DIGITALISERINGSSTYRELSEN

Public policy for qualified time-stamping

August 2023

Version 1.2

Contents

1. Introduction

1.1 Introduction

In some applications, it is necessary to determine that data existed at a given point in time. This applies e.g. in connection with storage of electronically signed data where it is important to be able to document that the electronic signature was generated at a point in time when the associated certificate was valid, i.e. had not expired or been revoked. This is solved by using a trust service that issues cryptographic time stamps where a hash value of data (including signed data) are linked with a point in time via an electronic seal.

The overall security of time stamps depend on the subordinate operation of the time stamping service. This time-stamp policy determines requirements for providers wanting to issue qualified time stamps, cf. eIDAS. Providers may choose to use alternative time-stamp policies if they comply with the requirements in [eIDAS] for trust service providers providing time stamps.

This document is created to meet the requirements in [ETSI EN 319 421]. Clause 2 to clause 7 follows the clause numbers from [ETSI EN 319 421]. Specific requirements related to qualified TSAs from [ETSI EN 319 421] clause 8 are integrated in clause 1 to clause 7 in this document.

Note that this English version is a courtesy translation, which might not be 100% accurate. In case of doubt, the Danish version should be regarded as the authoritative source.

1.2 Document name

This document named "Public policy for qualified time-stamping", abbreviated OPQT describes a public policy for issuance of qualified time stamps. The most recent version of this policy for issuance of time stamps is available at https://certifikat.gov.dk.

1.3 Policy administration

1.3.1 Organization administering the document

This policy is owned and maintained by the Danish Agency for Digital Government.

1.3.2 Contact person

Inquiries regarding this policy can be addressed to:

The Danish Agency for Digital Government

Landgreven 4

DK-1301 Copenhagen K

Telephone: +45 3392 5200

Email: digst@digst.dk

1.3.3 Policy approval procedure

This policy is approved by the Danish Agency for Digital Government following public consultation.

1.3.4 Publication

[REQ 1.3.4-01] Qualified trust service providers issuing time stamps under this policy shall publish the policy on their website together with the EU trust label for qualified trust services on a 24/7 basis and without access limitations.

1.4 Intellectual property rights

2. References

[eIDAS]	REGULATION (EU) No 910/2014 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
[ETSI EN 301 549]	ETSI EN 301 549 V2.1.2 - Accessibility requirements suitable for public procurement of ICT products and services in Europe
[ETSI EN 319 122]	ETSI EN 319 122-1 V1.2.1 and ETSI EN 319 122-2 V1.1.1 - Electronic Signatures and Infrastructures (ESI); CAdES digital signatures

[ETSI EN 319 401] ETSI EN 319 401 V2.3.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[ETSI EN 319 411-1] ETSI EN 319 411-1 V1.3.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[ETSI EN 319 411-2] ETSI EN 319 411-2 V2.4.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[ETSI EN 319 421] ETSI EN 319 421 V1.2.1 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamp

[ETSI EN 319 422] ETSI EN 319 422 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

[ETSI TS 119 312] ETSI TS 119 312 V1.4.2 - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[FIPS PUB 140-2] National Institute of Standards and Technology - Federal Information Processing Standard (140-2) - Security Requirements for Cryptographic Modules

[FIPS PUB 140-3] National Institute of Standards and Technology - Federal Information Processing Standard (140-3) - Security Requirements for Cryptographic Modules

[ISO/IEC 15408] Information technology -- Security techniques -- Evaluation criteria for IT security

[ISO/IEC 19790] Information technology -- Security techniques -- Security requirements for cryptographic modules

3. Definitions and acronyms

3.1 Definitions

Public key certificate: An electronic certificate specifying the subscriber's public key as well as additional information which uniquely links the public key to the identification of the subscriber. A public key certificate must be signed by a Certification Authority (CA) which thus confirms the validity of the certificate.

Time stamp: Data in electronic form that links other electronic data to a given point in time as proof that these data existed at the given point in time.

Time-stamping unit (TSU) See clause 4.2.

TSA practice statement: A specification of the principles and procedures used by a TSA when issuing certificates to comply with a related time-stamp policy. See also clause 4.5.

Time-stamp policy: A set of rules that sets out requirements for the issuance and use of time stamps or several specific contexts with common security requirements. This document is a time-stamp policy. See also clause 4.5.

Time-stamping authority (TSA) See clause 4.3.

3.2 Abbreviations

BCP	Business Continuity Plan
BTSP	Best Practice Time-Stamp Policy
CA	Certification Authority
ETSI	European Telecommunications Standards Institute
TSA	Time Stamping Authority
TSP	Trust Service Provider
TSU	Time Stamping Unit
UTC	Universal Time Coordinated

4. General concept description

4.1 General requirements for trust service providers issuing time-stamps

To ensure a uniform level of security for trust service providers, ETSI has published a number of standards that set out various requirements.

[ETSI EN 319 401] contains general requirements for trust service providers, whereas [ETSI EN 319 421] sets out specific requirements for trust service providers issuing electronic time-stamps.

This policy is a further specification of "best practices time-stamp policy (BTSP)" for TSAs that issue qualified electronic time-stamps, cf. [ETSI EN 319 421].

4.2 Time-stamping services

In this policy, the provision of a time-stamping service is broken down into the following service components:

- **Time-stamping unit:** This service component, TSU, generates and issues time-stamps. A TSA may have one or more TSUs to provide its service.
- **Time-stamping management:** This service component oversees and verifies that the time-stamping service is operated as specified in the TSA practice statement.

This division only serves to clarify the requirements through a classification and they are not to be considered as architectural requirements for an implementation.

4.3 Time-stamping authority (TSA)

Qualified trust service providers issuing qualified electronic time-stamps, cf. [eIDAS] article 41 and article 42, are referred to as time-stamping authority (TSA).

The TSA may use subcontractors in connection with the service provided, but it is always the overall responsibility of the TSA to ensure that the requirements of this policy are met.

4.4 Subscriber

A subscriber is a natural or legal person which, subject to agreement with the TSA, may request qualified electronic time-stamps.

If the subscriber is a natural person, the subscriber is directly responsible for complying with the terms and conditions for the use of the service.

If the subscriber is a legal person, the subscriber is responsible for complying with the terms and conditions for its end-users' use of the service. This means that it is the duty of the subscriber to enforce compliance with terms and conditions for the use of the service towards its end-users. In this context, end-users include natural persons working under an instruction from the subscriber as well as systems with the subscriber that use the TSA's services.

4.5 Time-stamping policy and TSA practice statement

A time-stamping policy is a Trust Service Policy as defined in [ETSI EN 319 401] that sets out requirements for trust service providers issuing electronic time-stamps.

A TSA practice statement is a Trust Service Practice Statement as defined in [ETSI EN 319 401] which describes how a given TSA has implemented the requirements for one or more time-stamping policies.

5. Introduction to time-stamping policy and general requirements

5.1 General requirement

[REQ 5.1-01] TSAs issuing electronic time-stamps under this policy shall be qualified trust service providers, cf. [eIDAS], and issue time-stamps with an accuracy of 1 second.

[REQ 5.1-02] If an accuracy of better than 1 second is provided by the TSA, then the accuracy shall be indicated in the published part of the TSA practice statement and in the issued time-stamps.

5.2 Identification

[REQ 5.2-01] Time-stamps issued under this policy shall include the 'object identifier' value:

itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)

in the 'policy' field in a time-stamp request, unless the response is an error message, whereby the TSA claims conformance with the BTSP, cf. [ETSI EN 319 421].

5.3 Infrastructure and applicability

5.3.1 Best practices time-stamp policy

[REQ 5.3.1-01] This policy is aimed at meeting the requirements of time-stamp for long term validity of electronic signatures (e.g. as defined in [ETSI EN 319 122]) but is generally applicable to any use which has a requirement for security and quality of requested electronic time-stamps where allowed by TSA terms and conditions.

[REQ 5.3.1-02] This policy may be used by qualified TSAs which provide time-stamping as an open service and/or to a closed group of subscribers.

6. Policies and implementation

6.1 Risk assessment

[REQ 6.1-01] The TSA shall carry out a risk assessment to identify, analyse and evaluate business and technical risks.

[REQ 6.1-02] The TSA shall implement the appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk.

[REQ 6.1-03] The TSA shall determine and document all security requirements and operational procedures that are necessary to comply with this policy. The documentation must be part of the TSA practice statement, cf. clause 6.2.

[REQ 6.1-04] The risk assessment shall be reviewed and revised at least once a year.

[REQ 6.1-05] The TSA's management shall approve the risk assessment and accept the residual risk identified.

6.2 TSA practice statement

[REQ 6.2-01] The TSA shall prepare a TSA practice statement addressing all requirements of this policy. This TSA practice statement shall include all external organizations supporting the TSA's services and shall conform to this policy. The TSA practice statement may be divided into a public and private part, with the public part of the TSA practice statement being published.

[REQ 6.2-01A] When the VA makes use of other parties, including trust service component providers through subcontracting, outsourcing or other third party arrangements, the CA shall maintain the overall responsibility for meeting the requirements of this policy.

This includes

> **[REQ 6.2-01B]** When the VA makes use of a trust service component provided by another party, the VA shall ensure that the use of the component interface meets the requirements as specified by the provider.
>
> **[REQ 6.2-01C]** When the VA makes use of a trust service component provided by another party, the VA shall ensure the necessary security and functionality required for compliance with this policy.

[REQ 6.2-02] The management of the TSA shall be responsible for and approve the overall TSA practice statement and ensure correct implementation, including that the practice statement is conformant with this policy and is communicated to relevant employees and partners.

[REQ 6.2-03] The TSA shall make the public part of the TSA's applicable practice statement available on the TSA’s website on a 24/7 basis.

[REQ 6.2-04] The TSA practice statement shall be reviewed and revised on a regular basis and at least once a year. The responsibility for maintaining the TSA practice statement must be determined and documented. Changes in the TSA practice statement must be documented.

[REQ 6.2-05] In the TSA practice statement, the TSA shall specify provisions upon termination of the service. These must at a minimum include information on who will be notified upon termination and who will take over customers and users, if these types of agreements exist.

[REQ 6.2-06] The TSA practice statement shall at least specify

a) the hashing algorithm (or algorithms) used to represent the datum being time-stamped;

b) the accuracy of the time in the time-stamps with respect to UTC;

c) synchronization source or sources;

d) any limitations on the use of the time-stamping service;

e) the subscriber's obligations, if any;

f) the relying party's obligations;

g) information on how to verify the time-stamp such that the relying party is considered to "reasonably rely" on the time-stamp (see clause 6.6) and any possible limitations on the validity period; and

h) any claim to meet the requirements on time-stamping services under national or European law.

Note: In relation to item h) above, the TSA shall in its practice statement at least specify that the time-stamping service is a qualified trust service, cf. eIDAS.

[REQ 6.2-07] The TSA practice statement should specify information on availability of the TSA's service.

6.3 Terms and conditions

[KRAV 6.3-01] The TSA shall make the terms and conditions regarding its services available to all subscribers and relying parties.

[REQ 6.3-02] The terms and conditions shall include:

a) a description of the service, including what policies are covered by the service;

b) any limitations on the use of the service;

c) the subscriber's obligations;

d) information for parties relying on the trust service;

e) the period of time during which event logs are retained;

f) limitations of liability;

g) limitations on the use of service, including the TSA's limitation of liability in terms of wrong use of the service;

h) the applicable legal system;

i) dispute procedures;

j) that the TSA is a qualified trust service, cf. the eIDAS Regulation;

k) the TSA's contact information; and

l) any undertaking regarding availability.

[REQ 6.3-03] Subscribers and parties relying on the trust service shall be informed of precise terms and conditions, including the items listed above, before entering into a contractual relationship.

[REQ 6.3-04] Terms and conditions shall be made available through a durable means of communication.

[KRAV-6.3-05] Terms and conditions shall be available in a readily understandable language.

[REQ 6.3-06] Terms and conditions may be transmitted electronically.

6.4 Information security policy

[REQ 6.4-01] The TSA shall live up to the requirements in the information security standard ISO 27001 and be able to document compliance through e.g. certification.

[REQ 6.4-02] The TSA shall define an information security policy which is approved by management and which sets out the organization's approach to managing its information security.

[REQ 6.4-03] Changes to the information security policy shall be communicated to third parties, where applicable. This may include subscribers, conformity assessment body, supervisory body and other authorities.

[REQ 6.4-04] A TSA's information security policy shall be documented, implemented and maintained, including the security controls and operating procedures for the TSA's facilities, systems and information assets providing the services.

[REQ 6.4-05] The TSA shall publish and communicate the information security policy to all employees who are impacted by it, including employees at subcontractors performing work for the TSA.

Note: Employees working for the TSA's organization but who do not carry out work related to its roles as TSA are not covered by the above requirement.

[REQ 6.4-06] The TSA shall retain overall responsibility for conformance with the procedures prescribed in its information security policy, even when the TSA's functionality is undertaken by outsourcers.

[REQ 6.4-07] The TSA shall set out and ensure efficient implementation of relevant controls at the subcontractors.

[REQ 6.4-08] The TSA's information security policy and inventory of assets for information security shall be reviewed at annually and if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

[REQ 6.4-09] Any changes that may impact on the level of security provided shall be approved by the TSA's management.

[REQ 6.4-10] The configuration of the TSA's systems shall be checked at fixed intervals and at least once a year for changes which violate the TSA's information security policy.

[REQ 6.4-11] The maximum interval between two of the above checks shall be documented in the TSA practice statement.

6.5 TSA obligations

6.5.1 General obligations

[REQ 6.5.1-01] The TSA shall adhere to any additional obligations indicated in the time-stamp either directly or incorporated by reference.

Note: If the TSA enters elements in time-stamps, e.g. in the form of extensions, and these contain implicit or explicit obligations, such obligations must be adhered to, even if they are not indicated in this policy.

6.5.2 TSA obligations towards subscribers

[REQ 6.5.2-01] The present document places no specific obligations on the subscriber. All TSA specific requirements for the subscriber shall be stated in the TSA's terms and conditions.

6.6 Information for relying parties

[REQ 6.6-01] The terms and conditions for relying parties shall at least include the following obligations on the relying party, before a time-stamp is accepted:

a) the relying party shall verify that the time-stamp is correctly signed and that the private key used to sign the time-stamp has not been marked as compromised until the time of the verification;

b) the relying party shall take into account any limitations on the usage of the time-stamp indicated by the time-stamp policy; and

c) the relying party shall take into account any other precautions prescribed in agreements or elsewhere.

Note: Conformance with item a) in the above requirements can be ensured by verifying that the certificate has been correctly signed and that the key used is valid with regard to validity period and that the certificate serial number is not found in the relevant updated certificate revocation list.

7. TSA management and operation

7.1 Introduction

[REQ 7.1-01] The TSA shall have a system or systems for quality and information security management appropriate for the time-stamping services it is providing, cf. REQ 6.4-01.

7.2 Internal organization

[REQ 7.2-01] The TSA shall be a legal entity.

[REQ 7.2-02] The TSA organization shall be reliable and non-discriminatory.

[REQ 7.2-03] The TSA should make its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the TSA's terms and conditions.

Note: It is possible for the TSA to limit the field of operation for its services, and the TSA should publish its field of operation in its practice statement. For example, the TSA may state that time-stamps are issued to one specific subscriber only, but that time stamps from the TSA can be verified by all relying parties.

[REQ 7.2-04] The TSA shall maintain sufficient financial resources and/or obtain appropriate liability insurance in accordance with applicable law, including eIDAS, to cover liabilities arising from its operations and/or activities.

[REQ 7.2-05] If the TSA is a private enterprise, the TSA shall obtain and maintain liability insurance, cf. REQ 7.2-04. Such insurance shall as a minimum provide a coverage of DKK 25 million per year.

[REQ 7.2-06] The TSA shall have the financial stability and resources required to operate in conformity with this policy.

Note: The above requirements must be assessed in respect of the context in which the TSA operates, including but not limited to the number of customers and the financial risk undertaken by the TSA in respect of the issued time-stamps.

[REQ 7.2-07] The TSA shall have policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters.

[REQ 7.2-08] The TSA shall have a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.

[REQ 7.2-09] Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the TSA's assets.

7.3 Personnel controls

[REQ 7.3-01] The TSA shall ensure that employees and contractors support the trustworthiness of the TSA's operations.

[REQ 7.3-02] The TSA shall employ a sufficient number of personnel having the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide time-stamping services.

[REQ 7.3-03] The TSA's personnel, including personnel of any subcontractors, should be able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of the two.

[REQ 7.3-04] The TSA shall employ staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding information security and personal data protection rules as appropriate for the offered services and the job function.

[REQ 7.3-05] The above training requirements should encompass regular (at least every 12 months) updates concerning new threats and current security practices.

[REQ 7.3-06] Appropriate disciplinary sanctions shall be used for personnel who violate the TSA's policies or procedures.

[REQ 7.3-07] Security roles and responsibilities, as specified in the TSA's information security policy, shall be documented in job descriptions or in documents available to all concerned personnel.

[REQ 7.3-08] Trusted roles, on which the security of the TSA's operation is dependent, shall be clearly identified and approved by the management.

[REQ 7.3-09] Trusted roles shall be approved by the management and accepted by the person to fulfil the role.

[REQ 7.3-10] The TSA's personnel (both temporary and permanent) shall have job descriptions defined from the view point of roles fulfilled with segregation of duties and least privilege, the sensitivity of data that can be accessed, background screening and employee training and awareness.

[REQ 7.3-11] Where appropriate, job descriptions shall differentiate between general functions and the TSA's specific functions. These should include skills and experience requirements.

[REQ 7.3-12] Personnel shall exercise administrative and management procedures and processes that are in line with the TSA's information security management procedures.

[REQ 7.3-13] Managerial personnel shall have experience or training in relation to operation of the TSA, knowledge of compliance controls for personnel with security responsibility and experience with information security and risk assessment that is sufficient to be able to perform management functions for the TSA.

[REQ 7.3-14] All TSA's personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSA's operations.

[REQ 7.3-15] Trusted roles shall include roles that involve the following responsibilities:

a) Security Officers: Overall responsibility for administering the implementation of the security practices.

b) System Administrators: Authorized to install, configure and maintain the TSA's critical systems for service management, including system restoration.

c) System Operators: Responsible for operating the TSA's critical systems on a day-to-day basis. Authorized to perform system backup.

d) System Auditors: Authorized to view archives and audit logs of the TSA's critical systems.

[REQ 7.3-16] Personnel that are to access or configure privileges for trusted roles shall be formally approved by a security manager at the senior management level.

[REQ 7.3-17] Personnel shall not have access to the trusted functions until the necessary checks are completed.

7.4 Asset management

7.4.1 General requirements

[REQ 7.4.1-01] The TSA shall maintain an inventory of its assets, including information assets. All information assets shall be classified according to the TSA's risk assessment, and the TSA shall ensure adequate protection of all assets.

7.4.2 Media handling

[REQ 7.4.2-01] All media in the TSA's operating system shall be handled securely in accordance with its classification, and

- media containing sensitive data shall be securely disposed of when no longer required;
- media shall be protected from damage, theft, unauthorized access and obsolescence; and

- sensitive data shall be protected against unauthorized access through re-used storage objects.

7.5 Access control

[REQ 7.5-01] The TSA shall implement effective access control that protects against unauthorized physical or logical access to the TSA's systems.

In particular:

- **[REQ 7.5-02]** The TSA shall implement controls (e.g. firewalls) to protect the TSA's internal network from unauthorized access, including access by subscribers and relying parties.
- **[REQ 7.5-03]** Firewalls shall also be configured to prevent all protocols and accesses not required for the operation of the TSA.
- **[REQ 7.5-04]** The TSA shall implement an efficient user administration, including administer user access of operators, administrators and system auditors applying the principle of "least privileges".
- **[REQ 7.5-05]** User accounts shall be checked regularly to ensure that the users at all times only have the necessary rights, cf. access control policy.
- **[REQ 7.5-06]** Access to information and application system functions shall be restricted in accordance with the access control policy.
- **[REQ 7.5-07]** The TSA's operating systems shall provide sufficient computer security controls for the separation of trusted roles identified in the TSA practice statement, including the separation of security administration and operational roles. Particularly, use of system utility programs shall be restricted and controlled to what is necessary.
- **[REQ 7.5-08]** The TSA's personnel shall be identified and authenticated before using critical systems and applications.
- **[REQ 7.5-09]** The TSA's personnel shall be accountable for their activities., e.g. through efficient event logging.

7.6 Cryptographic controls

7.6.1 General controls

[REQ 7.6.1-01] The TSA shall implement secure handling of cryptographic keys and cryptographic devices. The handling shall cover the full lifecycle of keys and devices.

7.6.2 TSU key generation

a) **[REQ 7.6.2-01]** The generation of the TSU's private signing keys shall be undertaken in a physically secured environment (as per clause 7.8) by personnel in trusted roles (as per clause 7.3) under dual control. The personnel authorized to carry out this function shall be limited to those required to do so under the TSA's practice statement.

b) **[REQ 7.6.2-02]** The generation of the TSU's private signing key shall be carried out within a cryptographic module which either:

   i) is a trustworthy system which is assured to EAL 4 or higher in accordance with [ISO/IEC 15408] or equivalent national or internationally recognized IT security evaluation criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures; or

   ii) meets the requirements of [ISO/IEC 19790], [FIPS PUB 140-2] level 3 or [FIPS 140-3] level 3.

   The cryptographic device should be as specified in i) above.

c) **[REQ 7.6.2-03]** The TSU key generation algorithm, the signing key length and signature algorithm used for signing time-stamps shall be as specified in [ETSI TS 119 312]. The recommendation for choice of cryptographic algorithms and key lengths defined in [ETSI TS 119 312] may be superseded by national recommendations.

d) **[REQ 7.6.2-04]** A TSU's signing key should not be imported into different cryptographic modules.

e) **[REQ 7.6.2-05]** If the same signing key is used in different cryptographic modules, the key shall be associated with the same public key certificate into all the different cryptographic modules.

f) **[REQ 7.6.2-06]** A TSU shall have a single private time-stamp signing key active at a time.

7.6.3 TSU private key protection

[REQ 7.6.3-01] Integrity and confidentiality of the TSU private keys shall be maintained.

In particular:

a) **[REQ 7.6.3-02]** The TSU private signing key shall be held and used within a cryptographic module which:

   i) is a trustworthy system which is assured to EAL 4 or higher in accordance with [ISO/IEC 15408] or equivalent national or internationally recognized IT security evaluation criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures; or

ii) meets the requirements of [ISO/IEC 19790], [FIPS PUB 140-2] level 3 or [FIPS PUB 140-3] level 3.

The cryptographic device should be as specified in i).

b) **[REQ 7.6.3-03]** If TSU private keys are backed up, they shall be copied, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see clause 7.8). The personnel authorized to carry out this function shall be limited to those required to do so under the TSA's practice statement.

c) **[REQ 7.6.3-04]** Any backup copies of the TSU private keys shall at all times be protected to at least the same level as the cryptographic module on which the key is generated and used to ensure its integrity and confidentiality.

7.6.4 TSU certificate

[REQ 7.6.4-01] The TSA shall guarantee the integrity and authenticity of the TSU signature verification (public) keys with at least the following particular requirements:

a) **[REQ 7.6.4-02]** TSU signature verification (public) keys shall be made available to relying parties in a certificate.

b) **[REQ 7.6.4-03]** The TSU certificate shall be issued by a qualified CA operating under [ETSI EN 319 411-1] and [ETSI EN 319 411-2].

c) **[REQ 7.6.4-04]** The TSU shall not issue time-stamp before its certificate is loaded into the TSU or its cryptographic device.

[REQ 7.6.4-05] When obtaining a TSU certificate, the TSA should verify that this certificate has been correctly signed by the CA (including verification of the certificate chain to a recognised qualified CA).

7.6.5 Rekeying TSU's key

[REQ 7.6.5-01] The validity period of the TSU's certificate must not be longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose (see clause 7.6.2c)).

7.6.6 Life cycle management of signing cryptographic hardware

[REQ 7.6.6-01] Cryptographic hardware used in connection with time-stamping shall be protected throughout its life cycle. AS a minimum, the following requirements must be met:

a) **[REQ 7.6.6-02]** Cryptographic hardware shall not be tampered with during shipment.

b) **[REQ 7.6.6-03]** Cryptographic hardware shall not be tampered with shall not be tampered with when and while stored.

c) **[REQ 7.6.6-04]** Installation, activation and duplication of the TSU's signing keys in cryptographic hardware shall be done only by personnel in trusted roles using, at least, dual control in a physically secured environment (see clause 7.8).

d) **[REQ 7.6.6-05]** TSU signing keys stored on TSU cryptographic hardware shall be erased in such a way that it is practically impossible to recover them when the cryptographic hardware is no longer to be used for signing using TSU signing keys.

7.6.7 Termination of TSU private keys

[REQ 7.6.7-01] The TSA shall define an expiration date for TSU's signing keys.

Note: The expiration date for the TSU signing key is not the same as the expiration date for the associated certificate.

[REQ 7.6.7-02] The expiration date for TSU's signing key shall not be longer than the end of validity of the associated certificate.

[REQ 7.6.7-03] The expiration date should take into account the lifetime defined in 'recommended key sizes versus time' from ETSI [ETSI TS 119 312].

[REQ 7.6.7-04] In order to be able to verify during a sufficient lapse of time the validity of the time-stamps, the validity of the TSU's signing key should be shorter than the certificate validity.

For example, signing keys may be valid for 1 year if the associated certificate is valid for 4 years.

[REQ 7.6.7-05] The expiration date for the TSU signing keys may be defined when the TSU cryptographic module is initialized or by setting a 'privateKeyUsagePeriod' extension within the TSU's certificate.

[REQ 7.6.7-06] The TSU signing keys shall not be used beyond the end of their validity period.

In particular:

a) **[REQ 7.6.7-07]** Operational or technical procedures shall be in place to ensure that a new key is put in place when a TSU signing key expires.

b) **[REQ 7.6.7-08]** The TSU signing keys, or any key part, including any copies, shall be destroyed such that the keys cannot be retrieved.

7.7 Time-stamping

7.7.1 Time stamp issuance

[REQ 7.7.1-01] Time-stamps shall conform to the time-stamp profile as defined in ETSI EN 319 422.

[REQ 7.7.1-02] In particular, time-stamps shall be marked as qualified time-stamps by including one qcStatements extension with the value "`esi4-qtstStatement-1`", cf. [ETSI EN 319 422] clause 9.1.

[REQ 7.7.1-03] The time-stamps shall be issued securely and shall include the correct time.

In particular:

a) **[REQ 7.7.1-04]** The time values the TSU uses in the time-stamp shall be traceable to at least one of the real time values distributed by a UTC(k) laboratory.

b) **[REQ 7.7.1-05]** The time included in the time-stamp shall be synchronized with UTC within the accuracy defined in this policy and, if present, within the accuracy defined in the time-stamp itself.

c) **[REQ 7.7.1-06]** If the TSA's clock is detected (see REQ 7.7.2-04) as being out of the stated accuracy (see clause 7.7.1-04) then time-stamps shall not be issued.

d) **[REQ 7.7.1-07]** The time-stamp shall be signed using a key generated exclusively for this purpose.

e) **[REQ 7.7.1-08]** The time-stamp generation system shall reject any attempt to issue time-stamps if the TSU's signing key has expired.

[REQ 7.7.1-09] TSUs issuing qualified time-stamps, cf. [eIDAS] under this policy, must not issue non-qualified time-stamps.

[REQ 7.7.1-10] TSAs issuing qualified time-stamps, cf. [eIDAS], under this policy from a TSU while also issuing non-qualified time-stamps from other TSUs shall use another subject name (subject distinguishedName) in certificates for TSUs issuing non-qualified time-stamps than in the certificate for the TSU issuing qualified time-stamps under this policy.

[REQ 7.7.1-11] The above non-qualified TSUs shall be accessed via other service interfaces for TSUs operating under this policy.

7.7.2 Clock synchronization with UTC

[REQ 7.7.2-01] The TSU clock shall be synchronized with UTC as defined in Recommendation ITU-R TF.460-6 within the declared accuracy with at least the following particular requirements:

a) **[REQ 7.7.2-02]** The calibration of the TSU clocks shall be maintained such that the clocks do not drift outside the declared accuracy.

b) **[REQ 7.7.2-03]** The declared accuracy shall be of 1 second or better.

c) **[REQ 7.7.2-04]** The TSU clocks shall be protected against threats which could result in an undetected change to the clock that takes it outside its calibration.

Note: Threats can include tampering by unauthorized personnel, radio or electrical shocks.

d) **[REQ 7.7.2-05]** The TSA shall detect if the time that would be indicated in a time-stamp drifts or jumps out of synchronization with UTC.

e) **[REQ 7.7.2-06]** If it is detected that the time indicated in a time-stamp drifts or jumps out of synchronization with UTC, the TSU shall stop time-stamp issuance.

f) **[REQ 7.7.2-07]** The clock synchronization shall be maintained when a leap second occurs as notified by the appropriate body. The change to take account of the leap second shall occur during the last minute of the day when the leap second is scheduled to occur. A record shall be maintained of the exact time (within the declared accuracy) when this change occurred.

7.8 Physical and environmental security

[REQ 7.8-01] The TSA shall control physical access to components of the TSA's systems based on the classification policy. This includes minimizing risks related to physical security.

[REQ 7.8-02] The TSA shall ensure that access to facilities is limited to authorized individuals.

[REQ 7.8-03] The TSA shall implement effective protection against

- loss, damage or compromise of assets and interruption to business activities; and
- compromise or theft of information and information processing facilities.

[REQ 7.8-04] Components that are critical for the secure operation of the TSA shall be located in a protected security perimeter with physical protection against intrusion, controls on access through the security perimeter and alarms to detect intrusion.

The following must be observed:

a) **[REQ 7.8-05]** Access controls shall be applied to the cryptographic module to meet the requirements of security of cryptographic modules as identified in clause 7.6.

b) The following additional controls apply to time-stamping management:
   - **[REQ 7.8-06]** The time-stamping management facilities shall be operated in an environment which physically and logically protects the services from compromise through unauthorized access to systems or data.

- **[REQ 7.8-07]** Every entry to the physically secure area shall be subject to independent oversight and non-authorized person shall be accompanied by an authorized person whilst in the secure area. Every entry and exit shall be logged.
- **[REQ 7.8-08]** Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the time-stamping management. Any parts of the premises shared with other organizations shall be outside this perimeter.
- **[REQ 7.8-09]** Physical and environmental security controls shall protect the facility that houses system resources, the system resources themselves, and the facilities used to support their operation. The TSA's physical and environmental security policy for systems concerned with time-stamping management shall address as a minimum the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering. Recovery plans shall be in place following operational disasters (disaster recovery).
- **[REQ 7.8-10]** Controls shall protect against equipment, information, media and software relating to the time-stamping services being taken off-site without authorization.

[REQ 7.8-11] Other functions may be supported within the same secured area provided that the access is limited to authorized personnel.

7.9 Operation security

[REQ 7.9-01] The TSA shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

[REQ 7.9-02] The TSA shall ensure that, prior to any system development (e.g. undertaken by the TSA or on behalf of the TSA), a plan approved by management is provided to ensure that security is built into the systems. The plan shall include an analysis of security requirements being met in order to maintain an adequate level of security.

[REQ 7.9-03] The TSA shall implement documented processes for release and change management of software, hardware and configuration changes. The TSA shall have documented processes for security update of proprietary and standard software and firmware. The processes shall include documentation of the changes.

[REQ 7.9-04] The integrity of TSA’s systems and information shall be protected against viruses, malicious and unauthorized software, and the TSA shall specify and apply procedures for ensuring that:

- security patches are applied within a reasonable time after they come available;
- security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and
- the reasons for not applying any security patches are documented.

[REQ 7.9-05] Media used within the TSA's systems shall be securely handled according to the classification and to protect media from damage, theft, unauthorized access and obsolescence.

[REQ 7.9-06] The TSA shall have media management procedures in place to protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

[REQ 7.9-07] The TSA shall establish and implement procedures for all trusted and administrative roles that may impact on the TSA's security and operations.

[REQ 7.9-08] The TSA shall plan and monitor future capacity requirements made to ensure that adequate processing power and storage are available at all times.

7.10 Network security

[REQ 7.10-01] The TSA shall protect its network and systems from attack and unauthorized access.

In particular:

- **[REQ 7.10-02]** The TSA shall segment its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between critical systems and services.
- **[REQ 7.10-03]** The TSA shall apply the same security controls to all systems co-located in the same zone.
- **[REQ 7.10-04]** The TSA shall restrict access and communications between zones to those necessary for the operation of the TSA.
- **[REQ 7.10-05]** The TSA shall explicitly forbid or deactivate not needed connections and services.
- **[REQ 7.10-06]** The TSA shall also configure all TSU systems by removing or disabling all accounts, applications, services, and ports that are not used in the TSU's operations.
- **[REQ 7.10-07]** The TSA shall review the established network and firewall rules set on a regular basis.
- **[REQ 7.10-08]** The TSA shall operate, maintain and protect all TSU systems in secure zones or high-security zones.
- **[REQ 7.10-09]** The TSA shall place particularly critical systems in high-security zones.

- **[REQ 7.10-10]** The TSA shall separate dedicated networks for administration of IT systems and the TSA's operational network.
- **[REQ 7.10-11]** The TSA shall not use systems used for administration of the security policy implementation for other purposes.
- **[REQ 7.10-12]** The TSA shall separate the production systems from systems used in development and testing.
- **[REQ 7.10-13]** The TSA shall establish communication between critical systems only through trusted channels that are physically or logically distinct from other communication channels and provide confidentiality, integrity and authenticity between the systems.
- **[REQ 7.10-14]** If a high level of availability of external access to the trust service is required, the external network connection shall be redundant.
- **[REQ 7.10-15]** At least once every quarter the TSA shall perform a vulnerability scan from external and internal IP addresses. The vulnerability scans shall be performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report. Scans shall be documented.
- **[REQ 7.10-16]** At least once a year, after set up and in case of significant infrastructure or application upgrades or modifications the TSA shall perform a penetration test. The penetration test shall be performed by a person or entity with the skills, tools, code of ethics and independence necessary to provide a reliable report. The penetration test shall be documented.
- **[REQ 7.10-17]** The TSA shall ensure that only trusted roles are granted access to secure zones and high-security zones.

7.11 Incident management

[REQ 7.11-01] System activities concerning access to IT systems, use of IT systems, and service requests shall be monitored.

In particular:

- **[REQ 7.11-02]** Monitoring activities must take account of the sensitivity of any information collected or analysed.
- **[REQ 7.11-03]** Abnormal system activities that indicate a potential security violation, including intrusion into the TSA's network, shall be detected and reported as alarms.
- **[REQ 7.11-04]** The TSA shall monitor the following events:
    a) start-up and shutdown of the log functions; and
    b) availability and utilization of needed services with the TSA's network.

- **[REQ 7.11-05]** The TSA shall act in a timely and co-ordinated manner in order to respond quickly to security events and to limit the impact of breaches of security.
- **[REQ 7.11-06]** The TSA shall appoint trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the TSA's procedures.
- **[REQ 7.11-07]** The TSA shall have procedures and emergency preparedness that ensure notification of a security event or loss of integrity to relevant parties, cf. applicable regulations, for example the data protection authorities and/or the eIDAS supervisory body at the latest 24 hours after the event has been identified.
- **[REQ 7.11-08]** Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person, the TSA shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.
- **[REQ 7.11-09]** The TSA's systems shall be monitored including the monitoring or regular review of audit logs to identify evidence of malicious activity implementing automatic mechanisms to process the audit logs and alert personnel of possible critical security events.
- **[REQ 7.11-10]** The TSA shall address any critical vulnerability not previously addressed by the TSA within a period of 48 hours after its discovery.
- **[REQ 7.11-11]** For any vulnerability, given the potential impact, the TSA shall either:
  a) create and implement a plan to mitigate the vulnerability; or
  b) document the factual basis for the TSA's determination that the vulnerability does not require remediation.
- **[REQ 7.11-12]** Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.

7.12 Collection of evidence

[REQ 7.12-01] The TSA shall record and keep accessible for an appropriate period of time, including after the activities of the TSA have ceased, all relevant information concerning data issued and received by the TSA, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.

In particular:

- **[REQ 7.12-02]** The TSA shall maintain the confidentiality and integrity of archived records concerning operation of its services.

- **[REQ 7.12-03]** The TSA shall ensure the completeness, confidentiality and integrity of archived records concerning the operation of its services in accordance with disclosed business practices.
- **[REQ 7.12-04]** Records, including audit log, shall be made available if required for the purposes of providing evidence in legal proceedings.
- **[REQ 7.12-05]** The precise time of significant environmental, key management and clock synchronization events shall be recorded.
- **[REQ 7.12-06]** The time used to record events as required in the audit log shall be synchronized with UTC at least once a day.
- **[REQ 7.12-07]** Records concerning services shall be held for a period of time as appropriate for providing necessary legal evidence and as notified in the TSA's terms and conditions.
- **[REQ 7.12-08]** The events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.

TSU key management

a) **[REQ 7.12-09]** Records concerning all events relating to the life-cycle of TSU keys shall be logged.

b) **[REQ 7.12-10]** Records concerning all events relating to the life-cycle of TSU certificates (if appropriate) shall be logged.

Clock synchronization

c) **[REQ 7.12-11]** Records concerning all events relating to synchronization of a TSU's clock to UTC shall be logged. This shall include information concerning normal re-calibration or synchronization of clocks used in time-stamping.

d) **[REQ 7.12-12]** Records concerning all events relating to detection of loss of synchronization shall be logged.

7.13 Business Continuity Plan

[REQ 7.13-01] The TSA shall define, test and maintain a Business Continuity Plan (BCP) to enact in case of a disaster.

[REQ 7.13-02] In the event of a disaster, including compromise of one of the TSA’s private signing keys, operations shall be restored within the delay established in the continuity plan, having addressed any cause for the disaster with appropriate remediation measures.

In particular:

a) **[REQ 7.13-03]** The TSA's disaster recovery plan shall address the compromise or suspected compromise of the TSU's private signing keys or loss of calibration of a TSU clock, which may have affected time-stamps which have been issued.

b) **[REQ 7.13.-04]** In the case of a compromise, or suspected compromise or loss of calibration when issuing time-stamp, the TSA shall make available to all subscribers and relying parties a description of the compromise that occurred.

c) **[REQ 7.13-05]** In the case of compromise to a TSU's operation, suspected compromise or loss of calibration, the TSU must not issue time-stamps until steps are taken to recover from the compromise.

d) **[REQ 7.13-06]** In case of major compromise of the TSA's operation or loss of calibration, the TSA shall make available to all subscribers and relying parties a description of the incident. Such description shall provide information that allows identifying the time-stamps which may have been affected, unless this breaches the privacy of the TSAs users or the security of the TSA services.

7.14 TSA termination and termination plans

[REQ 7.14-01] Potential disruptions to subscribers and relying parties shall be minimized as a result of the cessation of the TSA's services, and in particular continued maintenance of information required to verify the correctness of trust services shall be provided.

In particular:

- **[REQ 7.14-02]** The TSA shall have an up-to-date termination plan.

  Before the TSA terminates its services, at least the following procedures apply:

  a) **[REQ 7.14-03]** Before the TSA terminates its services, the TSA shall inform the following of the termination: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties, TSPs and relevant authorities such as supervisory bodies.
  b) **[REQ 7.14-04]** Before the TSA terminates its services, the TSA shall make the information of the termination available to other relying parties.
  c) **[REQ 7.14-05]** Before the TSA terminates its services, the TSA shall terminate authorization of all subcontractors to act on behalf of the TSA in carrying out any functions relating to the process of issuing time-stamps.
  d) **[REQ 7.14-06]** Before the TSA terminates its services, the TSA shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSA for a reasonable period, unless it can be demonstrated that the TSA does not hold any such information.

e) **[REQ 7.14-07]** Before the TSA terminates its services, the TSA's private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.
f) **[REQ 7.14-08]** Where possible the TSA should make arrangements to transfer provision of trust services for its existing customers to another TSA.

- **[REQ 7.14-09]** When the TSA terminates its services, the TSA shall maintain its obligations to make available its public keys to relying parties for a reasonable period or transfer such obligations to another reliable party.
- **[REQ 7.14-10]** When the TSA terminates its services, the TSA shall revoke all non-expired TSU's certificates.
- **[REQ 7.14-11]** Where the TSA is a privately held organization or a natural person, the TSA shall provide an irrevocable demand guarantee or the like with an approved institute to secure payment of its financial obligations in accordance with REQ 7.14-1 to REQ 7.14-10.
- **[REQ 7.14-12]** The TSA shall state in its practice statement the provisions made for termination of service. This shall include:
  a) information about the affected entities to be notified; and
  b) who will take over customers and users, where such form of agreement is available.

7.15 Compliance

[REQ 7.15-01] The TSA shall ensure that it operates in a legal and trustworthy manner as a qualified trust service that issues time-stamps:

In particular:

- **[REQ 7.15-02]** The TSA shall provide evidence on how it meets the applicable legal requirements. Including, in particular, eIDAS' regulation of qualified trust services, including any standards specified by the Commission, cf. [eIDAS] article 19 4.a).
- **[REQ 7.15-03]** Services and end user products provided by the TSA shall be made accessible for persons with disabilities, where feasible and applicable standards on accessibility such as ETSI EN 301 549 should be taken into account.
- **[REQ 7.15-04]** Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Annex A

The compliance with requirements for qualified time-stamps of this policy as set out in [ETSI EN 319 401] as well as [ETSI EN 319 421] and [ETSI EN 319 422].

OPQT	ETSI EN 319 401	ETSI EN 319 421 + ETSI EN 319 422
REQ 1.3.4-01		
REQ 5.1-01		
REQ 5.1-02		OVR-5.1-03
REQ 5.2-01		OVR-5.2-01
REQ 5.3.1-01		ETSI EN 319 421 clause 5.3.1
REQ 5.3.1-02		OVR-5.3-01
REQ 6.1-01	REQ-5-01	
REQ 6.1-02	REQ-5-02	
REQ 6.1-03	REQ-5-03	
REQ 6.1-04	REQ-5-04	
REQ 6.1-05	REQ-5-05	
REQ 6.2-01	REQ-6.1-01 REQ-6.1-03A REQ-6.1-04 REQ-6.1-05A	
REQ 6.2-01A	REQ-7.1.1-08	
REQ 6.2-01B	REQ-7.1.1-09	
REQ 6.2-01C	REQ-7.1.1-10	
REQ 6.2-02	REQ-6.1-02 REQ-6.1-06 REQ-6.1-07	

REQ 6.2-03	REQ-6.1-02 REQ-6.1-10	
REQ 6.2-04	REQ-6.1-08 REQ-6.1-09A	
REQ 6.2-05	REQ-6.1-11 REQ-7.12-10	
REQ 6.2-06		OVR-6.2-01
REQ 6.2-07		OVR-6.2-03
REQ 6.3-01	REQ-6.2-01	
REQ 6.3-02	REQ-6.2-02	
REQ 6.3-03	REQ-6.2-03	
REQ 6.3-04	REQ-6.2-04	
REQ 6.3-05	REQ-6.2-05	
REQ 6.3-06	REQ-6.2-06	
REQ 6.4-01		
REQ 6.4-02	REQ-6.3-01	
REQ 6.4-03	REQ-6.3-02	
REQ 6.4-04	REQ-6.3-03	
REQ 6.4-05	REQ-6.3-04	
REQ 6.4-06	REQ-6.3-05	
REQ 6.4-07	REQ-6.3-06	
REQ 6.4-08	REQ-6.3-07	
REQ 6.4-09	REQ-6.3-08	
REQ 6.4-10	REQ-6.3-09	

REQ 6.4-11	REQ-6.3-10	
REQ 6.5.1-01		OVR-6.5-01
REQ 6.5.2-01		ETSI EN 319 421 clause 6.5.2
REQ 6.6-01		OVR-6.6-01
REQ 7.1-01		OVR-7.2-03
REQ 7.2-01		OVR-7.2-02
REQ 7.2-02	REQ-7.1.1-01 REQ-7.1.1-02	
REQ 7.2-03	REQ-7.1.1-03	
REQ 7.2-04	REQ-7.1.1-04	
REQ 7.2-05		
REQ 7.2-06	REQ-7.1.1-05	
REQ 7.2-07	REQ-7.1.1-06	
REQ 7.2-08	REQ-7.1.1-07	
REQ 7.2-09	REQ-7.1.2-01	
REQ 7.3-01	REQ-7.2-01	
REQ 7.3-02		OVR-7.2-04
REQ 7.3-03	REQ-7.2-03	
REQ 7.3-04	REQ-7.2-02	
REQ 7.3-05	REQ-7.2-04	
REQ 7.3-06	REQ-7.2-05	
REQ 7.3-07	REQ-7.2-06	
REQ 7.3-08	REQ-7.2-07	
REQ 7.3-09	REQ-7.2-16B	

REQ 7.3-10	REQ-7.2-10	
REQ 7.3-11	REQ-7.2-11	
REQ 7.3-12	REQ-7.2-12	
REQ 7.3-13	REQ-7.2-13	
REQ 7.3-14	REQ-7.2-14	
REQ 7.3-15	REQ-7.2-15	
REQ 7.3-16	REQ-7.2-16A	
REQ 7.3-17	REQ-7.2-17	
REQ 7.4.1-01	REQ-7.3.1-01 REQ-7.3.1-02	
REQ 7.4.2-01	REQ-7.3.2-01 REQ-7.4-10 REQ-7.7-06	
REQ 7.5-01	REQ-7.4-01	
REQ 7.5-02	REQ-7.8-16	
REQ 7.5-03	REQ-7.8-17	
REQ 7.5-04	REQ-7.4-04	
REQ 7.5-05	REQ-7.4-05	
REQ 7.5-06	REQ-7.4-06	
REQ 7.5-07	REQ-7.4-07	
REQ 7.5-08	REQ-7.4-08	
REQ 7.5-09	REQ-7.4-09	
REQ 7.6.1-01	REQ-7.5-01	
REQ 7.6.2-01		ETSI EN 319 421 clause 7.6.2 a) TIS-7.6.2-01 TIS-7.6.2-02

REQ 7.6.2-02		TIS-7.6.3-03
REQ 7.6.2-03		TIS-7.6.3-05
REQ 7.6.2-04		TIS-7.6.2-06
REQ 7.6.2-05		TIS-7.6.2-07
REQ 7.6.2-06		TIS-7.6.2-08
REQ 7.6.3-01		TIS-7.6.3-01
REQ 7.6.3-02		TIS-7.6.3-02 TIS-7.6.3-03
REQ 7.6.3-03		TIS-7.6.3-04 TIS-7.6.3-05
REQ 7.6.3-04		TIS-7.6.3-06
REQ 7.6.4-01		TIS-7.6.4-01
REQ 7.6.4-02		TIS-7.6.4-02
REQ 7.6.4-03		TIS-7.6.4-03TIS-8.1-01
REQ 7.6.4-04		TIS-7.6.4-04
REQ 7.6.4-05		TIS-7.6.4-05
REQ 7.6.5-01		TIS-7.6.5-01
REQ 7.6.6-01		
REQ 7.6.6-02		TIS-7.6.6-01
REQ 7.6.6-03		TIS-7.6.6-02
REQ 7.6.6-04		TIS-7.6.6-03
REQ 7.6.6-05		TIS-7.6.6-04
REQ 7.6.7-01		TIS-7.6.7-01
REQ 7.6.7-02		TIS-7.6.7-02
REQ 7.6.7-03		TIS-7.6.7-03
REQ 7.6.7-04		TIS-7.6.7-04

REQ 7.6.7-05		TIS-7.6.7-05
REQ 7.6.7-06		TIS-7.6.7-06
REQ 7.6.7-07		TIS-7.6.7-07
REQ 7.6.7-08		TIS-7.6.7-08
REQ 7.7.1-01		TIS-7.7.1-01
REQ 7.7.1-02		ETSI EN 319 422 clause 9.1
REQ 7.7.1-03		TIS-7.7.1-02 TIS-7.7.1-03
REQ 7.7.1-04		TIS-7.7.1-04
REQ 7.7.1-05		TIS-7.7.1-05 TIS-7.7.1-06
REQ 7.7.1-06		TIS-7.7.1-07
REQ 7.7.1-07		TIS-7.7.1-08
REQ 7.7.1-08		TIS-7.7.1-09
REQ 7.7.1-09		TIS-8.2-01
REQ 7.7.1-10		TIS-8.2-02
REQ 7.7.1-11		TIS-8.2-03
REQ 7.7.2-01		TIS-7.7.2-01
REQ 7.7.2-02		TIS-7.7.2-02
REQ 7.7.2-03		TIS-7.7.2-03
REQ 7.7.2-04		TIS-7.7.2-04
REQ 7.7.2-05		TIS-7.7.2-05
REQ 7.7.2-06		TIS-7.7.2-06
REQ 7.7.2-07		TIS-7.7.2-07 TIS-7.7.2-08 TIS-7.7.2-09
REQ 7.8-01	REQ-7.6-01	
REQ 7.8-02	REQ-7.6-02	

REQ 7.8-03	REQ-7.6-03 REQ-7.6-04	
REQ 7.8-04	REQ-7.6-05	
REQ 7.8-05		OVR-7.8-02
REQ 7.8-06		OVR-7.8-03
REQ 7.8-07		OVR-7.8-04 OVR-7.8-05 OVR-7.8-06
REQ 7.8-08		OVR-7.8-07 OVR-7.8-08
REQ 7.8-09		OVR-7.8-09 OVR-7.8-10
REQ 7.8-10		OVR-7.8-11
REQ 7.8-11		OVR-7.8-12
REQ 7.9-01	REQ-7.7-01	
REQ 7.9-02	REQ-7.7-02	
REQ 7.9-03	REQ-7.7-03 REQ-7.7-04	
REQ 7.9-04	REQ-7.7-05 REQ-7.7-09	
REQ 7.9-05	REQ-7.3.2-02	
REQ 7.9-06	REQ-7.3.2-03	
REQ 7.9-07	REQ-7.7-08	
REQ 7.9-08		OVR-7.9-02
REQ 7.10-01	REQ-7.8-01	
REQ 7.10-02	REQ-7.8-02	
REQ 7.10-03	REQ-7.8-03	
REQ 7.10-04	REQ-7.8-04	

REQ 7.10-05	REQ-7.8-05	
REQ 7.10-06		OVR-7.10-03
REQ 7.10-07	REQ-7.8-06	
REQ 7.10-08		OVR-7.10-02
REQ 7.10-09	REQ-7.8-07	
REQ 7.10-10	REQ-7.8-08	
REQ 7.10-11	REQ-7.8-09	
REQ 7.10-12	REQ-7.8-10	
REQ 7.10-13	REQ-7.8-11A	
REQ 7.10-14	REQ-7.8-12	
REQ 7.10-15	REQ-7.8-13 REQ-7.8-13A	
REQ 7.10-16	REQ-7.8-14 REQ-7.8-14A REQ-7.8-15	
REQ 7.10-17		OVR-7.10-04
REQ 7.11-01	REQ-7.9-01	
REQ 7.11-02	REQ-7.9-02	
REQ 7.11-03	REQ-7.9-03	
REQ 7.11-04	REQ-7.9-04	
REQ 7.11-05	REQ-7.9-05	
REQ 7.11-06	REQ-7.9-06	
REQ 7.11-07	REQ-7.9-07	
REQ 7.11-08	REQ-7.9-08	

REQ 7.11-09	REQ-7.9-09	
REQ 7.11-10	REQ-7.9-10	
REQ 7.11-11	REQ-7.9-11	
REQ 7.11-12	REQ-7.9-12	
REQ 7.12-01	REQ-7.10-01	
REQ 7.12-02	REQ-7.10-02 REQ-7.10-08	
REQ 7.12-03	REQ-7.10-02 REQ-7.10-03	
REQ 7.12-04	REQ-7.10-04	
REQ 7.12-05	REQ-7.10-05	
REQ 7.12-06	REQ-7.10-06	
REQ 7.12-07	REQ-7.10-07	
REQ 7.12-08	REQ-7.10-02 REQ-7.10-08	
REQ 7.12-09		OVR-7.12-02
REQ 7.12-10		OVR-7.12-03
REQ 7.12-11		OVR-7.12-04 OVR-7.12-05
REQ 7.12-12		OVR-7.12-06
REQ 7.13-01	REQ-7.11-01	
REQ 7.13-02	REQ-7.11-02	
REQ 7.13-03		OVR-7.13-03
REQ 7.13-04		OVR-7.13-04
REQ 7.13-05		OVR-7.13-05

REQ 7.13-06		OVR-7.13-06
REQ 7.14-01	REQ-7.12-01	
REQ 7.14-02	REQ-7.12-02	
REQ 7.14-03	REQ-7.12-03	
REQ 7.14-04	REQ-7.12-04	
REQ 7.14-05	REQ-7.12-05	
REQ 7.14-06	REQ-7.12-06	
REQ 7.14-07	REQ-7.12-07	
REQ 7.14-08	REQ-7.12-08	
REQ 7.14-09	REQ-7.12-11	
REQ 7.14-10		OVR-7.14-02
REQ 7.14-11	REQ-7.12-09	
REQ 7.14-12	REQ-7.12-10	
REQ 7.15-01	REQ-7.13-01	
REQ 7.15-02	REQ-7.13-02	
REQ 7.15-03	REQ-7.13-03 REQ-7.13-04	
REQ 7.15-04	REQ-7.13-05	