Certipost e-Timestamping

Time-Stamping Authority Policy

Version	1.0
Effective date	01 09 2008
Object Identification Number (OID)	0.3.2062.7.1.6.2.1.0

Contents

Intellectual property rights

Foreword

This Time-Stamping Authority Policy or Time-Stamping Policy (TSP) is based on and thus compatible with the Technical Standard ETSI TS 102 023 V1.2.1 (2003-01) "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities"

For the interpretation of the present TSP, the following guidelines apply:

1) The international standardisation process influences the titles and subtitles of this TSP. In interpreting this TSP, the text under each title shall be given precedence over the wordings in the titles.
2) Reference of TSP locations has to be done in the following manner. First the TSP name has to be provided, followed by the heading numbering and the section/subsection numbering. For instance: Certipost Time-Stamping Authority Policy v1.0, section 1.3.2/c3
3) As a general rule the Time-Stamping Service Provider (CSP), acting in accordance with this TSP, shall undertake adequate measures to fulfil all requirements in this TSP. When a section is marked with "Not applicable", it means that this section is not applicable to Certipost e-Timestamping Time-Stamping Authority Policy.

Introduction

In creating reliable and manageable digital evidence it becomes necessary to use methods which associate date and time to transactions. A time-stamping service couples an accurate date and time to electronic data using a digital signature. The time-stamp tokens (TST) issued by the time-stamping service are used to prove that certain data existed at a certain moment in time and that it has not been changed since then.

A trusted time-stamp is a time-stamp issued by a trusted third party (TTP) acting as a Time-Stamping Authority (TSA).

The present policy document specifies the operation and management practices of the TSA such that subscribers and relying parties may have confidence in the operation of the time-stamping service.

Certipost assumes the role of Trusted Third Party time-stamping service provider when providing the Certipost e-Timestamping service.

In the sense of the directive 1999/93/EC of the European Parliament and the Council of 13 December 1999 on a Community framework for electronic signatures, a TSA can be seen as "an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures" or a Certification Service Provider (CSP).

The current Certipost e-Timestamping Time-Stamping Authority Policy, shall be reflected in contracts between the TSA and its Subscribers.

1. Scope

The present document describes the policy to which the Certipost e-Timestamping Authority (TSA) adheres, in order to confirm to subscribers and relying parties of the correct operation and management of the respective services, as per international state of the art standards.

The current Time-Stamping Policy specifies general rules used by the Certipost e-Timestamping Authority (TSA) for the issuance of Time-Stamp Tokens (TST). It defines the parties involved, their responsibilities, rights and the applicability range. These specific practices described in this present TSP are ruled and operated under the more general practices as described in the Certipost E-Trust Certificate Practise Statement (hereafter referred to as the [Certipost CPS]).

This TSP addresses the services provided by the Certipost e-Timestamping Authority that can be reached via: http://repository.tsa.certipost.eu .

Time-Stamp Tokens issued in accordance with the present TSP may be used to provide long-term proof of authenticity for any electronic data, amongst others long-term electronic signatures [TS 101 733], medical documents, executable code and electronic transactions.

Additional information and support can be received from service.desk@staff.certipost.be .

2. References

TS 102 023: Technical Specification ETSI TS 102 023 V1.2.1 (2003-01) "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities"

Certipost CPS: Certipost E-Trust Services Certification Practise Statement for Qualified, Normalised and Lightweight Certificates O.I.D. 0.3.2062.7.1.0.1.2 which can be obtained from http://www.e-trust.be/CPS/QNCerts .

TS 101 733: Technical Specification ETSI TS 101 733 v1.5.1 (2003-12) "Electronic Signature Formats"

RFC 3161: IETF RFC 3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) – August 2001

TS 101 861: Technical Specification ETSI TS 101 861 V1.2.1 (2002-03) "Time stamping profile"

3. Definitions and abbreviations

3.1. Definitions

Certipost or Certipost e-Timestamping	Certipost nv / sa, with registered offices in Centre Monnaie – Muntcentrum, 1,B-1000 Brussels, Belgium
Certipost E-Trust Infrastructure	The Certipost Public Key Infrastructure that is deployed by Certipost to provide the Certipost Certification Services.
Certipost Certification Practices Council	The Policy Authority within Certipost is called the Certipost Certification Practices Council (CEPRAC). It is the high level management body with final authority and responsibility for Specifying and approving the Certipost infrastructure and practices. Approving the Certipost Certification Practice Statement(s) and Certipost Certificate and Time-Stamping Policies. Defining the review process for certification practices and Certificate Policies including responsibilities for maintaining the Certification / TSA Practice Statements and Certificate / Time-Stamping Policies. Defining the review process that ensures that the Certification Authorities (CAs) properly implements the above practices. Defining the review process that ensures that the Certificate / Time-Stamping Policies are supported by the CAs Certification Practice Statement(s). Publication to the Subscribers and relying parties of the Certificates / Time-Stamping Policies and Certification Practice Statements and their revisions. Specifying cross-certification procedures and handling cross-certification requests.
Certipost Services	The Certipost Certification and Time-Stamping services.
Certification Authority Auditor (CAA)	The Certipost Internal CA Auditor that audits the operations of the CA related Entities.
Certification Practice Statement (CPS)	A statement of the practices, which a certification authority applies for the issuing of Certificates.
Certification Service Provider	Any physical or moral person which delivers and manages Certificates or provides other services related to electronic signatures.
Coordinated Universal Time (UTC)	Time scale based on the second as defined in ITU-R Recommendation TF.460-5
Relying Party	Recipient of a time-stamp token who relies on that time-stamp token

Subscriber	Entity requiring the services provided by the Certipost e-Timestamping Time-Stamping Authority and which has explicitly or implicitly agreed to its terms and conditions.
Time-Stamping Policy (TSP)	Named set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements
Time-Stamp Token (TST)	Data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time
Time-Stamping Authority (TSA)	Authority which issues time-stamp tokens
Time-Stamping Unit (TSU)	Set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a time
TSA Disclosure Statement	Set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements
TSA Practice Statement	Statement of the practices that a TSA employs in issuing time-stamp tokens. As the Certipost TSA is ruled by the same organisational structure, operating procedures, facilities and computer environment as the Certipost PKI infrastructure, the Certipost Certificate Practice Statement acts as well as the Certipost TSA practise statement.
TSA system	Composition of IT products and components organized to support the provision of time-stamping services

3.2. Abbreviations

CA Certification Authority

CPS Certification Practice Statement

CRL Certificate Revocation List

PKI Public Key Infrastructure

OCSP Online Certificate Status Protocol

TSA Time-Stamping Authority

TSS Time-Stamping Services

TST Time-Stamp Token

TSU Time-Stamping Unit

UTC Coordinated Universal Time

4. General concepts

4.1. Time-stamping services

The Time-Stamping Services (TSS's) consist of the infrastructure, the management and the provisioning of time-stamp tokens.

The infrastructure which is used to generate the TST's consists of:

- a communication interface to collect time-stamp requests and return TST's;
- a Time-Stamping Unit (TSU) which creates specific time-stamp tokens;
- a time source providing accurate date and time values to be included in the time-stamp tokens.

The management of the TSS is the service component that monitors and controls the operation of the TSS to ensure that the service is provided as specified by the TSA.

The TSS assures use of a reliable time source and proper management of all system components.

These services are provided by the Certipost CSP to the subscribers and are ruled by the same organisational structure, operating procedures, facilities and computer environment as the Certipost PKI infrastructure.

4.2. Time-Stamping Authority

The Certipost Time-Stamping Authority (TSA) is responsible for the provisioning of the TSS's described in the previous paragraph. It has the responsibility for the operation of the relevant TSU's which create and sign on behalf of the TSA.

It is this authority that is trusted by the users of the Certipost Time-Stamping services (i.e. subscribers as well as relying parties) to issue time-stamp tokens.

4.3. Subscriber

The subscriber may be an organization comprising several end-users or an individual end-user.

When the subscriber is an organization, some of the obligations that apply to that organization will have to apply as well to the end-users. In any case the organization will be held responsible if the obligations from the end-users are not correctly fulfilled and therefore such an organization is expected to suitably inform its end users.

When the subscriber is an individual end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

The Certipost TSA issues TST's to every interested party without any technical limits. The procedure to become a subscriber and the pricelist describing the related charging fees can be obtained upon request from service.desk@staff.certipost.be .

4.4. Time-stamp policy and TSA practice statement

4.4.1. Purpose

The present time-stamp policy is to be used in conjunction with the [Certipost CPS] which acts together with the present policy as TSA practice statement.

In general, the present Time-Stamping Policy states "what is to be adhered to", while the [Certipost CPS] states "how it is adhered to".

The present document specifies a Time-Stamping Policy to meet general requirements for trusted time-stamping services. The [Certipost CPS] specifies practice statements how these requirements are met (including personnel management, personnel selection, physical security, etc.).

The present Time-Stamping Policy is publicly available. Distribution of this document is restricted as described in the paragraph "

Intellectual property rights".

4.4.2. Level of specificity

The present TSP describes only general rules of issuing and managing TST's. Detailed descriptions of the infrastructure and related operational procedures are described in additional documents that are not made publicly available. These additional documents are only available to authorized Certipost personnel and, on a needs basis, to auditors of the TSA.

4.4.3. Approach

The present TSP is defined independently of the specific details of the specific operating environment of the Certipost TSA, whereas the [Certipost CPS] is tailored to the organizational structure, operating procedures, facilities, and computing environment of the Certipost TSA.

5. Time-stamp Policies

5.1. Overview

The present TSP is a set of rules used during the issuing TST's and regulating security level for the Certipost TSA.

TST's are issued with an accuracy of 1 second or better.

The Certipost e-Timestamping service signs the TST's using private keys that are dedicated for that purpose.

The profiles of the public key certificates used by the Certipost TSA comply with the [RFC 3161].

The TSA certificate is specified in section 8 Appendix of this document.

The Certipost TSA issues TST's according to [TS 101 861].

5.2. Identification

The object-identifier of the current policy is defined as follows:

Policy Identifier (OID)
0.3.2062.7.1.6.2.1.(version).(sub-version)

The OID is specified in every time-stamp issued by the TSS.

The TSP of the Certipost e-Timestamping service is available to the Subscribers and Relying parties on the following location: http://repository.tsa.certipost.eu .

5.3. User Community and applicability

The current policy does not define any limitations on users or applicability of the services delivered. The Certipost TSA can provide time-stamping services for time-stamping of any electronic data to any user, including closed communities.

5.4. Conformance

The Certipost TSA uses the identifier for the current policy in TST's as given in paragraph 5.2 Identification.

The Certipost TSA ensures compliance of provided services with regulations specified in paragraph 6.1 TSA obligations and ensures reliability of control mechanisms described in chapter 7 Requirements on TSA practices.

6. Obligations and liability

6.1. TSA obligations

6.1.1. General

This chapter includes all the obligations, liabilities, guarantees and responsibilities of the Certipost TSA, its subscribers and TST users (relying parties). This obligation and responsibilities are regulated by mutual agreements signed between the parties.

Certipost agreements with subscribers and relying parties describe mutual obligations and responsibilities, including financial responsibilities.

The current Time-Stamping Policy and the [Certipost CPS] are integral parts of the agreements signed between Certipost and the subscribers and relying parties.

Certipost guarantees that all the requirements of the Certipost TSA, including procedures and practices related to the issuance of TST's, review of system and security audit are in accordance with regulations described in chapter 7 Requirements on TSA practices of this policy.

The Certipost TSA acts in accordance with the above procedures. No exclusions of these regulations are allowed. Additional obligations of the TSA, subscribers and relying parties are described in the [Certipost CPS] paragraph 2.1 Obligations.

6.1.2. TSA obligations towards subscribers

Certipost guarantees permanent access to the TSS on a 24 hours a day and 7 days a week basis. Notwithstanding what is mentioned before, and outside maintenance windows, for each calendar month, the total time of unavailability of the time-stamping service, measured in minutes, cumulated over the whole month should not be more than 0.5% of the total number of minutes of that calendar month.

Moreover Certipost guarantees that:

- It complies with this TSP and with the TSA practice statement and its amendments as published under http://repository.tsa.certipost.eu ;
- It archives logging data of time-stamp issuance for a duration as legally required or – in case no legal requirement would apply - for a maximum duration of 25 years starting from the time mentioned in the TST;
- The TSU's maintain a minimum UTC time accuracy of 1 second;
- Its commercial activity is provided on the basis of reliable equipment and software;
- The activities and services provided are legal; in particular they do not violate intellectual property, license and other related rights.
- Services delivered are conforming to generally accepted norms.
- High availability access to the TSS systems is maintained except in case of planned maintenance or loss of time synchronization.
- Issued TST's do not contain any false data or mistakes.
- It will deliver, upon subscriber request, all elements that permit attestation of the reliability of date and time contained in the TST's.
- That it will maintain a competent and experienced team that can ensure the continuity of the TSS.

- It will ensure the on a permanent basis the physical and logical security, as well as the integrity of materials, software and databases required for the correct functioning of the TSS as described in the [Certipost CPS].
- It will monitor and control the TSS (a.o. Intrusion Detection) the whole TSA infrastructure, in order to prevent or limit any disturbance or unavailability of the TSS resulting from deliberate attacks, as described in the present policy and the [Certipost CPS].
- It will take all measures required according to generally accepted norms to secure its services, in order to prevent outages of the TSS.
- It will make available a back-up infrastructure that can be used in case of service interruption of the main infrastructure.

The TSA enforces controls to ensure compliance of the service with Service Level Agreements defined in this document.

6.2. Subscriber obligations

Subscribers retrieving TST's, should verify the electronic signatures posed by the Certipost TSA on the TST's.

Such verification comprises:

- Verification whether the signature on the TST is correct.
- Verification of the TSA certificate:

  Verification of the trusted path up to the trusted root certificate, and for each of the certificates in the chain (including the TSA certificate itself):

  - Verification whether the certificate is not expired at the moment of signature.
  - Verification whether the certificate was not revoked or suspended at the moment of signature.

Additional subscriber obligations are described in the [Certipost CPS], paragraph 2.1.3 Subscriber obligations.

6.3. Relying party obligations

Parties relying on TST's, should verify the electronic signatures posed by the Certipost TSA on the TST's.

Such verification comprises:

- Verification whether the signature on the TST is correct.
- Verification of the TSA certificate:

  Verification of the trusted path up to the trusted root certificate, and for each of the certificates in the chain (including the TSA certificate itself):

  - Verification whether the certificate was not revoked or suspended at the moment of signature.

In case the relying party intends to rely on a TST where the TSA certificate has expired, he should only do so when a non-repudiation proof exists (e.g. another TST, or notary record) that guarantees that the TST did exist before expiry of the certificate and has not been changed since. This is specifically of importance when the cryptographic functions or TSA certificate key length of the TST are not considered secure anymore at the time the party intends to rely on the TST.

This policy does not specify any limits according usage of TST's.

Additional relying party obligations are described in the [Certipost CPS], paragraph 2.1.4 Relying party obligations.

6.4. Liability

The liability of Certipost TSA and relying parties connected with the services is specified in mutual agreement or is as foreseen in the applicable legislation. The maximal financial responsibility (liability cap) for TSA is of 2.500 € per contractual agreement.

Without prejudice to the above limitations, Certipost TSA is held liable for direct damages as result of:

- Non respect of requirements specified in this policy;
- Any breach of confidentiality obligation with regards of personal data sent by subscribers;
- Damages to subscribers or relying parties in case of non-execution of contractual terms;
- Damages caused by its personnel in the context of the provisioning of services as described in the contract;
- Damages to partners / subscribers as a result of dysfunction of devices used by Certipost TSA;
- Lack of precision and/or integrity of data that it delivers or manages.

The other liabilities and regulation of the provision of TSA services are described in [Certipost CPS], Chapter 2.3 Liability.

Certipost TSA declines any responsibility with regards to the usage that is made with the TST it delivers and signs.

7. Requirements on TSA practices

Certipost TSA shall implement controls that meet ETSI TS 102 023 requirements.

7.1. Practice and Disclosure Statements

7.1.1. TSA Practice statement

- Risk Assessment: The provision of Certipost TSA services is placed in the more general context of the provision of Trust (Certification) Services as ruled in the [Certipost CPS]. A risk assessment has been and is carried out in order to evaluate business assets and threats to those assets in order to determine the necessary security controls and operational procedures that have been taken in place.
- Procedures, control mechanisms and technical infrastructure described in Chapter 6 of this document are the basis of the Certipost TSA functioning. Other controls are described in the [Certipost CPS].
- The Certipost TSA Practices Statements are currently the collection of the present document and the [Certipost CPS]. Both documents are available to the public and published on the Certipost website http://repository.tsa.certipost.eu, in accordance to the regulations described in the [Certipost CPS], Chapter 2.9 Intellectual Property Rights. Together with associated internal documents, they rule the Certipost TSA services operation.
- The terms and conditions regarding the use of the Certipost TSA services are disclosed and made available to all subscribers and relying parties as specified in section 7.1.2 of the present document.
- Final authority and management of the Certipost TSA services and its practices are ensured by the Certipost CEPRAC. This CEPRAC, Senior management and the Quality Control Manager of Certipost shall ensure that the practices are properly implemented. The CEPRAC is in charge of defining the review process for the practices, including the responsibilities for maintaining the TSA practices statement.
- The Certipost TSA will give due notice of changes it intends to make in practices statement. Any such changes will be subject to revision and approval by the CEPRAC. The Certipost TSA shall make the revised version immediately available as described in the [Certipost CPS].

7.1.2. TSA Disclosure Statement

Certipost TSA shall disclose to all subscribers and potential relying parties the terms and conditions regarding the use of its time-stamping services. TSA disclosure statement from Certipost TSA is compliant with requirements from ETSI TS 102 023 and is included in subscriber / relying contractual agreement.

Certipost TSA contact information is

Certipost nv / sa

CEPRAC e-Timestamping

Ninovesteenweg 196

9320 Erembodegem

Belgium

Every TST issued by Certipost TSA includes the policy identifier, defined in Chapter 5.2 of this document. Cryptographic hash functions, used in the time-stamping process are in accordance with normative requirements. Ex-

pected validity period of TST is 3 years. Accuracy of the time, which is provided in a TST is regulated in chapter 6.1.2 of this policy. Limitations related with TSA system have been defined in chapter 5.3 of this policy. Subscriber's obligations are described in chapter 6.3 of this policy. TST verification should be performed with the usage of appropriate software.

All TST's will be archived for duration of three years, starting from the time mentioned in the TST.

Liabilities are defined in chapter 6.4 of this policy.

Complaints, suggestions and remarks on Certipost TSA services should be addressed to the Certipost service desk de using the phone number +32 (0)70/22.55.33 or fax number +32 (0) 70/22.55.01 or via e-mail : service.desk@staff.certipost.be.

Provision of Certipost TSA services are ruled by the Belgian Laws.

7.2. Key management life cycle

7.2.1. TSA key generation

Certipost TSA ensures that any cryptographic keys are generated under controlled circumstances and in accordance with general key pair generation and installation practices as described in the [Certipost CPS] (section 6.1).

Certipost TSA keys are generated within a Hardware Security Module (HSM) complying with FIPS 140-1 level 3 in a physically secured environment, by personnel in trusted role in accordance with the [Certipost CPS]. TSA key generation algorithm is described in chapter 5.1 of this policy.

7.2.2. TSU private key protection

Certipost TSA ensures that TSU private keys are and remain confidential and maintain their integrity. Certipost TSA keys are generated, held and used within Hardware Security Module (HSM) complying with FIPS 140-1 level 3 in a physically secured environment, by personnel in trusted role in accordance with the [Certipost CPS].

The procedures and circumstances for TSA key back-up and key recovery in case of a disaster, failure of the system or system conservation are in accordance with the [Certipost CPS].

7.2.3. TSU public key Distribution

Certipost TSA ensures that the integrity and the authenticity of the TSU signature verification (public) keys and any associated parameters are maintained during its distribution towards relying parties. Certipost TSA certificates are published in the Certipost website http://ca.e-trust.be .

Certipost TSU certificates are issued by Certipost E-Trust Primary CA for Qualified Certificates in accordance with the [Certipost CPS].

7.2.4. Rekeying TSU Keys

The lifetime of the Certipost TSU certificates are not longer than the period of time that the chosen algorithm and key length are recognised as being fit for purpose.

Certipost TSA rekey procedure is executed upon expiry of validity period of the certificate of the TSA in accordance with the [Certipost CPS]. Public keys are archived for a period of 30 years. Private key protection is in accordance with the [Certipost CPS].

7.2.5. End of TSU key life cycle

Certipost TSA ensures that TSU private signing keys are not used beyond the end of their life cycle. In particular, operational and technical procedures are in place to ensure that a new key is put in place when a TSU's key expires, TSU private keys or any part, including any copies shall be destroyed such that the private key cannot be retrieved as in accordance with the [Certipost CPS]. TST generation system shall reject any attempt to issue a TST if the signing private key is expired.

7.2.6. Life cycle management of cryptographic module used to sign time-stamps

Certipost TSA ensures the security of the HSM throughout its lifecycle. Procedure and controls are in place in accordance with the [Certipost CPS], to ensure that TST signing cryptographic hardware (HSM) are not tampered with during shipment, while it is stored, that installation, activation and duplication of TSU's signing keys in HSM's shall be done only by personnel in trusted roles, in a physically secure environment, TST HSM's are functioning correctly, and that TSU private signing keys stored on TSU HSM's are erased upon device retirement.

7.3. Time-stamping

7.3.1. Time-stamp token

Certipost TSA ensures that TST are issued securely and include the correct time.

Every TST issued by Certipost TSA, shall include a unique identifier of the policy as described in section 5.2 of this policy. TST's issued by Certipost TSA include date and time value traceable to the real UTC time value. Accuracy of the time is defined in chapter 6.2 of this policy.

Each TST has a unique identifier and is signed using a key generated exclusively for this purpose. The TST shall include the policy ID of the TSU that created the timestamp and the TSA name (equal to the DName of the TSU Certificate).

7.3.2. Clock Synchronisation with UTC

The Certipost TSA ensures that its clock is synchronised with UTC within the declared accuracy.

Certipost TSA incorporates the time in the TST with the accuracy described in chapter 6.1.2 of this policy.

Certipost TSA ensures that if the time that would be indicated in a TST drifts or jumps out of synchronisation with UTC, this will be detected.

Certipost has security controls in place, preventing unauthorised operation, aimed at calibration of the clock out of order, any manipulation or physical damage to the clock.

7.4. TSA management and operation

7.4.1. Security management

Certipost TSA ensures that administrative and management procedures are applied which are adequate and correspond to recognised best practices.

All requirements and subjects related to security management are implemented as described in the [Certipost CPS].

7.4.2. Asset classification and management

Certipost TSA ensures that its information and other assets receive an appropriate level of protection.

The description of methods and measures undertaken for affirmation of continuity and stability of Certipost TSA system operation is described in the [Certipost CPS].

Certipost TSA maintains an inventory of all assets that are assigned a classification for the protection requirements in a consistent way with the risk analysis.

7.4.3. Personnel security

Certipost TSA ensures that the personnel and hiring practices enhance and support the trustworthiness of the TSA's operations. Description of the personnel security rules as well as the trusted roles used in Certipost TSA services environment is provided in the [Certipost CPS]. Managerial and operational personnel possess the appropriate skills and knowledge of time-stamping, digital signatures and Trust Services as well as security procedures for personnel with security responsibilities, information security and risk assessment.

7.4.4. Physical and environmental security

Certipost TSA ensures that physical access to critical services is controlled and physical risks to its assets minimised.

The implementation of the physical an environmental security is provided in accordance with the rules described in the [Certipost CPS].

7.4.5. Operations management

Certipost TSA ensures that the TSA system components are secure and correctly operated, with minimal risk of failure.

Certipost TSA possesses the procedures, processes and infrastructure to comply with the operational management and procedural security requirements as defined in the ETSI TS 102 023. This information is mainly internal company documentation, disclosed periodically to the TSA auditors.

7.4.6. System Access Management

Certipost TSA ensures that TSA system access is limited to properly authorised individuals in accordance with the [Certipost CPS].

7.4.7. Trustworthy Systems Deployment and Maintenance

Certipost TSA ensures that it uses trustworthy systems and products that are protected against modifications in accordance with the [Certipost CPS]. Analysis of security requirements shall be carried out at the design and requirement specifications stage of any systems development project undertaken by the TSA or on behalf of the TSA to ensure that security is built into IT systems. Change control procedures shall be applied for releases, modifications and emergency software fixes of any operational software.

7.4.8. Compromise of TSA Services

Certipost TSA ensures that in the case of events which affects the security of the TSA services, including compromise of TSU private signing keys or detected loss of calibration, that relevant information is made available to subscribers and relying parties in accordance with the [Certipost CPS] and in accordance with ETSI TS 102 023.

7.4.9. TSA termination

Certipost TSA ensures that potential disruptions to subscribers and relying parties are minimised as a result of the cessation of the TSA time-stamping services, and in particular ensures that continued maintenance of information required to verify the correctness of time-stamp tokens. TSA termination is also ruled in accordance of the [Certipost CPS].

7.4.10. Compliance with Legal Requirements

Certipost TSA ensures compliance with appropriate legal requirements and is acting under the Belgian law regulations, and in particular data protection and privacy regulations.

7.4.11. Recording of information concerning operation of time-stamping service

Certipost TSA ensures that all relevant information concerning the operations of the Certipost TSA time-stamping services is recorded for a defined period of time, in particular for the purpose of providing evidence for the purposes of legal proceedings, in accordance with the [Certipost CPS].

7.5. Organizational

Certipost TSA ensures that its organisation is reliable as required in ETI TS 102 023, subsections 7.5 a) to i). Certipost is a company owned by the Belgian Post Group and has the financial stability and resources required to operate in conformity with ETSI TS 102 023 and as generally ruled by the [Certipost CPS]. Registered address of Certipost is Centre Monnaie – MuntCentrum, 1, 1000 Brussels, Belgium.

8. Appendix

The TSA Certificate Profile is specified as follows:

TSA Certificate (Time-stamp signing certificate profile)					
Base Certificate	**OID**	**Include**	**Critical**	**Value**	
Certificate					
SignatureAlgorithm					
Algorithm		X		1.2.840.113549.1.1.5 (SHA-1 with RSA Encryption)	
SignatureValue		X		Issuing CA Signature	
TBSCertificate					
Version		X		2	
SerialNumber		X		Provided by the CA (validated on duplicates)	
Signature		X		Sha-1WithRSAEncryption	
Validity					
notBefore		X		Key Generation Process Date	
notAfter		X		Key Generation Process Date + 60 months	
SubjectPublicKeyInfo		X		Provided by PKCS10 request – key length 2048	
Issuer					
CountryName	{ id-at-6 }	X		BE	
CommonName	{ id-at-3 }	X		Certipost E-Trust Secondary Qualified CA for Legal Persons	
OrganizationalName		X		Certipost NV / SA	
Subject			Required		
CommonName	{ id-at-3 }		YES	Certipost NV / SA KBO 0475396406	
CountryName	{ id-at-6 }		YES	BE	
eMail			optional	tsa@certipost.eu	
Subject Serial Number			optional	<yyyy>[i]	
Locality			optional	Brussels	
State or province			optional		
Organization Unit			optional	Certipost e-timestamping services www.certipost.eu	
Organization			optional	Certipost	
Standard Extensions	**OID**	**Include**	**Critical**	**Value**	
CertificatePolicies	{id-ce 32}	X	FALSE		
PolicyIdentifier		X		0.3.2062.7.1.1.112.1	
PolicyQualifiers				NA	
PolicyQualifierId	{ id-qt-1 }	X		CPS	
Qualifier		X		http://www.e-trust.be/CPS/QNCerts	
DisplayText				"E-Trust Certificate Policy for Qualified Certificates for Legal Persons. Supported by SSCD, Key Generation by CSP. GTC, CP and CPS: www.e-trust.be/CPS/QNCerts"	
KeyUsage	{id-ce 15}	X	TRUE		
NonRepudiation		X		Set	
DigitalSignature		X		Set	
Extended KeyUsage	{id-ce 37}		TRUE		
Time stamping		X		Set	
Subject Alternative Name	{id-ce 17}		FALSE		
822 Email Address					
BasicConstraints	{id-ce 19}	X	FALSE		
CA		X		FALSE	
PathLenConstraint		X		None	
AuthorityKeyIdentifier	{id-ce 35}	X	FALSE		
SubjectkeyIdentifier		X	FALSE	SHA-1 Hash	
CRLDistributionPoints	{id-ce 31}	X	FALSE		
DistributionPoint		X			
ullName		X		http://crl.e-trust.be/QCA_LeP.crl	

[i] Year in which the certificate is used.