# *Guidance for the application of the levels of assurance which support the eIDAS Regulation*

## 1. Applicable definitions

For the purposes of this Annex, the following definitions apply:

Note on using the guidance: examples are used throughout – they are not normative or exclusive, but there to make the guidance easier to understand as points of reference.

The following words are used within this guidance:

- 'applicant' when describing someone who is trying to authenticate or has yet to be proven to be the legitimate natural or legal person.
- 'subject' when describing the legitimate natural or legal person that is, or to be, represented by the electronic identification means

The 'subject' and 'applicant' effectively become one and the same when an authentication has successfully been performed.

Throughout the Level of Assurance and this Guidance, the term *document* is to be understood to refer to both physical and electronic documents. The term *evidence* is to be understood to refer to physical and electronic evidence, and all other forms nationally accepted.

**(1) 'authoritative source' means any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity;**

GUIDANCE:

An authoritative source is any source that is nationally trusted to provide valid data. An authoritative source may be a register or any other information provided by a responsible entity. A source can only be authoritative for the information provided by it.

It is important to ensure that the provided information is authentic.

Where an authoritative source issues identity evidence then the information on that identity evidence can be considered to represent the identity as known to the authoritative source at the time of issuance as long as that identity evidence can be confirmed as being genuine.

A register, including those from private service providers (e.g. banks), can be used as an authoritative source provided the processes for entry in to those registers are suitably robust and ensures the quality of data and entity providing the register is nationally recognised as

being reliable and trustworthy. In particular it can be useful to take a risk-based approach and perform checks against multiple independent information sources to spread the risk that a register may contain inaccurate or poor quality data.

*Examples of authoritative sources can include:*

- *National Population registers for information on person's identity data (e.g. link name to national identity number etc, verify they are not deceased)*
- *Government registers which have associated governing processes to ensure reliable and correct data such as passport registers, driving license databases, tax registers, social security registers*
- *Business registers for information on legal person's identity and binding to natural persons*
- *Official identity documents such as passports and identity cards*
- *Assertions made by an authority about a person like official documents*

**(2) 'authentication factor' means a factor confirmed as being bound to a person, which falls into any of the following categories:**

GUIDANCE:

An essential characteristic of an electronic identification means is the number and categories of authentication factors it utilises. These definitions help to understand the different categories.

Authentication factors can be divided into the following categories, with further consideration of each given below:

- Knowledge-based factors;
- Possession-based factors;
- Inherent factors.

Authentication factors from different categories may also be combined, e.g. a cryptographic token that is protected via a fingerprint or PIN. An identification means that utilises more than one factor from different categories is called multi-factor, *for example: a smartcard (possession) that is activated via a PIN (knowledge) is a multi-factor identification means.*

If multi-factor authentication is used, the different factors should be chosen in a way to counter different threats/attack vectors.

Evaluating the strength of authentication needs to take into account not only the factor(s) itself, but also the mechanism to verify the factor(s).

**(a) 'possession-based authentication factor' means an authentication factor where the subject is required to demonstrate possession of it;**

The relevant security characteristic of a possession-based authentication factor (e.g. token) is the sole control of it by the owner. This implies that it is important that reproduction of it by a third party is so difficult and unlikely that the risk of this is negligible. The Level of Assurance depends on the level of resistance against reproduction. *For example: asymmetric cryptographic (private) keys, the private keys may be stored on dedicated hardware devices (e.g. smartcards), or software token, uniquely identifiable token (e.g. the SIM card of a cell phone) or devices with one-time-passwords (e.g. "RSA-Token" or printed cards).*

Typical attacks on possession-based authentication factors are theft, duplication or tampering (manipulation), as well as attacks on the proof-of-possession during authentication.

**(b) 'knowledge-based authentication factor' means an authentication factor where the subject is required to demonstrate knowledge of it;**

The knowledge-based factor likely to be known only by the owner of the factor and the verifying entity, *for example: PINs, passwords, memorable words or dates, pass phrases, pre-registered knowledge and other information likely to only be known by the subject.* In some cases even the verifying entity may not know the actual knowledge-based factor, but are able confirm that they and the applicant know the exact same information, *for example using the hash of a password*.

If knowledge is used as a factor it is necessary to mitigate against guessing (either random or brute force) of the knowledge by an adversary. *For example: where the knowledge is a password, good practice prescribes a suitable password policy (e.g. see safeguard S 2.11 "Provisions governing the use of passwords" of the BSI IT-Grundschutz catalogues, Single token authentication & Password entropy of NIST 800-63-2 Appendix A).*

Typical attacks on knowledge-based authentication factors are guessing, phishing eavesdropping or duplication. A characteristic of knowledge-based factors is that attacks are not necessarily noticed by the subject of the electronic identification means. *For example: brute force/dictionary attacks on a password with low entropy and without retry counter or a password that has been copied from a letter or email without knowledge of the owner or the verifier.*

**(c) 'inherent authentication factor' means an authentication factor that is based on a physical attribute of a natural person, and of which the subject is required to demonstrate that they have that physical attribute;**

GUIDANCE:

Inherent authentication factors should have a variance even between people of similar characteristics so that a person may be uniquely identified, *for example: fingerprints, palm prints, palm veins, face, hand geometry, iris, etc*.

A key consideration when a biometric factor is being used is to ensure that the person to whom it relates is physically present at the point of verification. This is to mitigate against spoofing or duplication.

**(3) 'dynamic authentication' means an electronic process using cryptography or other techniques to provide a means of creating on demand an electronic proof that the subject is in control or in possession of the identification data and which changes with each authentication between the subject and the system verifying the subject's identity**

GUIDANCE:

The primary purpose of dynamic authentication is to mitigate against attacks such as 'man-in-the-middle' or misusing verification data from a previously recorded authentication replay to the verifier. This includes:

- replay attacks, i.e. intercepting verification data and reusing them in a different authentication context

certain types of session hijacking, e.g. exchanging (parts of) the authentication contexts of two or more simultaneously occurring authentications. It is important to understand that multi-factor and dynamic authentication are not the same; multi-factor authentication does not require that the authentication is dynamic (e.g. PIN and fingerprint) and can therefore be more exposed to replay attack than a dynamic authentication.

Dynamic authentication might be implemented by the authentication factor (e.g. a one time key from a device) or by the authentication mechanism (e.g. dynamic challenge in a challenge-response authentication).

*Examples for dynamic authentications are:*

- *possession of a private key stored on a smart card and verified using a challenge-response-protocol*
- *protocols based on an ephemeral Diffie-Hellman and providing authentication (e.g. PACE), cryptographic nonces, timestamps and/or non-repeating sequence numbers.*
- *protocols based on a static-ephemeral Diffie-Hellman, if the ephemeral key is provided by the relying party (e.g. EAC)*
- *dynamically generated one time access code (e.g OTP tokens) or challenge response protocols where the one time code has been previously generated and*

*distributed out of band but selected dynamically during authentication (e.g. OTP cards)*

If the subject's private key is stored remotely (centrally stored, e.g. in an HSM operated by the identity provider), the authentication used to access the private key should also be dynamic.

**(4) 'information security management system' means a set of processes and procedures designed to acceptable levels risks related to information security.**

**GUIDANCE:**

## 2. Technical specifications and procedures

**The elements of technical specifications and procedures outlined in this Annex shall be used to determine how the requirements and criteria of Article 8 of Regulation (EU) No 910/2014 shall be applied for electronic identification means issued under an electronic identification scheme.**

**GUIDANCE:**

The requirements in 2.1-2.2 refers to requirements to the enrolment and issuance process. They are functional requirements which must be met at the latest when the eID is used.

### 2.1 Enrolment

GUIDANCE:

This document uses the term "Enrolment" to denote the complete process, consisting of several steps covered in the following subsections:

- Application and Registration (section 2.1.1)
- Identity proofing and verification (section 2.1.2 for natural persons, 2.1.3 for legal persons, and 2.1.4 for the binding between natural and legal person).

#### 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.**

GUIDANCE:

This depends on several factors, including the Level of Assurance of the eID scheme and the criticality of the terms and conditions for the functioning and security of the scheme.

*Examples:*

- *The information are part of national legislation and can therefore to be presumed to be known to the applicant*
- *The applicant gets the required information in written form*
- *The applicant explicitly accepts the terms and conditions*

2. **Ensure the applicant is aware of recommended security precautions related to the electronic identification means.**

GUIDANCE:

See 1. above.

*Examples for security precautions are:*

- *Choosing secure password / PIN according to policy*
- *Safely storing possession based electronic identification means*
- *Not handing over their electronic identification means to another person.*

See also section 2.4.6 on continuously monitoring the state of the art and communicating necessary precautions to the applicants.

**3. Collect the relevant identity data required for identity proofing and verification.**

GUIDANCE:

At least the information necessary to supply the Minimum Data Set needs to be available in the eID scheme. Information for the Minimum Data Set that is not known to or generated by the scheme needs to be collected, e.g. from the applicant or other sources.

See also the following sections, and refer to Article 7 (d) of the Regulation.

**2.1.2 Identity proofing and verification (natural person)**

**LOW**

**1. The person can reasonably 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.**

GUIDANCE:

Evidence can be *reasonably* assumed to be in possession of the subject, if there are no indications to the contrary, and experience assures that the evidence supporting the assumption is sufficient in practice.

*Examples:*

- *Possession can be assured by presenting the evidence physically or electronically.*
- *Possession can be assured by providing non-public information contained in documents sent to the subject to a known address.*

**2. The evidence can be assumed to be genuine, or to exist according to an authoritative source and the evidence appears to be valid.**

GUIDANCE:

The term "genuine" refers to the authenticity of the evidence at the time of issuance. It can be assumed to still be genuine if it is not been forged or manipulated and been issued by the authorised entity.

The term "validity" refers to the correctness of the evidence at the time of presentation. This can include, inter alia, correctness of the information contained in the evidence and revocation/suspension state.

Unless set out in national legislation or administrative practice, genuineness of physical evidence is usually done through physical inspection. For electronic evidence, verification of digital signatures by the authority issuing the evidence is a best practice.

To assure appearance of being genuine and valid, no elaborate checks are necessary at level Low.

**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.**

GUIDANCE:

In many Member States, a population register is an authoritative source for existence of the person. Also official evidence like register excerpts, identity documents or other officially provided evidence serve as authoritative source of the person's existence.

Existence includes that the person represented by the claimed identity is not deceased.

To proof that the applicant is the person asserted by the authoritative source, physical comparison like with a photo identification can be applied, or the evidence can be linked to an electronic authentication where attributes related to the authentication match the attributes held by the authoritative source (identifiers, name, data of birth, etc.)

**SUBSTANTIAL**

**Level Low, plus one of the alternatives listed in points 1 to 4 have 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**

GUIDANCE:

Verification of possession of physical evidence is usually done through presentation of the evidence during application or before, but reliably referencing to it at the time of application. Depending on the type of the evidence, physical presentation at the point of verification may be required, or remote presentation may be possible.

Verification of non-physical evidence may, as an example, comprise verification of access to a bank account or similar, via requesting the applicant to perform a transaction which requires actual access to the bank account.

**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**

GUIDANCE:

Note that the controls from Low apply also, implying that the evidence needs to appear to be valid.

Checking that physical evidence is genuine is usually done through physical inspection of the evidence's security features. Examples for security features are watermarks, inks, holograms, micro-printing, etc.

For electronic evidence, verification can for example be done via digital signatures or by online verification of the evidence against an authoritative source. Examples of such electronic evidence are population register excerpts, or excerpts of authorities' records that have verify identity information during enrolment.

**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;**

GUIDANCE:

The Member State practises may vary depending on the national infrastructure. Some Member States may rely on just a single authority and its security measures like a single identity document authority verifying the identity. Other Member States may go further in augmenting identity proof with multi-level security measures in matching several authorities' data (e.g. a tax application filing an assertion about the subject matching the subject's data with its own tax records, which further gets matched with the population register sending activation codes to the subject's official home address etc.).

The risk of lost, stolen, revoked, expired or suspended documents depends on the robustness and number of independent sources involved, but also on the likelihood that a lost or stolen credentials getting swiftly reported. Factors influencing the likelihood include frequency of use, value to the holder, etc. The evidentiary value of expired documents might also vary depending on the circumstances, e.g. which properties of the document that initiates expiry (e.g. some Member States might allow a driver's license be usable as evidence even if the holder's license to drive a car/a specific type of vehicle has expired)

*Examples for possible steps to minimize the risks can be:*

- *checking the validity against registers.*
- *revocation checks on PKI/smartcard based evidence.*
- *comparison of physical characteristics of the applicant against the evidence.*
- *applying established industry practices like "know-you-customer" in the financial sector (cf. anti-money laundering directive).*
- *measures to deter imposter usage of such documents, e.g. recording a current biometric (photograph, fingerprint etc) from the applicant.*

**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**

GUIDANCE:

No specific guidance given at this time.

**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;**

GUIDANCE:

For guidance on this see bullets above.

**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 the 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 or by an equivalent body**

GUIDANCE:

Examples of a such previously used procedure may be enrolment at an authority that requires unique identification (e.g. tax authorities), or opening a bank account that has identification and know-your-customer requirements under banking laws.

This possibility reflects the procedures referred to in Art. 24 (1) (d) of the eIDAS Regulation thus also clearly taking into account the requirement in Recital 16 of the Regulation on "… consistent application of this Regulation in particular with regard to assurance level high related to identity proofing for issuing qualified certificates."

Confirmation of the equivalent assurance means that the outcomes of the Level of Assurance are met by the procedures previously used in respect to the requirements pertaining to each level.

*Examples for bodies equivalent to conformity assessment bodies according to 765/2008 are national supervisory bodies.*

**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.**

GUIDANCE:

The requirements for identity proofing and verification can be fulfilled using an already issued electronic identification means. Note that identity proofing and verification is only part of the enrolment and issuing process. Requirements beyond the identity proofing and verification must be considered separately.

Note that renewal and replacement is covered in section 2.2.4. For level low and substantial renewal and replacement is possible with the same procedure detailed in this point.

**HIGH**

**Requirements of either point 1 or 2 have to be met:**

**1. Level substantial, plus one of the alternatives listed in points a to c has to be met:**

**a. Where the person has been verified to be in possession of photo or biometric identification evidence recognised by the Member State in which the application for the electronic identity means is being made and that evidence represents the claimed identity, the evidence is checked to determine that it is valid according to an authoritative source;**

GUIDANCE:

See guidance on the definition of 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;**

GUIDANCE:

The comparison of the physical characteristics must be performed on a sufficient level of reliability to ensure clear identity verification of the person.

Sufficiency of procedures can be indicated e.g. by a low false-match rate. Factors for this may include sufficient quality of the comparison data.

- Where staff are involved in the comparison, it is important that the requirements from section 2.4.5 on the staff being sufficiently skilled to perform the comparison are taken into account.

- Analogously, if automated matching is used, available best practice should be taken into account.

**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 substantial, then the entity responsible for the 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 or by an equivalent body**

**and**

**steps are taken that the results of this previous procedure remain valid;**

GUIDANCE:

In general, identification data verified at a previous time may be outdated, e.g. name change, change of address etc. This requirement aims at ensuring that the identification data is checked for validity / updated if necessary. Refer also to Article 7 (d) of the Regulation.

Using the examples given with point 3 of level substantial "tax authorities" and "banks" such steps taken that the results remain valid can be checking attributes of previous identity verification that may change (e.g. name, address) with other sources like a population register.

**c. 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**

**and**

**steps are taken that the results of this previous issuance procedure of a notified electronic identification means remain valid.**

GUIDANCE:

See substantial point 4.

**OR**

**2. Where the applicant does not present any recognised photo or biometric identification evidence, the very same procedures used at the national level of the Member State of the entity responsible for the registration to obtain such recognised photo or biometric identification evidence are applied.**

GUIDANCE:

This point accepts national procedures to obtain recognised photo or biometric identification evidence as valid procedures as a result of recognising such evidence.

*Examples for recognised photo or biometric identification evidence may be passports or identity cards.*

**2.1.3 Identity proofing and verification (legal person)**

GUIDANCE:

Considerations in the guidance on section 2.1.2 apply in many cases also to this section. The variety of applicable sources for information is likely to be more diverse in this section.

**LOW**

**1. The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made.**

GUIDANCE:

No specific guidance given at this time.

**2. The evidence appears to be valid and can be assumed to be genuine, or to exist according to an authoritative source where inclusion of a legal person in the authoritative source is voluntary and is regulated by an agreement between the legal person and the authoritative source.**

GUIDANCE:

No specific guidance given at this time.

**3. The legal person is not known by an authoritative source to be in a status that would prevent it from acting as that legal person.**

GUIDANCE:

No specific guidance given at this time.

**SUBSTANTIAL**

**Level low plus one of the alternatives listed in points 1 to 3 has to be met:**

**1. The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and (if applicable to the legal person) its registration number**

GUIDANCE:

Evidence recognised by Member States can be registers of company names, commercial registers, registers of associations, or similar official sources.

**and**

**the evidence checked to determine whether it is genuine, or known to exist according to an authoritative source, where inclusion of the legal person in the authoritative source is required for the legal person to operate within its sector**

GUIDANCE:

No specific guidance given at this time.

**and**

**steps have been taken to minimise the risk that the legal person's identity is not the claimed identity, taking into account for instance the risk of lost, stolen, suspended, revoked or expired documents;**

GUIDANCE:

No specific guidance given at this time.

**2. Where the procedures used previously by a public or private entity in the same Member State for a purpose other than issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.3 for the assurance level substantial, then the entity responsible for the registration need not 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;**

GUIDANCE:

No specific guidance given at this time.

**or**

**3. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, 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.**

GUIDANCE:

No specific guidance given at this time.

**HIGH**

**Level substantial plus one of the alternatives listed in points 1 to 3 has to be met:**

**1. The claimed identity of the legal person is demonstrated on the basis of evidence recognised by the Member State in which the application for the electronic identity means is being made, including the legal person's name, legal form, and at least one unique identifier representing the legal person used in a national context**

GUIDANCE:

No specific guidance given at this time.

**and**

**the evidence is checked to determine that it is valid according to an authoritative source;**

GUIDANCE:

No specific guidance given at this time.

**or**

**2. Where the procedures used previously by a public or private entity in the same Member State for a purpose other than issuance of electronic identification means provide for an equivalent assurance to those set out in section 2.1.3 for the assurance level high, then the entity responsible for the registration need not 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 this previous procedure remain valid;**

GUIDANCE:

No specific guidance given at this time.

**or**

**3. Where electronic identification means are issued on the basis of a valid notified electronic identification means having the assurance level substantial or high, 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.**

GUIDANCE:

No specific guidance given at this time.

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

**LOW**

**1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level low or above.**

GUIDANCE:

No specific guidance given at this time.

**2. The binding has been established on the basis of nationally recognised procedures.**

GUIDANCE:

No specific guidance given at this time.

**3. The natural person is not known by an authoritative source to be in a status that would prevent that person from acting on behalf of the legal person.**

GUIDANCE:

No specific guidance given at this time.

**SUBSTANTIAL**

**Point 3 of level low plus:**

**1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level substantial or high.**

GUIDANCE:

No specific guidance given at this time.

**2. The binding has been established on the basis of nationally recognised procedures, which resulted in the registration of the binding in an authoritative source.**

GUIDANCE:

No specific guidance given at this time.

**3. The binding has been verified on the basis of information from an authoritative source.**

GUIDANCE:

No specific guidance given at this time.

**HIGH**

**Point 3 of level low and point 2 of level substantial, plus:**

**1. The identity proofing of the natural person acting on behalf of the legal person is verified as having been performed at level high.**

GUIDANCE:

No specific guidance given at this time.

**2. The binding has been verified on the basis of a unique identifier representing the legal person used in national context; and on the basis of information uniquely representing the natural person from an authoritative source.**

GUIDANCE:

No specific guidance given at this time.

**2.2. Electronic identification means management**

GUIDANCE:

It should be noted throughout this section that good practice and the reasonable expectations on an verifier should be aware that subjects are likely to be operating from an untrusted environment.

**2.2.1 Electronic identification means characteristics and creation**

**LOW**

**1. The electronic identification means utilises at least one authentication factor.**

GUIDANCE:

Authentication factors can either be used directly in an authentication (e.g. sending a password), or they can be used indirectly to unlock a token which then provides the authentication (e.g. proof of a key).

**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.**

GUIDANCE:

Where there are references to taking measures towards the electronic identification means being under the control of the subject, it has to be noted that this can only relate to steps that it is reasonable to expect the issuer to take. How this is done relates to the requirements set out in [2.2.2].

**SUBSTANTIAL**

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

GUIDANCE:

Using multiple authentication factors from different categories in a complementary manner can increase the overall security of the identification means. A common example is combining a possession-based token with a password or PIN to unlock the token. Even if the token is lost or stolen, it still cannot be used for authentication without the PIN.

It should be noted that this is always talking about one electronic identification means – for the avoidance of doubt it should be clear that the different factors will relate to the same electronic identification means. Multiple factors are used in conjunction with each other as part of the authentication.

**2. The electronic identification means is designed so that it can be assumed to be used only if under the control of the subject to whom it belongs.**

GUIDANCE:

Binding the electronic identification means to the subject is a pre-requisite for using it for authentication. For example, a token without a personal user PIN or password will not suffice since everyone can use a lost or stolen token. Therefore at least one of the factors should demonstrate knowledge or an inherent characteristic of the subject.

**HIGH**

**Level substantial, plus:**

**1. The electronic identification means protects against duplication and tampering against attackers with high attack potential.**

GUIDANCE:

Protection against duplication and tampering refers to the whole electronic identification means and not to each individual authentication factor. The use of different authentication factors is meant to reduce risk, since different authentication factor categories are susceptible to different threats. Passwords might be observed when used by persons or systems (keyloggers) or if written down, possession based authentication factors might be stolen or lost, systems based on inherent authentication factors might be vulnerable to construed evidence (lookalikes/alterations of real biometrics, synthetic evidence, latex fingerprints etc ).

*Factor-specific examples of protection against tampering and duplication, include:*

- *Possession-based authentication factors: embed cryptographic key material in tamper-resistant hardware that prevents the key from being extracted outside the device either or manipulated in the device through physical or electronic means, hardware security module*

- *Inherent authentication factors: liveness detection, trusted environment, low false match rate*

According to good practice, an electronic identification means should have been proven to be resistant to tampering and duplication. This may include through testing; for example by being certified against relevant technical standards (e.g. Common Criteria).
For guidance on “high attack potential” see section 2.3.1.

**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.**

GUIDANCE:

'reliably protected' refers to the efforts taken to prevent the electronic identification means from being used without the subject's knowledge and active consent. As an example, a private key in a cryptographic key token should not be usable by a machine process without the user's active consent (e.g. by using a PIN).

This is a requirement to protect against: duplication, guessing, replay and manipulation of communication threats.

Other techniques that might be used, in addition to those mentioned previously:

- Strength of static passwords
- Biometric verification of the user
- Checks of the environment against malicious code
- Out of band verification
- For all secrecy based authentication factors (static passwords, one time password in hardware), guessing is a threat which should be mitigated in order to reach a very high level of resilience – e.g. by limiting the number of attempts/slowdown mechanisms and by ensuring sufficient entropy

### 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.**

GUIDANCE:

In case of a single factor (i.e. password) that is issued online, the activation code could be delivered via regular mail to the verified address of the subject or sent to the mobile phone of the applicant (e.g. via SMS) after having verified that the phone number indeed belongs to the subject (e.g. via call-back).

In case of multiple factors, at least one factor shall be delivered via a method described above and depending on the scheme, the use of activation codes may not be required.

**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.**

GUIDANCE:

Possible mechanisms include

- delivery in person
- delivery by registered mail

using some activation process, where it can be reasonably assumed that only the subject has the necessary information to activate the means (e.g. a transport-PIN delivered separately from the identification means).

For Substantial multiple authentication factors shall be used. Activation codes are not necessarily required. Several issuance, delivery and activation combinations are possible that meet Substantial:

- The delivery of the electronic identification means can be done via regular mail, its activation by sending a code to the bank account of the subject. The applicant enters the code to activate the electronic identification means. The assumption here is that bank authentication is of at least level Substantial.
- Separate delivery of the electronic identification means and the activation code via regular mail to the verified address of the subject.
- Delivery of the electronic identification means via regular mail to the address of the applicant. The electronic identification means is handed over after having verified the identity of the applicant.

**HIGH**

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

GUIDANCE:

This control requires an activation process to be performed, i.e. secure delivery alone is not sufficient. In general, an activation process requires user interaction of some kind.

The aim of an activation process – beyond ensuring that the means are delivered to the correct subject – is an explicit step of the subject to take ownership of the means. Only after this the means can be used for authentication.

For High the activation process shall ensure that only the legitimate owner can activate the electronic identification means and that the activation process is protected from accidental loss and insider threats such as collusion.

The registration and issuance of electronic identification means shall never be performed by a single person.

Where activation codes are used the applicant has to it within a specified period of time.

*For example*

- *The issuance of the electronic identification means at the registration desk and the delivery of an activation code via regular mail to the verified address of the subject.*
- *The delivery of an online-requested electronic identification means via regular mail and the issuance of an activation code to a trusted party (e.g. a nearby post office). The participant has to collect the activation code personally on presentation of an ID-document.*
- *The electronic identification means is requested online and is physically handed over by a trusted courier after having verified the identity of the applicant. An activation code is sent separately via regular mail to the verified address of the subject.*

### 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 efficient manner.**

GUIDANCE:

This should be publically accessible. Examples may include, by phone, a website, an e-mail address etc. Where a verifier receives such a request, action should be taken as soon as possible.

**2. The existence of measures taken to prevent unauthorised suspension, revocation and/or reactivation.**

GUIDANCE:

This will generally imply authentication of the requester's authorisation to act in that way. It should be determined who can authorise suspension and/or revocation besides the user – for example relevant public authorities.

**3. Reactivation shall take place only if the same assurance requirements as established before the suspension or revocation continue to be met.**

GUIDANCE:

No specific guidance given at this time.

### 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 be based on a valid electronic identification means of the same, or higher, assurance level.**

GUIDANCE:

No specific guidance given at this time.

**HIGH**

**Level low, plus:**

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

GUIDANCE:

No specific guidance given at this time.

As set out in the guidance relating to the definition of authoritative source (above), that may include the eID means itself. Further consideration is needed on the guidance around this point.

## 2.3. Authentication

**This section focuses on the threats associated with the use of the authentication mechanism and lists the requirements for each assurance level. In this section controls are understood to be commensurate to the risks at the given level.**

### 2.3.1 Authentication mechanism

GUIDANCE:

The authentication mechanisms used in the authentication phase cannot prevent all attacks completely, they can only offer resistance to attacks on a certain level of security/assurance. A standard way to quantify the resistance of different mechanisms is to rank them according their resistance against attacks with a certain attack potential (i.e. strength of an attacker).

The Level of Assurance use the terms “enhanced-basic”, “moderate” and “high” to denote the different attack potentials. This terminology is borrowed from ISO/IEC 15408 “Information technology – Security techniques – Evaluation criteria for IT security” and ISO/IEC 18045 “Information technology – Security techniques – Methodology for IT security evaluation”. The text of the standards is also freely available at www.commoncriteriaportal.org/cc (CCPART1-3 being equivalent to ISO/IEC 15408 and CEM equivalent to ISO/IEC 18045).

ISO/IEC 15408-1 defines “attack potential – measure of the effort to be expended in attacking a [mechanism], expressed in terms of an attacker's expertise, resources and motivation”.

Annex B.4 of ISO/IEC 18045 / CEM contains Guidance on how to calculate the attack potential necessary to exploit a given weakness of an authentication mechanism.

In order to meet the requirements set out in the implementing act, some assessment of resistance against potential attacks should be carried out.

The assessment should take relevant threats into accounts. For example, ISO 29115 mentions: online guessing, offline guessing, credential duplication, phishing, eavesdropping, replay attack, session hijacking, man-in-the-middle, credential theft, spoofing and masquerading.

During assessing attack resistance, the whole authentication mechanism should be taken into account including the risks resulting from verification of the possession of the electronic identification means.

*For example*

- *For LoA high, it is not sufficient that a smart card protects a cryptographic key against manipulation with high attack potential, also the cryptographic protocol should protect the verification of the possession of the key against manipulation/replay against high attack potential.*
- *For a one-time-password token, where the generated one-time-password is transmitted via a secure channel (e.g. TLS), the strength of the possession-based-factor is limited not only by the strength of the token, but also by the strength of the secure channel.*
- *The mechanism for proof-of-possession of a time-based one-time-password generator is the submission of a generated one-time-password to the verifier. The strength of this mechanism is limited, among others, by the length of the one-time-password, the time-window for validity of the password, and the confidentiality of the transmission.*

Reasonable assumptions on the level of security of components used by, but not part of, the authentication scheme (e.g. the environment of the user, browser, smart phone, etc.) should be taken into account during the risk assessment.

Components can be operated in different configurations with different security settings.

*As an example, the assessment might assume that the user operates a personal firewall and virus protection on his/her computer.*

*As a counterexample, currently it would not be reasonable to assume that the browser of the user is configured to use only secure cipher suites for Transport Layer Security (TLS); however this can be enforced by the service.*

The assessment might presume reasonable settings for the components not part of the authentication scheme.

**LOW**

**1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity.**

GUIDANCE:

The release of person identification information is about transmitting the minimum data set (MDS) to the relying party.

**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.**

GUIDANCE:

Stored personal data shall be subject to strict access controls. Measures should be used to protect person identification data*, for example encryption and hashing in accordance with good practice such as ENISA Algorithms, Key Sizes and Parameters Report* or national cryptographic guidance.

All access should be audited.

**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.**

GUIDANCE:

*All required verification steps shall be clearly described, implemented and tested.*

**SUBSTANTIAL**

**Level low, plus:**

**1. The release of person identification data shall be preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication process.**

GUIDANCE:

In practice this means the authentication means should include either a one-time code or one time challenge-response to ensure it is truly dynamic. The one-time code or challenge should be generated in a way where it cannot be tampered with.

When using random numbers in a challenge-response protocol care should be taken to ensure the "quality" of these numbers, *for example by following good practice for cryptographically secure pseudo-random number generators.*

**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.**

GUIDANCE:

No specific guidance given at this time.

**HIGH**

**Level substantial, plus:**

**The authentication mechanism implements security controls for the verification of the electronic identification means, so that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms.**

GUIDANCE:

If cryptography is used to secure an authentication mechanism, strong cryptographic protocols and appropriate key lengths should be selected.

An important method to ensure the strength of cryptographic protocols are cryptographic analyses such as cryptographic security proofs.

When protocols are known not to be secure (e.g. SSLv3), that should be taken into account; as should any known practical attacks on certain cryptographic protocols and measures put in place to counter any attacks where such protocols are being used.

Where the authentication mechanism uses a cryptographic solution then not only the cryptographic primitives, but also the protocols and the environment, especially key management, should be taken into account.

*Example: A typical mechanism for key management is utilizing a Public Key Infrastructure. The operational security of the CA directly influences the security of the authentication mechanism. Besides the purely technical security of the CA, also the organizational aspects.*

*If several CAs are trusted for issuance of certificates for a certain part of an eID scheme, the overall security of all trusted CAs must be taken into account.*

*As an example for the latter, if identification of communication endpoints is performed using certificates from an "Internet PKI", i.e. issued by CAs whose root certificate is contained in the trust store of the browser of the user, the security of all CAs contained in the trust stores must be considered. In general, according to good practice, if the infrastructure of the eID scheme uses an Internet PKI, then for LoA High, the user should be recommended to use adequate security mechanisms.*

*The authentication should protect against manipulation of authentication data in order to deceive the subject into believing they are authenticating to a different relying party.*

### 2.4. Management and organisation

**All participants providing a service related to electronic identification in a cross-border context ("providers") shall have in place documented information security management practices, policies, approaches to risk management, and other recognised controls so as to provide assurance to the appropriate governance bodies for the electronic identification schemes in the respective Member States that effective practices are in place. Throughout section 2.4, all requirements/elements shall be understood as commensurate to the risks at the given level.**

GUIDANCE:

All participants includes the parties of the cross border authentication process, including the identity provider and validation services operated by the member state, (if any) but not the authoritative sources used.

As a general principle in risk management is that it is up to the organisation to choose which level of risk which it finds acceptable. This general principle is modified by the requirement in 2.4, since the organisation should have controls that are commensurate to the risks at the given level.

Many / most of the requirements of this section are fulfilled if either

- an Information Security Management System according to ISO/IEC 27001:2013 is in place and audited

- the providers delivering operational services are qualified Trust Service Providers according to the eIDAS-regulation

This does not preclude other standards, e.g. suitable national schemes fulfilling the requirements in this section, to be used.

A mapping of the requirements to ISO/IEC 27001:2013 and the requirements for qTSPs is provided as part of the guidance of the requirements [TBD]. In case of an informatnio security management system according to ISO/IEC 27001:2013, all requirements from sections 2.4.4 – 2.4.6 are covered by relevant controls from that standard.

**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 Member State, with an established organisation and fully operational in all parts relevant for the providing of the services.**

GUIDANCE:

No specific guidance given at this time.

**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.**

GUIDANCE:

No specific guidance given at this time.

**3. Providers are able to demonstrate the ability to assume the risk of liability for damages, as well as having sufficient financial resources for continued operations and providing of the services.**

GUIDANCE:

It can be assumed that a public authority has sufficient financial resources to absorb any liabilities under the regulation. Other ways of demonstrating fulfilment of this requirement include

- Appropriate insurance coverage for the obligations.
- A contract with a public authority covering the obligations.

- A legal obligation for a public authority to take over liability/operations if necessary.

**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.**

GUIDANCE:

No specific guidance given at this time.

**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.**

GUIDANCE:

This pertains for both cessation of service as well as shut-down by external authorities. Such plans should cover all foreseeable circumstances leading to a discontinuation of the service / continuation by another provider.

**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.**

GUIDANCE:

Publication can be covered by

- having the information contained in a law.
- providing the information in publically accessible documents.

**2. Appropriate policy and procedures are 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.**

GUIDANCE:

A user is an active participant in a scheme, a subscriber can also be an applicant before getting issued an electronic identification means (and activating it, if applicable).

In this context notify does not only mean that information should always be directed to the user. A notification in the sense of this requirement could also be done by publishing the required information on the website of the provider depending on its content of the change and national law.

**3. Appropriate policies and procedures are to be put in place that provide for full and correct responses to requests for information.**

GUIDANCE:

No specific guidance given at this time.

**2.4.3 Information security management**

**LOW**

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

*GUIDANCE:*

Managing information security risks is relevant for all parts of the eID scheme. To be effective, the ISMS needs to consider the relevant risks to all parts of the scheme.

Depending on the organisational structure of an eID scheme, it may also be appropriate to have several ISMSes for the different operators of components of the scheme.

**SUBSTANTIAL**

**Level low, plus:**

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

GUIDANCE:

ISO/IEC 27001:2013 is a well-known and proven standard for the management of information security risk. Refer also to section 2.4.7 for assuring compliance.

### 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.**

GUIDANCE:

Where records are kept then the records management system should ensure that the integrity and confidentiality is maintained throughout their lifetime.

For an information security management system according to ISO/IEC 27001:2013, this requirement is covered as part of the controls A.12 ‘Operational security’ in combination with A.18 ‘Compliance’ (especially A.12.4 Logging and monitoring).

**2. Retain, as far as permitted by national law or other national administrative arragement, 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.**

GUIDANCE:

Records, in particular those used to non-repudiation, shall be maintained for a sufficient period as prescribed/allowed by national law in order to support any challenge or legal process. When records are no longer needed then they shall be properly destroyed. This applies to any media, electronic or print, where such records are maintained.

For an information security management system according to ISO/IEC 27001:2013, this requirement is covered as part of controls A.18 ‘Compliance’ (cf. A.18.1.3).

### 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.**

GUIDANCE:

Where staff require proven skills then there should be a training programme that ensures the staff can demonstrate and maintain their skills.

*For example*

*Good practice for staff inspecting physical documents (e.g. passports, ID cards) may include:*
*Low*

- *Have awareness that document fraud takes place.*
- *Have the ability to accurately and consistently check documents for anomalies like spelling mistakes, differing fonts, missing pages and inconsistencies in document layout and alignment.*

*Substantial*

- *Have received training in the detection of fraudulent documentation using the nationally recognised quality training material.*
- *Be able to identify tampered documents/laminate.*
- *Be able to identify basic printing techniques.*

*High*

- *Have good working knowledge of document design and their security features.*
- *Have knowledge through appropriate training of the various types of watermarks, security fibres and printing techniques.*
- *Be able to identify forged and counterfeit documents through examination.*
- *Have the ability to make effective use of reference material.*

For an information security management system according to ISO/IEC 27001:2013, this requirement is covered as part of controls A.7 'Human resource security' (cf. in particular A.7.2.2)

**2. The existence of sufficient staff and subcontractors to adequately operate and resource the service according to its policies and procedures.**

GUIDANCE:

For an information security management system according to ISO/IEC 27001:2013, this requirement is covered as part of controls A.12 'Operations security' (cf. A.12.1.2 'Capacity management') which also addresses the capacity of human resources.

**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.**

GUIDANCE:

Security critical services, e.g. revocation, should be resilient to outages and interruptions. This should sufficiently protect the service from outages and natural events such as fire, flood, storm, and earthquakes etc. that affect a single facility.

If relevant, facilities should be physically secure through the use of appropriate locks, access control mechanism and physical monitoring (e.g. CCTV). These may be provided by the facility as a service, it is not required that the operator of the service performs these functions.

There should be process in place to monitor for unauthorised access and raise alerts to the service when possible unauthorised events occur.

For an information system management system according to ISO/IEC 27001:2013, this requirement is covered as part of controls A.11 'Physical and environmental security' and A.9 'Access control'. The monitoring mechanisms should be also considered also as part of control A.12 'Operations security'.

**4. Facilities used for providing the service shall ensure access to areas holding or processing personal, cryptographic or other sensitive information is limited to authorised staff or subcontractors.**

GUIDANCE:

For an information security management system according to ISO/IEC 27001:2013, this requirement is covered as part of controls A.9 'Access control', whose objective is particularly to limit access to information and information processing facilities, A.10 'Cryptography' and A.18.1.5 'Regulation of cryptographic 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.**

GUIDANCE:

It is important to separate the assessment of protection requirements of confidentiality and integrity. While protection of integrity (or authenticity) is basically determined by the level of assurance, confidentiality of person related data shall also take into account the type of data and possible legal requirements on data protection.

The confidentiality of personal data must be protected, controls should be in place based on an assessment using a risk-based approach according to the selected information security management system. These should cover areas such as protection from hacking, abuse, misuse, denial-of-service (DoS) and distributed-denial-of-service (DDoS) attacks.

Confidentiality and authenticity/integrity of personal data during cross-border transmission is covered by the Implementing Act on the Interoperability Framework.

For an information security management system according to ISO/IEC 27001:2013, this requirement is covered as part of the controls A.10 ‘Cryptography’, A.12 ‘Operations security’, (relating to availability) A.17 ‘Information security aspects of business continuity management’ and A.18.1.5 ‘Regulation of cryptographic controls’

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

GUIDANCE:

It has to be considered that communication channels may arise between different parties involved within an identification scheme, e.g. between the owner of the identification means and a service or between municipality and manufacturer.

One possibility for technical controls for communication channels are technical guidelines issued by an authority that gives requirements on cryptography and security measures to be used. This will typically be achieved using cryptographic protocols with described verification steps.

Requirements for communication channels between nodes of the eIDAS Interoperability Framework are given in the eIDAS Technical Specification for the framework.

For an information security management system according to ISO/IEC 27001:2013, this requirement is covered as part of the controls A.10 ‘Cryptography’, A.13 ‘Communications security’ and A.18.1.5 ‘Regulation of cryptographic controls’, which may also include references to technical guidelines as stated above.

**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 plaintext.**

GUIDANCE:

For an information security management system according to ISO/IEC 27001:2013, this requirement is covered as part of the controls A.9 ‘Access control’ and A.10 ‘Cryptography’.

**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.**

GUIDANCE:

For an information security management system according to ISO/IEC 27001:2013, this requirement is covered as part of the controls A.14 ‘Security in development and support processes’ and A.16 ‘ Information security incident management’.

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

GUIDANCE:

For an information security management system according to ISO/IEC 27001:2013, this requirement is covered as part of the controls in A.8 ‘Asset management’.

**SUBSTANTIAL**

**Level low, plus:**

**Sensitive cryptographic material, if used for issuing electronic identification means and authentication, is protected from tampering.**

GUIDANCE:

Sensitive cryptographic material refers to key materials used to issue electronic identification means, authenticating users and issuing of assertions (when applicable). Protection of these types of cryptographic keys is of paramount importance for the security of an electronic identification scheme.

Tamper protection mechanisms are intended to counter any attempts to expose, manipulate or misuse the cryptographic key material throughout its full life-cycle. This is achieved by implementing both physical and logical security controls for the protection of these keys.

It is common practice that these security controls are implemented as part of a hardware security module (HSM). Such products fulfilling this purpose should provide transparency in the security mechanisms implemented and meet the highest quality and security standards. Security certification can give accompanying evidence and is good practice to assess the quality of HSMs, like certification under Criteria Recognition Arrangement (CCRA) and/or the Senior Officials Group Information Systems Security Mutual Recognition Agreement (SOGIS-MRA), or FIPS-140. Products should be sourced from a trusted vendor and commissioned in a way that ensures the chain of custody of the units, from the manufacturing of the unit to the point where the HSM is taken into production.

For an information security management system according to ISO/IEC 27001:2013, this requirement should be covered as part of controls A.10 ‘Cryptography’ and A.11 ‘Physical and environmental security’.

### 2.4.7 Compliance and audit

**LOW**

**The existence of periodical internal audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.**

GUIDANCE:

Audits take the level of risk connected to the system/parts of the system into account. This implies that the depth of an audit may be quite different for different level of assurance.

The requirement for an internal audit can also be fulfilled by an audit contracted to an external party. For level low, an independent audit is not required (see below for "independent").

Standard procedure for information security management system audits is to cover all parts of the system within three years, including surveillance audits every year.

For an information security management system according to ISO/IEC 27001:2013, this requirement is covered as part of the controls A.18 'Compliance' (cf. A.18.2 'Information security review').

**SUBSTANTIAL**

**The existence of periodical independent internal or external audits scoped to include all parts relevant to the supply of the provided services to ensure compliance with relevant policy.**

GUIDANCE:

An audit which is managed internally by the organisations own standards, and where the result is communicated primarily to the organisations own management, is according to recognised definitions an internal audit (even though there may be externally sourced competences involved). An internal audit should be conducted objectively by an independent audit function, and can form the basis for an organisation's self-declaration of compliance. The audit should be conducted independently from the operating managers of the function being audited to avoid bias and conflict of interests.

External (third-party) audits are audits which are conducted by independent auditing organisations, such as regulators or those providing certification. The goal is to assess the organisation being audited to a certain set of principles and criteria, and to make a statement whether the management's assertion to those principles is fairly stated. External audits

typically require an auditing standard, such as the ISO/IEC 27007 auditing standard or systrust/webtrust (of AICPA/CICA).

ISO 19011:2011 provides guidance on auditing management systems, including the principles of internal and external auditing, as well as guidance on the evaluation of competence of individuals involved in the audit process.

**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.**

GUIDANCE:

This requirement can be fulfilled by an audit/certification according to ISO/IEC 27007.

**2. Where a scheme is directly managed by a government body, it is audited in accordance with the national law.**

GUIDANCE:

No specific guidance given at this time.