Requirements for Identity Providers

Composed according to Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market and Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

Version information		
Valid from	**Version**	**Changes**
14.09.2019	2.0	Preambula added. Terminology - terms of electronic identification means and authoritative source added. Clause 2.3 - added requirement for eID characteristics and design compliance to PSD2 regulations for strong customer authentication, QSCD or similar security level (high) according to Commission Implementing Regulation 2015/1502 of 8 September 2015. Previous clauses 3.1-3.11 under section 3 were deleted and new requirement defined. Clause 3 requires from IDP for qualified certificates that identity scheme under which electronic identity means are issued have been notified or evaluated by a member state to be on the level high. If IDP is evaluated against assurance level high requirements, then no need to define further requirements, except that the physical presence of the natural person during the issuance of electronic identification mean has to be ensured. When these two requirements are fulfilled, then qualified e-signature certificates can be issued according to the eIDAS art 24 para 1 (b).
01.01.2017	1.0	Initial version

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
eIDAS	Regulation (EU) No 910/2014 [8] of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
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. Enrolment

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 and only if at least:

1. strong customer authentication solution compliant with requirements provided in the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (1) and Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication is used; or
2. based on Qualified Signature Creation Device (QSCD); or
3. other solution ensuring similar or higher security level is used whereas following requirements are fulfilled:

1. The electronic identification means utilises at least two authentication factors from different categories;
2. 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;
3. The electronic identification means protects against duplication and tampering as well as against attackers with high attack potential;
4. The electronic identification means is designed so that it can be reliably protected by the person to whom it belongs against use by others.

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 following requirements must be met by the Identity Provider:

- An electronic identification scheme under which electronic identification means are issued by Identity Provider have been notified according to the eIDAS Article 9(1) or evaluated by member state on the assurance level high. Evaluation must be publicly available;
- During the issuance of electronic identification means under this electronic identification scheme a physical presence of the natural person has to be ensured.