Requirements for Identity Providers

Version 1.0

Effective since 01.01.2017

Composed according to Regulation (EU) No 910/2014 of the European Parliament and of the Council and Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015.

1. Terminology

Term	Definitions
Electronic identification means	A material and/or immaterial unit containing person identification data and which is used for authentication for an online service. in a context of this document when its necessary, it can be interpreted as electronical identification channel.
Authoritative source	Source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to prove identity

2. Requirements for non-qualified certificates

To use external electronic identity provider as a source of Smart-ID user identity information the following requirements must be met by the Identity Provider.

2.1. Enrollment

Identity Provider ensures that the applicant is aware of the current terms and conditions related to the use of the electronic identification means.

2.2. Identity proofing and verification

The person has been verified to be in possession of photo or biometric identification evidence and that evidence represents the claimed identity and 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.

2.3. Electronic identification means characteristics and design

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

2.4. **Issuance, delivery and activation**

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

2.5. **Suspension, revocation and reactivation**

It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner.

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

2.6. **Renewal and replacement**

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.

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

2.7. **Information security management**

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

2.8. **Record keeping**

Recording and maintenance of relevant information is made using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention.

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.

2.9. **Facilities and staff**

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.

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

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.

2.10. **Technical controls**

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.

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

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

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

2.11. **Compliance and audit**

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.

3. **Requirements for qualified certificates**

To use external electronic identity provider as a source of user identity information the following requirements must be met by the Identity Provider.

3.1. **Enrollment**

Identity Provider ensures that the applicant is aware of the terms and conditions related to the use of the electronic identification means.

3.2. **Identity proofing and verification**

Identity scheme is notified by a member state to be on the level substantial or high.

3.3. **Electronic identification means characteristics and design**

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

The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential.

The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.

3.4. **Issuance, delivery and activation**

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

3.5. **Suspension, revocation and reactivation**

It is possible to suspend and/or revoke an electronic identification means in a timely and effective manner.

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

3.6. **Renewal and replacement**

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.

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

3.7. **Information security management**

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

3.8. **Record keeping**

Recording and maintenance of relevant information is made using an effective record-management system, taking into account applicable legislation and good practice in relation to data protection and data retention.

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.

3.9. **Facilities and staff**

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.

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

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.

3.10. **Technical controls**

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.

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

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

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

3.11. **Compliance and audit**

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.