associated with the issuing of an eID are provided to the applicant before entering into an agreement (terms of service) with the issuer. Verify that the description includes conditions for changing the conditions.

2.1.2 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.

The provisions of section 2.1.2 maps to several clauses in the Swedish Trust Framework. First, paragraph 3 corresponds to K5.8 and K5.9 of the Swedish Trust Framework:

K5.8 Issuers of Swedish eID shall verify that the information provided in the application is complete and consistent with the personal data registered in an official register.

K5.9 If the information to be verified in an official register is marked confidential (protected identity), the necessary checks may be made using other equivalent means.

Secondly, paragraph 1 and 2 sets out the minimum requirements for identity proofing and verification, which is stated in K5.11 and K6.6 respectively in the Swedish Trust Framework. The principle of the Swedish Trust Framework for level 2 is that the identity evidence is provided to the applicant by the issuer as part of the enrolment process, and subsequently used to setup the eID means. Typically, the issuer of an eID means would

send a one-time code to the registered address of the applicant and the applicant would then use this code to prove their identity.

K5.11 Remote identification of the applicant

Level 2: Issuers of Swedish eID that identifies the applicant remotely,

shall identify the applicant by providing the credentials in accordance with K6.6 Level 2.

K6.6 Providing of credentials remotely

Level 2: An issuer of Swedish eID shall in the process of providing a

level 2 credential confirm the contact details recorded in an official register.

Applicable guidance

As a fundamental requirement for issuing of eIDs on all assurance levels it must be ensured that the personal information on which the issuance is based corresponds to information recorded in an official register. If issuing takes place in an existing relationship (e.g. an employment), where this information has been obtained at an earlier time, the correctness of the information must be verified against an official register at the time of issue. The Swedish population register is the authoritative source for such records. Official registers include SPAR[3], but the corresponding service from e.g. a credit bureau is also considered to meet the requirements.

For issuing and providing eID on the lowest assurance (level 2), a secret (for example a one-time code) or a device that can generate one time codes can be sent by regular mail to the applicants residential address in the population register. This information can then be used by the issuer to confirm the identity of the applicant remotely, a process which corresponds to the provisions of section 2.1.2 (low) paragraph 1 and 2 but also requires the issuer to verify the possession of the confidential information (*verified to be in possession*, as opposed to *assumed*). The confidentiality and security of the postal item is protected through the Swedish Criminal Code (SFS 2010:1045) chapter 4 section 8-9, whereby anyone who unlawfully accesses the content of an item of post may be liable for a fine or imprisonment for up to two years.

In some situations, it may not be practically possible to send a letter to the person's civil registration address. Such situations could arise, for example, when issuing eID to Swedes abroad.

In such cases, alternative contact details may be used provided that the issuance process can be carried out with equivalent trustworthiness. This can be achieved, for example, by obtaining alternative contact information certified by the person's employer or equivalent. For people, either in Sweden or abroad, that have a protected identity, post

[3] https://www.government.se/government-agencies/statens-personadressregister/

can be sent to the Swedish Tax Agency's which forwards them to the person’s real address.

Audit criteria

1. Verify that the registration process involves confirming the personal information provided in the application against an official register.
2. Make an assessment whether the source of personal information meets the requirements of an official register.
3. If the issuer relies on remote identification at level 2, verify that the identity evidence that was issued by the eID provider is based on information from the official register and that the letter is adequately protected as it is being conveyed from the issuer to the applicant.

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.

The provisions of section 2.1.2 (substantial) paragraph 3 correspond to K5.11 (level 3) of the Swedish Trust Framework.

K5.11 Remote identification of the applicant

Level 3: Issuers of Swedish eID who has already identified the applicant in a relationship concerning financially or legally significant transactions, and where the applicant can be identified remotely using other reliable means equivalent to Swedish eID Level 3, may use this method to determine applicant's identity.

Level 4: Not applicable.

The conformity assessment body is the Agency for Digital Government, and the means to provide an equivalent assurance is audited and determined on a case-by-case basis for each Issuer.

The provisions of section 2.1.2 (substantial) paragraph 4 corresponds to K5.12 of the Swedish Trust Framework.

K5.12 Remote identification using Swedish eID

Level 3: An issuer of Swedish eID may, in addition to what was stated in K5.11, also identify the applicant remotely using another Swedish eID of at least assurance level 3, if the issuer is not prevented by contractual clauses to use such identification as the basis for issuing of a new eID.

Level 4: Not applicable.

Remote identification according to K5.12 may only be based upon an approved Swedish eID. This implies that the issuer of that eID must have undergone the audit process successfully and contracted with the agency to receive the trust mark. In the process of issuing an eID based on K5.12, the requirements of K5.8 still applies, implicating that the personal information of the claimed identity still has to be checked against an official register to ensure its correctness.

Applicable guidance

In order to be able to issue eID at level 3 remotely under the provisions of K5.11, it is required that the issuer itself bears a significant legal or financial risk in relationship with the application.

This normally implies that the issuer provides an e-service to the applicant, where the consequences for the issuer in the event of incorrect authentication may lead to significant damage. The possible consequences in the event of incorrect authentication shall correspond to those stated for assurance level 3 in Figure 1.

The provision K5.11 makes it possible for certain issuers of eID means to issue eIDs at level 3 remotely, via e.g. on-line banking service.

Additionally, an issuer who can identify the applicant remotely through another Swedish eID of at least assurance level 3, may issue a new eID based on this authentication provided that there are no contractual arrangements with the issuer of the original eID that would prevent that the original eID to be used for issuing other eIDs, which can be the case for commercial reasons.

The provision also allows an issuer, which otherwise would not be covered by the remote procedures described in K5.11 Level 3, to remotely renew an eID previously issued by the same issuer.

These provisions do not apply at level 4, as identification of the applicant at this level must always take place face to face with an appropriately trained official.

Audit criteria

1. If the issuer relies on the provisions of K5.11 for remote identification on level 3, make an assessment of the relationship between the applicant and the issuer, the potential impact an incorrect authentication could have on the issuer and that this impact corresponds to those of assurance level 3 in the risk model.
2. If the issuer relies on the provisions of K5.12 for remote identification on level 3, verify that those in use have been certified by the Agency for Digital Government.

HIGH

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

(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 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

HIGH

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.

Remote issuance is not allowed for Swedish eID on assurance level 4, for which reason section 2.1.2 (high) paragraph 1 (b) and (c) is not applicable.

For Swedish eID, the provisions of section 2.1.2 (high) paragraph 2 are also not applicable for an issuer. The applicant will have to resort to obtaining an Adequate ID Document before being able to receive an eID. It is, however, possible for an issuer of such Adequate ID Documents to also issue eID in the same process, but in that case paragraph 1(a) is applied at the time of delivery of the eID means, which corresponds to K5.10 of the Swedish Trust Framework. These provisions also correspond to section 2.1.2 (high) paragraph 1(a).

K5.10 In-person identification of the applicant

Issuers of Swedish eID shall verify the applicant's identity in person, in an equivalent manner as for the issuance of an Adequate ID document.

Applicable guidance

The requirement for in-person identification is the same as when issuing an Adequate ID document, meaning the identification is carried out with the support of a documented process and by specially trained personnel. It is also expected that the identity check in connection with the issuance of the eID is based on the applicant already possessing an Adequate ID document through which the applicant can prove his identity. The valid Adequate ID documents include the Swedish driving license, the Swedish passport, a certified ID card, the national ID card and the Swedish Tax Agency's ID card[4].

The various provisions that apply to the issuance of ID cards to persons who do not possess an Adequate ID document do not apply to the issuance of eID. If they do not have an Adequate ID Document the applicant must obtain one before an eID can be issued.

In this context, it should also be noted in particular that the identification check that is expected to follow when handing out a registered mail is not considered to meet the requirements for in-person identification.

Identification by registered mail can, however, be used as part of a remote identification procedure as referred to in K5.11 level 3, where the registered mail is combined with additional checks to ensure the trustworthiness of the identification.

[4] More information on Adequate ID documents are provided in the White Paper.

Audit criteria

1. If the issuer relies on the provisions of K5.10 for in-person identification on any level, verify that the identity check is carried out by appointed and trained personnel based on established procedures.
2. Verify that only Adequate ID documents are accepted as proof of identity for in-person identity proofing.

2.1.3 Identity proofing and verification (legal person)

Not applicable.

2.1.4 Binding between the electronic identification means of natural and legal persons.

Not applicable.

2.2 Electronic identification means management

2.2.1 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.

The provisions of section 2.2.1 (low) paragraph 1 and 2 corresponds to K6.1 of the Swedish Trust Framework:

K6.1 Technical requirements for credentials

Level 2 and 3: Credentials for electronic identification must always include a second factor, where one part consists of a token of electronically stored information that the user shall demonstrate control of, and the other is a personal code which the user shall demonstrate knowledge of to activate the token

Level 4: Credentials for electronic identification by Swedish eID of level 4 must always include a second factor, where one part consists of a personal security (hardware) module token that the user shall be able to demonstrate control of, and the other is a personal code which the user should demonstrate knowledge of to activate the token.

K6.2 The activation mechanism and personal code shall be designed so that it is unlikely that an outsider is able to compromise the security function.

Levels 3 and 4: The security function must include mechanisms that prevent the duplication of the eID.

Applicable guidance

There are three main categories of authentication factors; knowledge-based factors ("something you know"), inherent-based factors ("something you are") or possession-based factors ("something you have"). For all assurance levels of Swedish eID, multi-factor authentication is required. The baseline is that a personal code is combined with possession of (physical control over) a stored data structure. However, solutions other than a personal code for activation are acceptable if the eID issuer can demonstrate that the level of security of their solution remains equivalent.

Knowledge-based factors

The term personal code refers to a knowledge-based authentication factor, such as passwords, passphrases, combinations of numbers or any other information such that it is not linked to any particular device, medium or software. This implies that the holder of this information uses it to prove a claimed identity through "something you know".

The provisions of K6.2 implies that the complexity requirements of the personal code must be designed so that the resources required to compromise it are in proportion to the other security features of the eID, meaning that this should not be a weaker link in the chain of security controls.

This can be achieved in several different ways, for example:

1. In cases where a personal (hardware) security module is used, ensure it is blocked and rendered unusable after a certain number of incorrect activation attempts, where the number of permitted attempts is in proportion to the complexity of the activation code. For example, the number of incorrect attempts permitted for a 6 digit PIN is less than that for a 10 digit PIN.
2. In cases where two-factor solutions other than a personal security module are used:
   (a) The complexity of the personal code means that an exhaustive search for the correct code can be assumed to require disproportionate effort.
   (b) The activation of the eID using the correct personal code requires significant computational effort, i.e. that the number of cryptographic operations needed to validate whether the correct code has been entered is sufficiently large to require significant computational effort to make it an impractical attack, which further strengthens the protection of the private key material.
   (c) A part of the activation procedure is done on-line with the issuer, which enables the issuer to block the eID after a certain number of incorrect attempts.

The resulting strength in the activation mechanism using a personal code shall also correspond to the validity period of the eID, so that it is unlikely that an adversary will provide the necessary resources to compromise the activation mechanism within the validity period of the eID.

Possession-based factors

A token of electronically stored information refers to a possession-based factor which holds a data structure used to prove control over the device in which this data is stored, i.e. "something you have". The provided proof of possession of the token is required to be based strong cryptographic mechanisms, to ensure that an authentication cannot be forged. Generally, this type of authentication factor cannot be used as the sole authentication factor due to the risk of sudden loss of control over it, but must be combined with an inherent or knowledge-based factor, or both.

Inherent-based factors

An inherent-based authentication factor implies capturing some biometric property of the eID holder and using this as a proof of the claimed identity. A biometric property should never be considered a secret since traces of it is dispersed continuously in our everyday life and the biometric properties cannot be changed.

The fundamental authentication function for biometrics is the ability to capture a biometric property from a living person through a sensor that is in direct contact with the person in question, and where this sensor is sufficiently secure and reliable both in capturing the biometric property and in determining whether the captured property is genuine (that is, it originates from a human being). Due to this and current limitations of biometric sensors in consumer devices, inherent-based authentication factors may not be used for identification of persons remotely, but may be used as an alternative or complement to an activation code.

SUBSTANTIAL

1. The electronic identification means utilises at least two authentication factors from different categories.

1. 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.

The provisions of section 2.2.1 (substantial) paragraph 1 is a requirement for assurance level 2 in the Swedish Trust Framework, and was described in the previous section.

The provisions of section 2.2.1 (substantial) paragraph 2 corresponds to the provisions of K6.1 for level 3 and 4 in the Swedish Trust Framework as explained previously in this section.

Applicable guidance

Swedish eID that meet the requirements for assurance level 3 which are not based on a personal security module of the kind mentioned earlier must implement protection from duplication to further make it more difficult for adversaries to compromise the private key material. This can be accomplished by including information from the environment in which the token is stored, such as data associated with the hardware, as part of the underlying activation mechanism. In addition to this, one can also use operating system features that prevent foreign processes from reading the encrypted key material.

In the evaluation of a particular technical design if it meets the requirements of the trust framework, an overall assessment must be made, where all of the above-mentioned aspects are taken into account and weighed against the threats that exist at the respective assurance level.

HIGH

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.

The provisions of section 2.2.1 (high) paragraph 1 and 2 corresponds to the provisions of K6.1 and K6.2 for assurance level 4 in the Swedish Trust Framework.

For assurance level 4, a personal physical security module must be used as the holder of the key material. Such a device protects the confidential key material from both logical and physical compromise. These types of devices include smart cards, but the corresponding functionality can be integrated into, for example, smart phones, watches and wearables. The personal security module stores the key material and performs the cryptographic operations in such a way that the critical key parameters never leave the security module. It is appropriate that such devices have a well-recognised certification for example Common Criteria (ISO/IEC15408) against an appropriate protection profile.

Audit criteria

1. Evaluate the design of the eID means to establish that its multi-factor properties comply with the requirements of the trust framework at the designated assurance level.
2. Evaluate the activation mechanism to determine whether it provides adequate resistance to unauthorised activation attempts.
3. For tokens not based on hardware, make an overall assessment of the protection mechanisms of confidential key material to determine if it meets the requirements of the trust framework, taking into account the threats that exist at the respective assurance level.

2.2.2 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.

The provisions of section 2.2.2 (low) corresponds to K6.6 for assurance level 2 of the Swedish Trust Framework as described in section 2.1.2 (low). Issuance, delivery and activation may take place in the same channel as the application has been identified through. This way, the eID can be assumed to reach only the intended person.

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.

The provisions of section 2.2.2 (substantial) correspond to K6.6 for assurance level 3 of the Swedish Trust Framework. It should also be pointed out that K6.7 may also be used, which is described in the next section.

K6.6 Providing of credentials remotely

Level 3: An issuer of Swedish eID who has identified the applicant using an electronic procedure in accordance with K5.11 Level 3 or K5.12 Level 3 shall use this channel for providing of the credentials, and shall separately and independently from the providing of the credentials, ensure that the user is informed that such eID have been issued, or by other means ensure the corresponding degree of control that the subject is made aware where there is a risk for identity theft in connection with the providing of the credentials.

Level 4: not applicable.

The provisions of K6.6 for level 3 states that if both the eID and the activation code is provided through the same channel, there should be a notification sent to the person who has applied for the eID.

Applicable guidance

A fully automated remote issuance procedure often means that both the eID and the personal code are provided at the same time. In such cases a notification that the issuance of an eID has taken place must be sent via an alternative communications channel to the individual. It aims to provide a better chance in detecting and reacting on attempts of identity theft, enabling the individual to quickly take measures to limit any harmful effects of such an event.

For example, a traditional letter sent from the issuer to the address from the civil register for the subject would meet the requirements of this provision. However, in some situations this may not be practical. This could arise, for example, when issuing of eIDs to Swedes abroad or to individuals with protected identities, where there is no civil registration address available to the issuer, or persons with particular occupations that requires them to stay elsewhere for long periods of time.

In these cases alternative contact details may be used provided that the issuance process as a whole can be carried out with an equivalent level of security. This can be achieved, for example, by using other contact information obtained at an earlier time or by obtaining contact information which can be certified by the person's employer or equivalent trustworthy authority. It is then assumed that the collection and verification of such information takes place in a way that implies that there is no security dependence on any individual persons within the issuing organisation or the registration office at the time of issue. For persons with a protected identity, confirmations can be conveyed to the person via the Swedish Tax Agency's postal service, both in Sweden and abroad.

It is also possible to send confirmations electronically, which can often be an advantage as they reach the individual more quickly and may provide a higher level of security than a traditional mailbox. It is then required that this alternative electronic channel is based on information that has been registered and verified independently of the recently issued eID. It is fundamental that this communication channel does not have a security dependency on the eID that was provided. It must therefore not be possible to take control of or change the alternative communication channel at the time of the providing of the eID. Although it may possible to update such contact information using the eID provided, the issuer can ensure that the electronic confirmation is also sent to the contact information that was registered a certain time before the issuance. In this way, it is reasonably ensured that the confirmation reaches the person in question, even if a fraudster at the time of notification tries to manipulate the alternative communication channel. It is also assumed that the alternative communication channel is verified in some way, so that it is reasonably ensured that the recipient can receive information transmitted this way, for example by using this channel regularly also for other purposes of significant importance.

It should be noted that providing an activation code or similar, instead of a notification, through the separate channel also complies with these provisions.

HIGH

The activation process verifies that the electronic identification means was delivered only into the possession of the person to whom it belongs.

The provisions of section 2.2.2 (high) correspond to K6.7 of the Swedish Trust Framework, which is applicable on all assurance levels

K6.7 Providing of credentials in-person

An issuer of Swedish eID shall, in-person and upon completion of identity verification in accordance with K5.10, provide the credential while obtaining a signed acknowledgement of receipt, and shall furthermore provide the personal code which the user should use to activate the token, separately and security-independently from the token and based on the contact details recorded in the official register or other information of the same degree of credibility.

Applicable guidance

Methods for delivery and activation which involves two separate channels enables several security-enhancing controls. By basing part of the activation procedure on information that is provided independently of the registration function, and which cannot be changed or controlled by any single person in this function, the security dependence on individuals within the registration function is reduced. The purpose is to primarily alleviate:

1. personnel-related risks in the registration function, where a dishonest person or a person under threat or for other reasons tries to obtain an eID in another individual's name, and
2. risks arising from deficiencies in the identification of the applicant; for example, through the use of forged ID documents or by look-alikes.

It is therefore fundamental not to base the entire delivery and activation process on the same communication channel or to depend on a single person in the registration function. If, for example, the delivery of the eID is done in-person, while the activation and personal code is sent using a traditional letter directly from the issuing function to the civil registration address of the eID holder, the activation procedure is completely separate from and independent of the registration function.

If registration offices or other delivery points are used for in-person delivery of both the eID and the activation credentials, the requirement for delivery and activation through two separate channels can be also achieved through a segregation of duties.

Audit criteria

1. Test the procedures for issuance, delivery and activation to verify that credentials are provided in compliance with the provisions of the trust framework.
2. If the issuer relies on information retrieved from other sources than an official register, evaluate if the information from this source has an equivalent degree of credibility.
3. If notifications are sent as part of the issuing process, verify that neither the applicant nor personnel acting in the registration function is able to divert such notifications at the time of issue.

2.2.3 Suspension, revocation and reactivation

LOW

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 requirements as established before the suspension or revocation continue to be met.

The provisions of section 2.2.3 (low) correspond to K6.8 and K6.9 of the Swedish Trust Framework:

K6.8 Issuers of Swedish eID shall provide a revocation service with adequate availability where the user can request revocation of the eID.

K6.9 Issuers of Swedish eID shall promptly and in a secure manner process and effectuate the revocation request, and take measures to prevent systematic abuse of the revocation service, or other such deliberate actions, that may lead to extensive blocking of issued eID, so that users' electronic identities are available when needed.

Applicable guidance

Issuers of eID means must provide a revocation service where the user can request revocation of the eID 24 hours a day, seven days a week. The revocation service must be protected against abuse, so that it is reasonably ensured that the person requesting the revocation is authorised to do se. Identification of the person requesting the revocation can be done, for example, by confirmation through previously provided mobile phone number (SMS) or by e-mail. A revocation request must be processed and effectuated without undue delay.

To ensure that users can revoke their eID when required, issuers must also be adequately prepared to handle denial of service attacks in the parts related to the revocation service.

Audit criteria

1. Make an assessment of the revocation methods and the service levels of the issuers' revocation service, to determine that it has an adequate availability to users.
2. Verify the measures taken by the issuer to prevent systematic abuse of the revocation service.

2.2.4 Renewal and replacement

LOW

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.

HIGH

Where renewal or replacement is based on a valid electronic identification means, the identity data is verified with an authoritative source.

The Swedish Trust Framework requires that any renewal or replacement of an eID must follow the same procedures as initial issuance. Hence, there are no separate provisions for renewal or replacement.

2.3 Authentication

2.3.1 Authentication mechanism

Provisions for the authentication phase is stated in chapter 7 and 8 in the Swedish Trust Framework. Chapter 7 deals with the requirements for the authentication protocol used between the holder and the verifier, when verifying the authenticity and validity of the eID presented.

The scope of chapter 8 of the Swedish Trust Framework concerns situations where there is an Identity Provider (IdP) function which provides authentication services (assertions) to relying parties within an identity federation.

For authentication services provided for cross-border use, both sections apply.

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 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.

The provisions of section 2.3.1 (low) paragraph 1 correspond to K7.1 of the Swedish Trust Framework.

K7.1 Issuers of Swedish eID shall ensure that during the authentication phase, reliable checks are made of the authenticity and validity of the eID.

The provisions of section 2.3.1 (low) paragraph 2 are covered by K4.1 which mandate that the eID issuer shall have introduced sufficient and appropriate technical controls to protect the to the integrity, confidentiality, availability and accountability of the issuers' systems, and the information being processed in those systems must protect person identification data using all reasonable means available to the issuer. In particular, confidential cryptographic key material used by the issuer in the authentication process must be protected using hardware security modules.

The provisions of section 2.3.1 (low) paragraph 3 correspond to K7.2 of the Swedish Trust Framework.

K7.2 Issuers of Swedish eID must ensure that technical security controls are implemented when verifying an electronic identity, so that it is highly unlikely that an adversary can force through the protection mechanisms by guessing, eavesdropping, replay or manipulation of communication.

It should be noted that K7.2 applies for all assurance levels. The cryptographic protocols used should all rely on strong cipher suites based on proven primitives in trustworthy implementations, regardless of assurance level.

SUBSTANTIAL

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 can subvert the authentication mechanisms.

The provisions of section 2.3.1 (substantial) paragraph 1 has no specific corresponding clause in the Swedish Trust Framework as all defined assurance levels depend on multi-factor authentication where at least one factor is a cryptographic token, which can be reliably authenticated using a cryptographic protocol and dynamic authentication is therefore inherent to the authentication process.

The provisions of section 2.3.1 (substantial) paragraph 2 corresponds to K7.2 of the Swedish Trust Framework, as stated previously.

HIGH

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 provisions of section 2.3.1 (high) correspond to K7.2 of the Swedish Trust Framework, as stated previously.

An additional requirement of the trust framework (on all assurance level) having an impact on the authentication phase is K4.3, which, among other things, requires cryptographic hardware security modules to be used on the issuer side for all sensitive cryptographic key material used for authenticating users:

K4.3 Sensitive cryptographic key material that is used to issue eIDs, authenticating users and issuing of identity assertions, must be protected in a manner where:

(a) access is restricted, logically and physically, to the roles and applications strictly requiring it,

(b) cryptographic key materials are never stored in plaintext on persistent storage media,

(c) cryptographic key materials are protected when not in use, directly or indirectly, through cryptographic hardware security module with active security mechanisms that protect against both physical and logical attempts to compromise the key material,

(d) security mechanisms for the protection of key material is well-founded and based on recognised and well-established standards; and

(e) **Level 3 and 4:** activation data for the protection of key material is managed through multi-person control.

In addition, the following requirements apply when issuing assertions which relying parties are using to identify users of e-services.

K8.1 Issuers of Swedish eID shall ensure that the identity assertion service has adequate availability and that the release of identity assertions is preceded by a reliable authentication of the claimed electronic identity and its validity.

Level 4: Assertions shall include a reference to cryptographic key material that the issuer has verified that the holder has control over (holder-of-key).

K8.2 Submitted identity assertions shall be valid only for as long as required for the user to gain access to the requested e-service, and protected so that the information is only readable by the intended recipient and that the recipient of the assertion can verify the assertions authenticity.

K8.3 Issuers of Swedish eID, shall, with regard to the risks of misuse of the Identity Provider function, limit the validity period within in which several consecutive identity assertions may be issued to a certain user, before the user is required to be re-identified in accordance with the provisions of section 7.

Applicable guidance

The requirements in K7.1 stipulate that the authentication process used when an eID is verified must include such checks that both ensure that the eID in question is genuine, and that it is not revoked or that its period of validity has expired.

The requirements in K7.2 mean that authentication protocol must be based on sound and proven cryptographic mechanisms which, commensurate to the risks, makes it *highly* unlikely that an adversary will force these security measures.

In cases where the authentication takes place against an Identity provider service according to section 8, these requirements also implies that the Identity provider service must be identifiable by the user in a secure manner. It must be obvious to the user that he communicates with the issuer of the eID he holds, and in this, all available means aimed at preventing the user from being misled into identifying themselves to the wrong party shall be applied.

To ensure that eID holders are able to use their eIDs when needed, issuers must ensure the appropriate availability of the IdP function, also during periods of exceptional use and attempted denial of service attacks. The requirement in K8.1 implies that the IdP function, prior to the issuance of an identity assertion, must have carried out a successful authentication in accordance with section 7 of the trust framework.

For issuing identity assertions at level 4, it is also required that the identity assertions include a reference that can be linked to a cryptographic key that the issuer has previously verified that the holder has control over. Typically, this key is the same key used to

establish the transport security, which, however, does not necessarily have to be the same key material used to authenticate the user in the IdP function.

The purpose of these controls is to prevent an intermediary, who is able to intercept an identity assertion, from being able to use it in another session. This function is commonly referred to as *token binding*.

The Agency for Digital Government publishes in the technical framework the formats, algorithms and other requirements that shall apply for the construction and signing of identity assertions[5]. The maximum validity time for an assertion and also the maximum session time during which the user is allowed to do single-sign-on shall be limited in accordance with K8.2 and K8.3.

The issuer's own private key materials shall be managed and used in protected hardware in accordance with K4.3.

Audit criteria

1. Evaluate the security protocol used to authenticate users and confirm it relies on well-known and proven standards.
2. Verify that any confidential key material used on the issuers' side is protected using hardware security modules, and that such key material is under multi-person control (for assurance level 3 and 4).
3. Evaluate the controls implemented by the issuer to mitigate the risks of users being deceived to authenticate to an intermediary and make an assessment of these being appropriate and sufficient.
4. Verify that the validity periods of issued assertions and are reasonably constrained.

[5] https://docs.swedenconnect.se/technical-framework/latest/00_-_Swedish_eID_Framework_-_Introduction.html

2.4 Management and organisation

2.4.1 General provisions

LOW

1. Providers delivering any operational service covered by this Regulation are a public authority or a legal entity recognised as such by national 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 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.

The provisions of section 2.4.1 (low) paragraph 1 correspond to K2.1 of the Swedish Trust Framework:

> K2.1 Issuers of Swedish eID that is not a public body should be operated as a registered legal entity, and take out and maintain for the operation's necessary insurances.

The provisions of section 2.4.1 (low) paragraph 2 correspond to K2.2 of the Swedish Trust Framework:

> K2.2 Issuers of Swedish eID should have an established organisation, be fully operational in all affected parts of this document, and be well versed in the legal requirements applicable as an issuer of Swedish eID.

The provisions of section 2.4.1 (low) paragraph 3 correspond to K2.3 of the Swedish Trust Framework:

K2.3 Issuers of Swedish eID shall have the ability to assume the risk of liability for damages, as well as to maintain sufficient financial resources to cover operations for at least 1 year.

The provisions of section 2.4.1 (low) paragraph 4 correspond to K2.6 of the Swedish Trust Framework:

K2.6 An issuer of Swedish eID that has outsourced the operation of one or more security critical processes to another party, shall contractually define the critical processes that the subcontractor is responsible for and what requirements apply to these, and clarify the contractual relationship in the practice statement.

The provisions of section 2.4.1 (low) paragraph 5 correspond to K5.5 of the Swedish Trust Framework:

K5.5 An issuer of Swedish eID that ceases operating their eID means shall inform their users and the Agency for Digital Government. The issuer shall retain the archived records in accordance with K2.7 and K2.8.

Applicable guidance

The provisions in this part aim to ensure that issuers have a stable legal and financial standing that is sufficient for the relying parties and holders of Swedish eID, in order to be able to trust the stability and continuity of the business, and that the issuer can be held liable in the event of any damages caused by the issuer.

Regarding the requirements for required insurances in K2.1, this refers to such insurances that are necessary to ensure the continuity of the business in the event of extraordinary events. If the issuer's financial position is such that insurances are not needed to cover damages that may arise (e.g. through sudden events or that the issuer has been found liable for damages), then the requirement for insurance can be disregarded. The provision K2.2 means that the issuer must be able to demonstrate complete compliance with all requirements before any audit is initiated. Audit trails must exist which shows that all controls have been implemented and are effective. In a newly established business, it can be the case that no customers are connected to the service. In that case, the compliance with the requirements must be demonstrated through a reasonable number of pilot users.

The requirement K2.3 does not intend to regulate the issuer's possible liability for damages, but only the issuer's ability to bear the risk of such liability for damages.

Even if the issuer has outsourced some parts of its operations to one or more subcontractors, the issuer is responsible for these subcontractor as for its own operations. They must ensure compliance with all requirements that follow from the trust framework, including ensuring the agency has the same transparency into the subcontractors' business as into the issuers' own business.

The provision K2.6 clarifies the responsibilities in such subcontractor relationships. Which subcontractors are responsible for which parts must be declared so that the agency can assess whether there may be any vulnerability aspects in the use of a certain supplier, possibly by several other issuers using the same subcontractor for the performance of a similar service.

The requirements of K5.5 implies that the issuer shall have established a termination plan. The obligations to maintain and keep records follows from K2.7 and K2.8 which is explained in more detail in 2.4.4 (record keeping).

Audit criteria

1. Verify that the Issuer is a registered legal entity or public authority.
2. Verify that the Issuer has sufficient financial resources to continue operations for at least one year.
3. Based on the Issuer's financial position, make an assessment whether insurances may be needed to cover the liability for damages. If so, verify that the Issuer has taken out such insurances to a sufficient amount.
4. Verify that the Issuer has established its organisation and is fully operational.
5. Identify what subcontractors are involved in the providing of the services, verify that there are adequate contractual arrangements established between the Issuer and the subcontractors and make an assessment if the outsourcing may imply any underlying vulnerabilities to the eID scheme.

2.4.2 Published notices and user information

LOW

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 responses to requests for information.

The provisions of section 2.4.2 (low) paragraph 1 correspond to K5.3 and K5.5 of the Swedish Trust Framework:

K5.3 Issuers of Swedish eID shall provide a practice statement which includes:

(a) the issuer's identity and contact information,

(b) general descriptions of the services and solutions that the issuer provides, including the methods applied for the issuance, revocation and discontinuation of the service,

(c) terms and conditions associated with the service provided, including the user's obligation to protect their electronic identity, the issuer's obligations and responsibilities, service levels and any other guarantees made,

(d) information about the processing of personal identifiable information, and how this is done, and

(e) procedure for changing the practice statement, terms or other conditions for the services provided.

Applicable guidance

The practice statement should describe the services the issuer provides on a high level, where the intended audience is an interested general public. As such it is not intended to go into the level of detail as is being customary for a Certification Practice Statement (CPS). Neither is its format specified. It shall, however, contain the mentioned topics and in particular what responsibilities and obligations will lie with the user to protect the eID means.

Audit criteria

1. Verify that the Issuer has published information consistent with the requirements of K5.3 (a – e).
2. Verify that the Issuer's applied terms and conditions contain the user's obligation to protect their electronic identity and the provided credentials, and that provisions for changing those terms and conditions are included.

2.4.3 Information security management

LOW

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

SUBSTANTIAL

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

The provisions of section 2.4.3 (low) paragraph 1 and 2 correspond to K2.4 and K2.5 of the Swedish Trust Framework:

K2.4 Issuers of Swedish eID must for those parts of the operations covered by the trust framework have an information security management system (ISMS) based on ISO/IEC 27001 or equivalent principles for the management and control of information security, including:

(a) All security-critical administrative and technical processes must be documented on a formal basis, with roles, responsibilities and authorities clearly defined.

(b) Issuers of Swedish eID shall ensure that the operations at all times have sufficient human resources available to meet its commitments.

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

(d) Issuers of Swedish eID shall establish an incident management process that systematically ensures the quality of the service, the reporting procedures and that appropriate reactive and preventive measures are taken to mitigate or prevent damage caused by such events.

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

(f) Issuers of Swedish eID shall regularly evaluate the effectiveness of the information security controls and take measures for improvements of the information security management system.

In addition, for assurance level 4, the Swedish Trust Framework requires a fully developed ISMS according to the standard:

K2.5 Maturity and scope of the information security management system

Level 4: The information security management system shall comply to

SS-ISO/IEC 27001:2014 or equivalent international versions of the standard, and within the scope of the ISMS include all the requirements imposed on issuers of Swedish eID.

Applicable guidance

The requirements in K2.4 focus on control, monitoring and audit of the information security management. To support this a management system according to the international standard ISO/IEC 27001 should be used. However, issuers who have implemented equivalent principles for the management and control of information security, fulfilling the purpose of the requirement, may rely on those principles. Central to compliance is that management has demonstrated its commitment to establish, implement, operate, monitor, review, maintain and improve the management system, that the processes for each step are documented and planned, and that the necessary resources to implement and maintain the system are provided.

The scope and applicability of the information security management system must be documented and established by the management through a statement of applicability or equivalent documents. In particular, the points listed above shall be included within the framework of the management system and its controls.

The process for risk analysis must be documented and applied, and must be based on a risk analysis methodology that provides consistent, correct and comparable results. The process must also include designing, implementing and following up risk mitigation measures, as well as obtaining the risk owner's acceptance of residual risk. The results of such risk analyses must be preserved to enable follow-up and internal audit.

For issuers who provide services on assurance level 4, the management system must comply with the requirements of the information security management system standard SS-ISO/IEC 27001:2014 or corresponding international versions of the standard. Compliance at this level can be proven by certification of the information security management system, carried out by an accredited auditor.

Audit criteria

1. Verify that the Issuer has implemented an information security management system which at least includes the aspects enumerated in K2.4 (a – f) by reviewing the governing documentation developed by the issuer.
2. Sample the risk management process by inspecting one or more documented risk analyses and follow risks from identification to treatment and acceptance of residual risk.
3. Inspect a protocol from the managements review and verify that the status of the information security was reported and that the review included a decision from the management on the continued activities.

2.4.4 Record keeping

LOW

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.

The provisions of section 2.4.4 (low) paragraph 1 and 2 corresponds to K2.7, K2.8 and K3.3 of the Swedish Trust Framework:

K2.7 Issuers of Swedish eID shall retain:

(a) application forms and documents relating to the providing, acceptance or revocation of eID,

(b) agreements, policy documents and practice statements, and

(c) log records, documentation and other evidence demonstrating compliance with the requirements imposed on issuers of Swedish eID, which enables auditing and demonstrating that the security-critical processes and controls are in place and are effective

K2.8 The time for retention shall not be less than ten years, and the issuer shall be able to restore records into readable form throughout that time, unless destruction is required to preserve the rights of data subjects and is supported by law or other regulation.

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

Applicable guidance

The provisions in this section aim to ensure accountability in the issuer's operations and to produce evidence for compliance auditing. The ability to account to every event is also important for the ability investigate any incidents.

The requirement in K2.7(c) should be interpreted so that it includes registering and preserving records of all such events that may be relevant for compliance audit. It includes in particular the technical systems the issuer uses to provide the functionality, and that those systems record all and any such events in a security log.

The term retain is also understood to include that the information to be retained is protected against disclosure and unauthorized modification or destruction. The data to be collected and recorded in accordance with K2.7 includes collecting information in security logs from the relevant systems. The information may also be of a sensitive nature. The records must be protected so that they can be used to carry out regular and systematic audits, in order to ensure that unauthorized access to systems and information has not occurred.

Issuers must therefore ensure that the personnel who have access to the technical system environment do not have access to the security log, and that there is thus a segregation of duties in these parts. The requirement also covers information stored in traditional form on paper.

The fact that information must be able to be reproduced in readable form throughout its archiving period means that information stored electronically must be stored in such a format and on such storage media that it is reasonably ensured that the equipment and software required to retrieve and restore the information is available 10 years after the information was once written to the media.

Audit criteria

1. Verify that the Issuer collects and retains records and other evidence from the issuance and other life-cycle events of eIDs.
2. Verify that access to records are restricted and that the principle of segregation of duties are applied between those managing the records and the administrators who may cause events to be recorded in the Issuer’s systems.
3. Verify the retention periods of records and make notes of shorter retention periods (< 10 years) and on what grounds the Issuer applies those.

2.4.5 Facilities and staff

LOW

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 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.

The provisions of section 2.4.5 (low) paragraph 1 to 4 correspond to K3.1, K3.2 and K3.4 of the Swedish Trust Framework:

K3.1 For the operations essential elements are to be physically protected against damage caused by environmental events, unauthorised access and other external effects. Access control should be applied so that access to sensitive areas are restricted to authorised personnel, that information-carrying media are stored and discarded in a safe manner, and that access to these protected areas are continuously monitored.

K3.2 Before a person assumes one of the roles identified in accordance with K2.4(a), and which are of particular importance for the security of the provided services, the issuer of Swedish eID shall have completed background checks in order to ascertain that the person can be considered to be reliable and that the person has the qualifications and training required to adequately, properly and securely perform the duties imposed by the role.

K3.4 **Level 3 and 4:** Issuers must throughout the issuance process ensure that segregation of duties is applied in such a way that no single individual has the possibility to obtain an eID in another person's name.

Applicable guidance

Issuers must identify the roles that have the potential to override security controls that could mean that eIDs are falsely issued. Persons assuming such a role must have undergone background checks. The issuer is expected to set up its own process for background checks and aptitude testing, which may include verification of academic merits, references from both specified and unspecified previous employers, a financial risk assessment of the person with credit checks and investigation of any potential conflicts of interests. Parts of the test may need to be repeated at certain intervals, which should also be included in the documented process. Personnel who have since long been employed by

the issuer and proved to be reliable do not need to undergo renewed background checks, except for those part that need to be regularly repeated in accordance with the foregoing.

For assurance levels 3 and 4, particularly rigorous requirements are set regarding the segregation of duties in the process of issuing an eID. At no stage should an individual alone be able to circumvent, suspend or otherwise override a security control in such a way that he can obtain an eID (including activation code) in another person's name.

This includes arranging routines, processes and the technical infrastructure in such a way that misuse of critical components cannot occur without several people colluding. Particularly critical parts are, of course, the issuance and delivery of the eID, where special provisions apply in accordance with K6.6–K6.7. However, the requirement also includes the possibility of exploiting functions in the technical infrastructure where the issuer systems reside. Critical components usually consist of hardware security modules, key materials required for communication with and between the issuer systems, the issuer system itself, and storage systems and databases used by the issuer system.

Audit criteria

1. Verify that the issuer has established a background screening and training program for staff that ensures the personnel in trusted roles are reliable and have the competence required to fulfil their responsibilities in a safe manner.
2. Review the principles applied for segregation of duties, such as what trusted roles have been defined and how these must be combined to carry out critical tasks. Assess the effectiveness of those controls.

2.4.6 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.

The provisions of section 2.4.6 (low) paragraph 1 correspond to K4.1 of the Swedish Trust Framework:

> K4.1 Issuers of Swedish eID shall ensure that the technical controls that are implemented are sufficient to achieve the level of security deemed necessary with regard to the operation's nature, extent and other circumstances, and that these controls are functional and effective.

Applicable guidance

Technical controls shall be applied to ensure the integrity, confidentiality, availability and accountability of the systems and the information that the systems process. The effectiveness of the controls must be regularly evaluated as part of the process for continuous improvement.

In addition to the mandatory measures specified in K4.2-K4.4, the issuer shall design and implement the protective measures it deems appropriate and sufficient in the light of the risk analysis and the established risk acceptance criteria. Principles that should be applied are defence-in-depth and overlapping security measures. This includes e.g. encryption measures, physical and logical segmentation of communications networks and restrictive access control to system resources and information assets.

The risk analysis is also expected to identify the identity provider (IdP) function (section 8 in the Swedish Trust Framework) as particularly exposed to risk, as this normally has a high degree of exposure to untrusted networks, while the security dependence on this is very high. Particularly rigorous technical security controls and quality assurance routines are therefore expected to surround this function, which is thus also covered by the requirements in K4.1, if such an IdP function is provided by the issuer.

Audit criteria

1. Review how the Issuer has documented its baseline for IT-security and make an assessment whether those controls documented corresponds to the level of risk in the Issuer's IT environment.
2. Review how the Issuer develops, updates and advances its baseline for IT-security, to verify it is subject to continual improvement.

LOW

2. Electronic communication channels used to exchange personal or sensitive information are protected against eavesdropping, manipulation and replay.

The provisions of section 2.4.6 (low) paragraph 2 corresponds to K4.2 of the Swedish Trust Framework:

K4.2 Electronic communication channels used to exchange sensitive data shall be protected against eavesdropping, manipulation and replay.

Applicable guidance

Security-critical communication to, from or between physically protected environments requires protection against eavesdropping and manipulation. In general, it is more effective to apply strong cryptographic methods to protect such communications, rather than to physically protect the connections along their entire route. Protection of communication is intended to be applicable both as protection on the application level or as protection only during communication (transport protection). However, it is always required that the identities of the communicating parties are mutually verified. The authentication mechanism and the management of the data on which the authentication is based must in terms of security correspond to those of the level of assurance of the eIDs that the system manages.

Audit criteria

3. Verify that controls to protect communication are in place by conducting interviews and inspecting relevant documentation.

LOW

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.

The provisions of section 2.4.6 (low) paragraph 3 correspond to K4.3 of the Swedish Trust Framework:

K4.3 Sensitive cryptographic key material that is used to issue eIDs, authenticating subjects and issuing of identity assertions, must be protected in a manner that:

(a) access is restricted, logically and physically, to the roles and applications strictly requiring it,

(b) cryptographic key materials are never stored in plaintext on persistent storage media,

(c) cryptographic key materials are protected when not in use, directly or indirectly, through cryptographic hardware security modules with active security mechanisms that protect against both physical and logical attempts to disclose the key material,

(d) security mechanisms for the protection of key material is well-founded and based on recognized and well-established standards; and

(e) **Level 3 and 4:** activation data for the protection of key material is managed through multi-person control

Applicable guidance

Cryptographic key material here refers to such key material that is used to issue eIDs, authenticate users and issue identity assertions in accordance with section 8. Key materials used, for example, in network equipment and for the protection of communications are not intended to be covered by these requirements.

Such key material as is covered by the requirements of K4.3 shall be protected by the use of cryptographic hardware security modules (HSM) that offers both logical and physical protection. The security of the HSMs must be credible, meaning that they must be based on well-known standards and principles, sourced from credible suppliers and where the security functions of the devices have been reviewed by a recognised and independent assessment body. In this, it is appropriate to use products that are certified according to e.g. Common Criteria (ISO/IEC 15408), ISO/IEC 19790:2006 or FIPS 140-2 (level 3 or higher).

In the case of product certification according to the Common Criteria, it is intended that this must be done in relation to a protection profile (PP) designed for the purpose, e.g. CWA 14167-2, by a certification body recognized within the Common Criteria Recognition Arrangement (CCRA) and/or Senior Officials Group Information Systems Security Mutual Recognition Agreement (SOGIS-MRA).

Access to the hardware modules and the technical and physical environment in which they are installed shall be restricted to those persons whose duties require it. For assurance level 3 and 4, activation of the key material must be under multi-person control.

Audit criteria

4. Verify that procedures and mechanisms are in place to protect encryption keys during generation, storage, use and destruction.

LOW

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.

The provisions of section 2.4.6 (low) paragraph 4 correspond to K4.4 of the Swedish Trust Framework:

K4.4 Issuers shall have in place documented procedures to ensure that the required level of protection in the IT environment can be maintained over time and in relation to changes, including adequate emergency preparedness to meet changing risk levels and incidents.

Applicable guidance

The provision of K4.4 covers the entire life cycle of the relevant IT systems, from development or acquisition, to configuration, operation, change and decommissioning. All these parts must rely on a formally documented procedures. The IT system and its environment must be monitored in order to be able to detect incidents and anomalies at an early stage. Processes must be established that ensure continuous monitoring of emerging technical threats and that immediate preventive and reactive measures can be taken in response to changing risk levels or incidents that have occurred.

Audit criteria

5. Verify that procedures are in place for change management, incident management, software development and monitoring to support secure administration and operation of the Issuer's systems during its entire life-cycle.

LOW

5. All media containing personal, cryptographic or other sensitive information are stored, transported and disposed of in a safe and secure manner.

The provisions of section 2.4.6 (low) paragraph 5 are part of K3.1 (physical controls) of the Swedish Trust Framework:

K3.1 For the operations essential elements are to be physically protected against damage caused by environmental events, unauthorised access and other external effects. Access control should be applied so that access to sensitive areas are restricted to authorised personnel, that information-carrying media are stored and discarded in a safe manner, and that access to these protected areas are continuously monitored.

Applicable guidance

All locations that house equipment or information carrying media where sensitive data is processed or stored (temporarily or permanently) are considered to require extensive and comprehensive physical protection to prevent information loss or disclosure of confidential data to unauthorized persons.

The physical perimeter protection of the facility should be sufficiently delaying so that the reactive measures (security staff, police, etc.) is able to avert any attempted intrusion into the protected areas. A more remote and unmanned location can therefore be considered to require stronger physical protection, compared with a manned location with guards on watch around the clock.

The physical protection should be arranged in successive barriers of gradually higher degree of protection. According to this reasoning, spaces for equipment that stores e.g. cryptographic key material shall be placed in the inner layers that obtain the highest level of protection, and to which only those personnel who strictly require it to perform their duties have access.

The standards prepared by the Swedish Theft Protection Association (SSF) can be used by issuers to size mechanical intrusion protection and intrusion alarms for protected spaces. The mechanical intrusion protection should then as a rule meet at least SSF 200 protection class 2, and have an alarm protection that meets at least SSF 130 alarm class 2.

Audit criteria

6. Review access conditions set up by the Issuer for the physical access to facilities used for accommodating sensitive equipment and data.
7. Assess the security standards of each of these facilities to determine its suitability for the purpose.

2.4.7 Compliance and audit

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.

The provisions of section 2.4.7 (high) paragraph 1 correspond to K2.9 of the Swedish Trust Framework:

> K2.9 The information security management system and the compliance with all the requirements imposed on the organisation as an issuer of Swedish eID, shall over a three-year period be subject to internal audit, conducted by independent internal control function, unless the size of the organisation or other viable reason justifies the audit to be conducted in another manner.

Applicable guidance

The issuer shall set up an internal audit function that periodically reviews the operations. The internal auditor shall independently plan the audit and document it in an audit plan. The plan shall be scoped to cover all elements of the trust framework over a three-year period, where critical parts is expected to be audited annually. Such audit elements shall be selected on the basis of a risk and materiality analysis and be based on the application form submitted by the Issuer to the Agency for Digital Government.

The internal auditor shall be independent in the performance of the assignment in a manner that ensures an objective and impartial audit. The internal auditor must also have the competence and experience required to be able to determine with reasonable certainty compliance with the requirements. Such a degree of certainty is considered to require sampling and verification of objective evidence.

The results of the internal audit must be documented in an internal audit report and include a statement if the internal auditor considers that the descriptions provided in the application documents to be a fair and accurate description of how the issuer meets the requirements of the trust framework or whether these may descriptions be subject to material inaccuracies.

Audit criteria

1. Verify the existence of an internal audit function by inspecting the audit plan. Make an assessment of the audit plan to determine if it is based on a materiality and risk analysis.
2. Make an assessment of the appointed auditor's competence and independence to determine if the auditor can be expected to able to act impartial and conduct a thorough and objective audit.

3. Review a report and the control program from a conducted audit to verify the scope and depth of the audit is sufficient to establish whether the Issuer's descriptions provided to the agency are fairly stated.