

Auditing of Remote Trust Services – Today and Tomorrow

Matthias Wiedenhorst

Remote Trust Services

-

What do I mean?

Remote Trust Services – What do I mean?

- Creation of (qualified) electronic signatures / seals on behalf of the subject
 - Enrollment of subjects
 - Management of a remote QSCD on behalf of the subject
 - generation, usage and destruction of subject private keys
 - Realization of sole control
 - Authentication of the subject
 - Creation of the signature / seal

Auditing of Remote Trust Services – Today

Auditing of Remote Trust Services – Today

- eIDAS



Trusted List Browser

Tool to browse the national eIDAS Trusted Lists and the EU List of eIDAS Trusted Lists (LOTL).

European Commission > CEF Digital > eSignature > Trusted List Browser > Search > Type of service

What type of service are you looking for? step 1/2

Check all

Qualified trust services

<input type="checkbox"/> Qualified certificate for electronic signature	<input type="checkbox"/> Qualified certificate for electronic seal	<input type="checkbox"/> Qualified certificate for website authentication
<input type="checkbox"/> Qualified validation service for qualified electronic signature	<input type="checkbox"/> Qualified preservation service for qualified electronic signature	<input type="checkbox"/> Qualified validation service for qualified electronic seal
<input type="checkbox"/> Qualified preservation service for qualified electronic seal	<input type="checkbox"/> Qualified time stamp	<input type="checkbox"/> Qualified electronic registered delivery service

Non-qualified trust services

<input type="checkbox"/> Certificate for electronic signature	<input type="checkbox"/> Certificate for electronic seal	<input type="checkbox"/> Certificate for website authentication
<input type="checkbox"/> Validation service for electronic signature	<input type="checkbox"/> Generation service for electronic signature	<input type="checkbox"/> Preservation service for electronic signature
<input type="checkbox"/> Validation service for electronic seal	<input type="checkbox"/> Generation service for electronic seal	<input type="checkbox"/> Preservation service for electronic seal
<input type="checkbox"/> Time stamp service	<input type="checkbox"/> Electronic registered delivery service	<input type="checkbox"/> Non-regulatory, nationally defined trust service
<input type="checkbox"/> Undefined type		



Auditing of Remote Trust Services – Today

- eIDAS

ANNEX II

REQUIREMENTS FOR QUALIFIED ELECTRONIC SIGNATURE CREATION DEVICES

3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.
4. Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:
 - (a) the security of the duplicated datasets must be at the same level as for the original datasets;
 - (b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

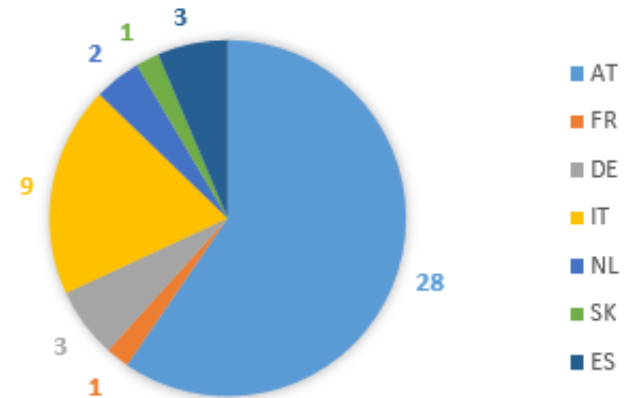
Auditing of Remote Trust Services – Today

- Creation of advanced signature / seal based on a qualified certificate on behalf of the subject
 - Signing certificate must be issued by a corresponding QTSP
- Creation of qualified signature / seal on behalf of the subject
 - Signing certificate must be issued by a corresponding QTSP
 - Issuing QTSP must ensure that keys are generated and stored in a certified remote QSCD, operated by a QTSP

Auditing of Remote Trust Services – Today

- Certification for (Remote) QSCDs
 - COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016
 - Type 1 QSCDs: Common Criteria Protection Profiles EN 419 211-x
 - Type 2 QSCDs: Alternative process with a “comparable security level” to be defined by each certification body

TYPE 2 QSCD BY COUNTRY OF CERTIFICATION



Auditing of Remote Trust Services – Today

- Creation of (qualified) electronic signatures / seals on behalf of the subject is not regarded as a qualified trust service today
 - No requirement for independent auditing of such signing services
 - No ex-ante supervision
 - But may only be provided by a QTSP
 - eIDAS does not restrict the type of QTSP
 - ETSI TS 119 612 v2.1.1 (TSL specification) specifies it only for QTSPs issuing certificates
- Problem:
 - No harmonization with regard to service provisioning

Auditing of Remote Trust Services – Tomorrow

Auditing of Remote Trust Services – Tomorrow

- Disclaimer
 - The following section is based on a draft version as published in June 2021
 - Text of the final eIDAS 2.0 may change during the further process



Auditing of Remote Trust Services – Tomorrow

- eIDAS Draft

Article 29

Requirements for qualified electronic signature creation devices

1. Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.
 - 1a. Generating, managing and duplicating electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider providing a qualified trust service for the management of a remote electronic qualified signature creation device.
2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Auditing of Remote Trust Services – Tomorrow

- A new qualified trust service for the management of remote QSCD is introduced
- 39a mutatis mutandis

Article 29a

Requirements for a qualified service for the management of remote electronic signature creation devices

1. The management of remote qualified electronic signature creation devices as a qualified service may only be carried out by a qualified trust service provider that:
 - (a) Generates or manages electronic signature creation data on behalf of the signatory;
 - (b) notwithstanding point (1)(d) of Annex II, duplicates the electronic signature creation data only for back-up purposes provided the following requirements are met:
 - the security of the duplicated datasets must be at the same level as for the original datasets;
 - the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.
 - (c) complies with any requirements identified in the certification report of the specific remote qualified signature creation device issued pursuant to Article 30.

Article 39a

Requirements for a qualified service for the management of remote electronic seal creation devices

Article 29a shall apply mutatis mutandis to a qualified service for the management of remote electronic seal creation devices.

Auditing of Remote Trust Services – Tomorrow

- Mandatory implementing act regarding technical specifications for service provisioning and auditing of such QTSP

Article 29a

Requirements for a qualified service for the management of remote electronic signature creation devices

2. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish technical specifications and reference numbers of standards for the purposes of paragraph 1.

Article 39a


Requirements for a qualified service for the management of remote electronic seal creation devices

Article 29a shall apply mutatis mutandis to a qualified service for the management of remote electronic seal creation devices.

Auditing of Remote Trust Services – Tomorrow

- Possible candidates for standards regarding remote signing:
 - ETSI TS 119 431-1 “Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
 - CEN EN 419 241-1: Trustworthy Systems Supporting Server Signing Part 1: General System Security Requirements


ETSI TS 119 431-1 v1.2.1 (2021-05)



TECHNICAL SPECIFICATION

**Electronic Signatures and Infrastructure
Policy and security requirements for trust service providers
Part 1: TSP service components operating a remote QSCD / SCDev**

EUROPEAN STANDARD	EN 419241-1
NORME EUROPÉENNE	
EUROPÄISCHE NORM	July 2018
ICS 35.030	Supersedes CEN/TS 419241:2014
English Version	
Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements	
Systèmes fiables de serveur de signature électronique - Partie 1: Exigences de sécurité générales du système	
Vertrauenswürdige Systeme, die Serversignaturen unterstützen - Teil 1: Allgemeine Systemicherfordernisse	
This European Standard was approved by CEN on 30 April 2018.	
CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN member.	
This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.	
CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.	



EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1049 Brussels

© 2018 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members. Ref. No. EN 419241-1:2018 E

Auditing of Remote Trust Services – Tomorrow

- Update of Implementing Act expected
- Possible candidates for standards regarding remote QSCD certification:
 - CEN EN 419 241-2: Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing
 - CEN EN 419 221-5: Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services

Article 30

Certification of qualified electronic signature creation devices

1. Conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States.
2. Member States shall notify to the Commission the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.
3. The certification referred to in paragraph 1 shall be based on one of the following:
 - (a) a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in the list established in accordance with the second subparagraph; or
 - (b) a process other than the process referred to in point (a), provided that it uses comparable security levels and provided that the public or private body referred to in paragraph 1 notifies that process to the Commission. That process may be used only in the absence of standards referred to in point (a) or when a security evaluation process referred to in point (a) is ongoing.

The Commission shall, by means of implementing acts, establish a list of standards for the security assessment of information technology products referred to in point (a). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Auditing of Remote Trust Services – Tomorrow

- Creation of (qualified) electronic signatures / seals on behalf of the subject will be a qualified trust service in the future
 - Requirement for independent conformity assessment of such services
 - Notification and Initiation requirements according to eIDAS Article 21
 - ex-ante supervision by responsible supervisory body
 - Updated ETSI TS 119 612 v2.2.1 (TSL specification) specifies it as separate QTS
- Result:

Addition of this qualified trust service facilitates harmonization with regard to service provisioning

Contact



Matthias Wiedenhorst
Head of Certification
Division TSP

IT Infrastructure
+49 201 8999-536
m.wiedenhorst@tuvit.de

www.tuvit.de