Time Stamp Authority

Certificate Policy

Certificate Practice Statement

Date	Rev	Description of changes
7-Mar-2023	01	First release

1 INTRODUCTION 6

1.1 OVERVIEW 6
1.2 DOCUMENT NAME AND IDENTIFICATION 7
1.2.1 EFFECT 7
1.3 PARTICIPANTS AND RESPONSIBILITIES 8
1.3.1 TRUSTPRO QTSP TIME STAMP AUTHORITY 8
1.3.2 SUBSCRIBERS 9
1.3.3 RELYING PARTIES 9
1.4 PERMITTED USAGECPS 9
1.5 POLICY ADMINISTRATION 10
1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT 10
1.5.2 CONTACT PERSON 10
1.5.3 ENTITY RESPONSIBLE FOR THE SUITABILITY OF THE PRACTICE STATEMENT FOR THE *QUALIFIED SIGNATURE CERTIFICATE POLICY* 10
1.5.4 CP APPROVAL PROCEDURES 10
1.6 DEFINITIONS AND ACRONYMS 10
1.6.1 DEFINITIONS 10
1.6.2 ACRONYMS 15

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 16

2.1 REPOSITORIES 16
2.2 TIME STAMP PRESERVATION 16
2.3 PUBLICATION OF THE PUBLIC KEY FOR TIME STAMP VERIFICATION 17
2.4 TIME OR FREQUENCY OF PUBLICATION 17
2.4.1 FREQUENCY OF THE PUBLICATION OF TERMS AND CONDITIONS 17
2.4.2 FREQUENCY OF THE CERTIFICATES DISCLOSURE 17
2.4.3 ACCESS CONTROLS ON REPOSITORIES 17

3 IDENTIFICATION AND AUTHENTICATION 19

3.1 NAME 19
3.1.1 TYPE OF NAMES 19
3.1.2 NEED FOR NAMES TO BE MEANINGFUL 19
3.1.3 APPLICANTS' ANONYMITY AND PSEUDONYM 19
3.1.4 INTERPRETATION RULES OF THE TYPES OF NAMES 19
3.1.5 UNEQUIVOCALNESS OF THE NAMES 19
3.2 INITIAL IDENTITY VALIDATION 19
3.3 IDENTIFICATION AND AUTHENTICATION FOR THE RENEWAL OF THE KEYS AND CERTIFICATES 19
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION OR SUSPENSION REQUESTS 20

4 OPERATIONAL REQUIREMENTS 21

4.1 REQUEST FOR TIME STAMP EMISSION OR VERIFICATION 21
4.1.1 WHO CAN APPLY FOR TIME STAMP EMISSION OR VERIFICATION 21
4.1.2 REGISTRATION PROCESS AND RESPONSIBILITY 21

4.2 PROCESSING THE REQUEST 21
4.3 TIME STAMP CREATION 22
4.4 ACCEPTANCE OF THE CERTIFICATE 22
4.5 KEY PAIR AND CERTIFICATE USAGE 22
4.6 CERTIFICATE RENEWAL 23
4.7 RE-ISSUING THE CERTIFICATE 23
4.8 CERTIFICATE MODIFICATION 23
4.9 CERTIFICATE STATUS SERVICES 23
4.9.1 OPERATIONAL CHARACTERISTICS 24
4.9.2 SERVICE AVAILABILITY 24
4.9.3 END OF SUBSCRIPTION 25
4.9.4 KEY ESCROW AND RECOVERY 25

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS 26

5.1 PHYSICAL CONTROLS 26
5.1.1 SITE LOCATION AND CONSTRUCTION 27
5.1.2 PHYSICAL ACCESS 27
5.1.3 POWER AND AIR CONDITIONING 28
5.1.4 WATER EXPOSURES 28
5.1.5 FIRE PREVENTION AND PROTECTION 29
5.1.6 MEDIA STORAGE 29
5.1.7 WASTE DISPOSAL 29
5.1.8 BACKUP 29
5.2 PROCEDURAL CONTROLS 30
5.2.1 TRUSTED ROLES 30
5.2.2 ROLES REQUIRING SEPARATION OF DUTIES 31
5.3 STAFF CONTROLS 32
5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS 32
5.3.2 BACKGROUND CHECK PROCEDURES 32
5.3.3 TRAINING REQUIREMENTS 33
5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS 33
5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE 34
5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS 34
5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS 34
5.3.8 DOCUMENTATION SUPPLIED TO STAFF 34
5.4 AUDIT LOGGING PROCEDURES 35
5.4.1 TYPES OF EVENTS RECORDED 35
5.4.2 FREQUENCY OF AUDIT LOG PROCESSING 35
5.4.3 RETENTION PERIOD FOR AUDIT LOG 35
5.4.4 PROTECTION OF AUDIT LOG 36
5.4.5 AUDIT LOG BACKUP PROCEDURES 36
5.4.6 AUDIT COLLECTION SYSTEM 36
5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT 37
5.4.8 VULNERABILITY ASSESSMENTS 37
5.5 RECORDS ARCHIVAL 37
5.5.1 TYPES OF RECORDS ARCHIVED 37
5.5.2 RETENTION PERIOD FOR ARCHIVE 37

5.5.3 PROTECTION OF ARCHIVE 37
5.5.4 ARCHIVE BACKUP PROCEDURES 38
5.5.5 ARCHIVE COLLECTION SYSTEM 38
5.5.6 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION 38
5.6 TSU KEY CHANGEOVER 39
5.7 COMPROMISE AND DISASTER RECOVERY 39
5.7.1 CORRUPTION OF RESOURCES, SOFTWARE, AND DATA 39
5.7.1 ENTITY PRIVATE KEY COMPROMISE PROCEDURES 39
5.7.2 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER 40
5.8 TERMINATION OF TIME STAMP SERVICE 40

6 TECHNICAL SECURITY CONTROLS 41

6.1 TSU KEY PAIR GENERATION AND INSTALLATION 41
6.1.1 KEY ALGORITHM AND LENGTH 41
6.1.2 PUBLIC KEY QUALITY CONTROLS AND GENERATION 41
6.2 KEY PAIR GENERATION 42
6.2.1 TSA PUBLIC KEY DELIVERY TO RELYING PARTIES 42
6.2.2 KEY SIZES 42
6.2.3 KEY USAGE PURPOSES 43
6.2.4 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 43
6.2.5 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS 43
6.2.6 PRIVATE KEY MULTI-PERSON CONTROL 43
6.2.7 PRIVATE KEY ESCROW 44
6.2.8 PRIVATE KEY BACKUP 44
6.2.9 PRIVATE KEY ARCHIVAL 44
6.2.10 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE 44
6.2.11 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE 44
6.3 ACTIVATION DATA 44
6.4 COMPUTER SECURITY CONTROLS 44
6.4.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS 44
6.5 LIFE CYCLE TECHNICAL CONTROLS 45
6.6 TIME ACCURACY 45

7 CERTIFICATE, CRL AND OCSP PROFILES 46

7.1 TSU CERTIFICATE PROFILES 46
7.1.1 VERSION NUMBER 47
7.1.2 CERTIFICATE EXTENSIONS 47
7.1.3 ALGORITHM OBJECT IDENTIFIERS 47
7.1.4 NAME FORMS 47
7.1.5 NAME CONSTRAINTS 47
7.1.6 TSU CERTIFICATE POLICY OBJECT IDENTIFIERS 47
7.1.7 TSU CERTIFICATE PROFILE DETAILS 47
7.2 CRL PROFILE 48
7.2.1 VERSION NUMBER(S) 48
7.2.2 CRL AND CRL ENTRY EXTENSIONS 48
7.3 OCSP PROFILE 48
7.3.1 VERSION NUMBER(S) 49

7.3.2 OCSP Extensions 49

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 50

8.1 Frequency or Circumstances of Assessment 50
8.1 Identity/Qualifications of Assessor 50
8.2 Assessor's Relationship to Assessed Entity 50
8.3 Topics Covered by Assessment 51
8.4 Actions Taken as a Result of Deficiency 51

9 OTHER BUSINESS AND LEGAL MATTERS 52

9.1 Fees 52
9.1.1 Certificate Issuance or Renewal Fees 52
9.1.2 Certificate Access Fees 52
9.1.3 Revocation or Status Information Access Fees 52
9.1.4 Fees for Other Services and Refund Policy 52
9.2 Financial Responsibility 52
9.3 Confidentiality of Business Information 52
9.3.1 Scope of Confidential Information 53
9.3.2 Information Not Within the Scope of Confidential Information 53
9.3.3 Responsibility to Protect Confidential Information 53
9.4 Privacy of Personal Information 53
9.4.1 Privacy Plan 53
9.4.2 Information Treated as Private 54
9.4.3 Information Not Deemed Private 54
9.4.4 Responsibility to Protect Private Information 54
9.4.5 Notice and Consent to Use Private Information 54
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 54
9.4.7 Other Information Disclosure Circumstances 54
9.5 Intellectual Property Rights 54
9.6 Representations and Warranties 55
9.7 Limitations of warranty 55
9.8 Limitations of Liability 55
9.9 Indemnities 55
9.10 Term and Termination 55
9.11 Individual Notices and Communications with Participants 55
9.12 Amendments 55
9.13 Dispute Resolution Provisions 55
9.14 Governing Law 55
9.15 Compliance with Applicable Law 56
9.16 Miscellaneous Provisions 56
9.16.1 Severability 56
9.16.2 Enforcement 56
9.16.3 Force Majeure 56

REFERENCES 57

1 Introduction

This document contains the integrated *Qualified Certificate Policy* and *Certification Practice Statement* concerning the qualified Time Stamp service of TrustPro QTSP Ltd Time Stamp Authority (hereinafter the *Provider*).

The *Provider* provides its services for its *clients* under contractual relationship.

The present document describes the framework of the provision of the mentioned services, includes the detailed procedures and miscellaneous operating rules, and makes recommendations for the *Relying Parties* for the verification of the timestamps created by the services.

This document complies with the requirements set by the eIDAS Regulation; the service provided according to these regulations is an EU qualified trust service.

TrustPro QTSP Ltd is registered as a trust service provider by DCCAE – Department of Communications, Climate Action and Environment.

1.1 Overview

The service provided by the *Provider* complies with the Best Practices Time Stamp Policy (BTSP) as defined in ETSI 319 421 identified by the OID: 0.4.0.2023.1.1.

Digital time stamping service is provided for both digitally signed and unsigned documents. The time stamping service allows anybody to establish the existence of a computer document before a certain time, associating a date and time from a certified time source with the digital evidence obtained from the document. The timestamp is a digitally signed data record that securely and verifiably links any digital document to a time reference (date and time). The timestamp is signed and issued by a trust service provider that provides time stamping systems (Time Stamping Authority (TSA)) that certifies the trust system keys (Time Stamp Unit (TSU)) to which users direct their requests according to need; anyone who has requested and stored a time stamp for a particular document will subsequently be able to prove that this document actually existed at the date/time reported in the stamp signed by that TSU/TSA certification chain.

In particular, the digitally signed document time stamp allows for the verification and validation of the digital signature, even if the author's

certificate is expired or revoked, provided that the time stamp was assigned to the document when the certificate was valid.

This document summarizes all the information the *Client*s should know. This aims to foster that:

- Clients and future Clients get better acquainted with the details and requirements of the services provided by the *Provider*, and the practical background of the service provision,
- the Clients be able to see through the operation of the *Provider*, and thus more easily decide whether the services comply, or which type of services meet their individual needs and expectations.

The content and format of the present document complies with the requirements of the RFC 3647 [13] framework.

Requirements for end user activity related to the used services can be contained besides the present document in the *General Terms and Conditions* of the service agreement concluded with the provider, the Certificate Policies applied by the *Provider*, and other regulation or document independent from the *Provider* as well.

1.2 Document Name and Identification

Issuer	TrustPro QTSP Ltd Time Stamp Authority
Document name	Time Stamp Authority Practice Statement – Certificate Policy
Code	**QTSP-TSA-CP/CPS**
Document version	1.0
Date of effect	07-03-2023
OID	1.3.6.1.4.1.52969.2

1.2.1 Effect

The present document shall be reviewed at least annually and their amendment to the potentially changed requirements and prerequisites shall be ensured.

Subject Scope	This document is related to the provision and usage of the services concerning the issuance of qualified time

	stamps.
Temporal Scope	The present version of this document is effective from the date of effect, until withdrawal. The effect automatically terminates at the cessation of services.
Personal Scope	The effect of this document extends each of the participants mentioned in section 1.3.
Geographical Scope	The present TSA Practice *Statement* includes specific requirements for services primarily provided for European *Clients*, operating by the European law. The *Provider* can extend the geographical scope of the service, in this case, it shall use not less stringent requirements than those applicable to European conditions.

1.3 Participants and responsibilities

The participants applying the services provided within the framework of present document are:

- TrustPro QTSP Ltd Time Stamp Authority,
- the Clients of TrustPro QTSP Ltd Time Stamp Authority (Subscribers),
- relying parties,
- other participants.

1.3.1 TrustPro QTSP Time Stamp Authority

TrustPro QTSP Time Stamp Authority (TSA) is the trusted third party that provides the time stamping service. TrustPro is the trust service provider (TSA) that provides the qualified time stamping service (TSU) by operating in accordance with the eIDAS Regulation and the European Telecommunications Standards Institute standards (ETSI).

Provider data

Name	TrustPro QTSP Time Stamp Authority
Company	TrustPro QTSP Ltd
Head office	Guinness Enterprise Centre Taylor's Lane, Dublin 8

	Ireland, D08 N9EX
Telephone number	+353 14861130
Internet address	https://www.trustpro.eu
Online H24 7x7 customer support	https://support.trustpro.eu

TrustPro QTSP Ltd is qualified trust service provider according to the 910/2014/EU Regulation [1] (hereinafter: eIDAS), established in Ireland and operates as an independent business unit.

TrustPro QTSP highlights the importance of *Client* experience and security. To maintain a high level of services, the *Provider* outsources services preferably to companies with quality management system compliant with the ISO 9001 standard and information security management system compliant with ISO 27001 [14] standard.

1.3.2 Subscribers

The *Subscriber* is the natural or legal person to whom the time stamp is provided and who enters in contract relationship with the Provider.

1.3.3 Relying Parties

The Relying Party is not necessarily in a contractual relationship with the Provider.

The Provider maintains its contacts with the Relying Parties mainly through its website.

1.4 Permitted Usage

Time stamps issued by the Provider, as specified in this CPS, are qualified under the eIDAS Regulation.

The certificate issued by the TSA will be used to verify the stamp.

Any use outside the limits and contexts specified in the CPS and contracts is prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The organization administering the present *Certification Practice Statement* is TrustPro QTSP Time Stamp Authority, as defined in section 1.3.1.

1.5.2 Contact Person

Questions related to the present *Certification Practice Statement* can be addressed at info@trustpro.eu.

1.5.3 Entity Responsible for the Suitability of the Practice Statement for the *Qualified Signature Certificate Policy*

The provider that issued the *Certification Practice Statement* is responsible for its conformity with the Qualified Signature Certificate Policy referenced in it and for the provision of the service according to the regulations contained therein.

The *Certification Practice Statements* and the provision of the services are supervised by Department of Communications, Climate Action and Environment (DCCAE), hereinafter National Authority.

1.5.4 CP-CPS Approval Procedures

The approval and the issuance of the new or any modified versions of this document is under control of the TrustPro QTSP steering committee.

1.6 Definitions and Acronyms

1.6.1 Definitions

Certificate	The electronic time stamp unit certificate, issued within the framework of the Trust Service by the service provider, which includes the certificate related verification data and the certificate usage related information, and which as an electronic document is reliably protected against the available counterfeiting technologies at the time of the issuance and during its validity period
Certificate Policy	A Trust Service Policy which concerns the

	Certificate issued within the framework of the Trust Service
Client	The collective term for the Subscriber and every related Subject denomination
Compromise	A cryptographic key is compromised when unauthorized persons might have gained access to it
Cryptographic Key	An individual digital signal series controlling cryptographic transformation, the knowledge of which is required for encryption, decryption, electronic signature creation and verification
Data Center	A facility designed for the placement and operation of computer systems and associated components. These components typically include telecommunications systems and communication connections, redundant power supply, data storage, air conditioning, fire protection and safety systems
Electronic Signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign
Electronic Time Stamp	Means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time
Extraordinary Operational Situation	An extraordinary situation causing disturbance during the operation of the Trust Service Provider, when the continuation of the normal operation of the Trust Service Provider is not possible either temporarily or permanently
Hash	A fixed-length bit string that is dependent on the electronic document, from which it is derived from, with a very small probability that two different documents would have the same hash, and it is practically impossible prepare a document with the same hash.
Hardware Security Module (HSM)	A hardware-based secure tool that generates, stores, and protects cryptographic keys and provides a secure

	environment for the implementation of cryptographic functions
Intermediate Certification Unit	A Certification Unit whose Certificate was issued by another Certification Unit
Key Management	The production of cryptographic keys, their delivery to users or its algorithmic implementation, as well as the registration, storage, archival, revocation, suspension and termination of keys which are closely linked to the used security method
Organization Administrator	That natural person who is eligible to act during the application, reinstatement and revocation or suspension of the Certificates issued to the Organization and to grant the issuance of organization related personal electronic signature. Certificates and the revocation or suspension of such Certificate. The Organization administrator can be appointed by a person eligible for representing the organization. Designation of an Organization Administrator is not compulsory for every Organization, if not designated, then the person eligible to represent the Organization performs the tasks aforementioned
Private Key	In the public key infrastructure, the element of an asymmetric cryptographic key pair for an actor that the Subject shall keep strictly secret. In case of electronic signatures, the Signatory generates the signature with the help of the private key. During the issuance of Certificates, the Certification Authority uses the private keys of the Certification Unit for placing an electronic signature or seal on the Certificate to protect it
Public Key	In the public key infrastructure, the element of an asymmetric cryptographic key pair belonging to an actor, which should be made public. The disclosure is typically in the form of a Certificate, which links the name of the actor with its public key. In case of an electronic signature, the public key of the signature creator party is needed to verify the signature

	authenticity. The authenticity of the Certificates can be verified with the public key of the Certification Unit
Qualified Electronic Time Stamp	An electronic Time Stamp which meets the requirements laid down in Article 42 of the eIDAS regulation [1]
Qualified Trust Service	A Trust Service that meets the applicable requirements laid down in the eIDAS Regulation
Qualified Trust Service Provider	A Trust Service Provider who provides one or more Qualified Trust Services and is granted the qualified status by the supervisory body
Relying Party	Recipient of the electronic document, who acts relying on the electronic signature based on a given certificate
Represented Organization	If the Certificate is issued to the Subject for the purpose of using it for its activities or for signing on behalf of the Organization then the Represented Organization is the Organization in question, which is also specified in the Certificate
Revocation	Revocation is the termination of the Certificate's validity before the end of the validity period indicated on the Certificate. The Certificate revocation is permanent, the revoked Certificate cannot be reinstated any more
Suspension	The certificate validity can be suspended before the end of the Certificate validity. The suspension state can be removed or passed to revoked.
Root Certificate	Also known as top level certificate. Self-signed Certificate, which is issued by a specific Certification Unit for itself, which is signed with its own private key, so it can be verified with the Signature-Verification Data – indicated on the certificate
Service Agreement	The contract between the Trust Service Provider and the Trust Service client, which includes the conditions for the provision of the Trust Service and for using the services
Subscriber	A person or organization signing the service agreement with the Trust Service Provider in order to use some of its services
Trust Service	Means an electronic service normally

	provided for remuneration which consists of: the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or the creation, verification, and validation of Website Authentication Certificate; or the preservation of electronic signatures, seals or certificates related to those services
Trust Service Policy	A set of rules in which a *Trust Service Provider*, relying party or other person requires conditions for the usage of the *Trust Service* for a community of the relying parties and/or a class of applications with common safety requirements
Trust Service Practice Statement	The statement of the Trust Service Provider of the detailed procedures or other operational requirements used in connection with the provision of specific Trust Services
Trust Service Provider	A natural or a legal person who provides one or more *Trust Service*s either as a qualified or as a non-qualified *Trust Service*
Trust Service Supervisory Body	The National Authority, the supervising authority monitoring the *Trust Service*s
Validation	Means the process of verifying and confirming that an electronic signature or a seal is valid
Validation Chain	The electronic document or its hash, and the series of information assigned to one another (especially those certificates, information related to certificates, data used for signature or seal creation, the current status of the certificate, information on the withdrawal, as well as information on the validity data of the certificate issuer provider and its revocation or suspension information), with the help of which it can be established that the advanced or qualified electronic signature, seal or time-stamp placed on the electronic document was valid at the

	time of the signature, seal or time-stamp placement.
Validation Data	Means data that is used to validate an electronic signature or an electronic seal

1.6.2 Acronyms

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
eIDAS	electronic Identification, Authentication and Signature
HSM	Hardware Security Module
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy
RA	Registration Authority
TSP	Trust Service Provider
TSA	Time-Stamping Authority: Trust service provider using one or more time stamp emission systems - see ETSI 319 421 [21]
TST	Time-Stamp Token: term used in international advertising for the time stamp
TSU	Time-Stamping Unit: a set of hardware and software managed as a single time stamping system consisting of only one active key - see ETSI 319 421 [21]
UTC	Coordinated Universal Time as defined in ITU-R TF.460-6 (2000) - see ETSI 319 421 [21]

2 Publication and Repository Responsibilities

The *Provider* discloses contractual conditions and policies electronically on its website.

The new documents to be introduced are disclosed on the website 30 days before coming into force.

Any change in the provision of qualified trust services described in this document will be notified to the National Authority (DCCAE), as well as the intention to cease services provided.

The documents in force are available on the site in addition to all previous versions of all documents.

The *Provider* notifies its *clients* about the change of the *General Terms and Conditions.*

All documents published are original and signed by the Provider with Qualfied Electronic Signature.

2.1 Repositories

The *Provider* publishes this document, other policy documents, terms, and conditions its operation is based on, CA certificates, certificates owners have chosen to publish, and other trust centre related informations on this web page:

https://docs.trustpro.eu

The *Certification Authority* guarantees, that the availability of its system publishing its service *Certificates*, the *Certificate Repository* and the revocation or suspension status information on an annual basis will be available at least 99.95% per year, while service downtimes may not exceed at most 3 hours in each case.

2.2 Time stamp preservation

All time stamps emitted are stored in a digital archive for twenty years.

2.3 Publication of the public key for time stamp verification

The integrity and authenticity of the TSU server public key is guaranteed as it is distributed by issuing a public key certificate:

- The certification request is issued by authorised personnel and forwarded to CA dedicated to the certification of time stamp keys.
- The CA generates the certificate.

The time stamp certificate format, containing the TSU public key, meets that specified in ETSI 319422 [22], in this way full readability and verifiability is guaranteed in the context of eIDAS.

The public key used by TSU is distributed through the certificate.

2.4 Time or Frequency of Publication

2.4.1 Frequency of the Publication of Terms and Conditions

The disclosure of this document and related new versions are compliant with the terms described in Section 9

The *Provider* discloses other regulations, contractual conditions, and their new versions if necessary.

The *Provider* publishes extraordinary information without delay in accordance with the legal requirements and in the absence thereof when necessary.

2.4.2 Frequency of the Certificates Disclosure

The *Provider* regarding the disclosure of some *Certificate*s follows the practices below:

- the *Certificate*s of the root certification units operated by it are disclosed before commencing the service.

2.4.3 Access Controls on Repositories

Access is provided to anyone for reading purposes to public information of the Certificates and status information disclosed by the Certification Authority

according to the particularities of publication. The information disclosed by the Certification Authority shall only be amended, deleted, or modified by the Certification Authority. The Certification Authority shall prevent unauthorized changes to the information.

3 Identification and Authentication

3.1 Name

3.1.1 Type of names

The key used by the TSU in the certificate is identified with the assigned Distinguished Name (DN), which should therefore be valued and compliant with the X500 standard. Certificates are issued according to ETSI standards for issuing qualified certificates for time stamping.

3.1.2 Need for names to be meaningful

The Distinguished Name (DN) certificate identifies the TSU as a Time Stamping Unit, in the Organization Unit "Qualified Time Stamping Authority".

3.1.3 Applicants' anonymity and pseudonym

n/a

3.1.4 Interpretation rules of the types of names

The Provider complies with the X500 standard.

3.1.5 Unequivocalness of the names

The Distinguished Name (DN) certificate contains a name that identifies the TSU used, the month and year of issue: each TSU uses a unique certificate.

3.2 Initial identity validation

n/a

3.3 Identification and authentication for the renewal of the keys and certificates

n/a

3.4 Identification and authentication for revocation or suspension requests

n/a

4 Operational Requirements

4.1 Request for time stamp emission or verification

4.1.1 Who can apply for time stamp emission or verification

The time stamping service is intended to address time stamp emission or verification request for electronic documents from the TSU server by means of properly configured software modules.

The request for time stamp emission or verification may be made by the Applicant using the signature/verification software provided by the Provider, which allows you to affix the timestamp to digitally signed and non-signed documents and allows immediate verification.

The Applicant may use its own software through a protocol defined in RFC 3161 [23], RFC 5816 [24] and profiled by the ETSI 319 422 [22] standard using URLs and credentials agreed with the Provider.

Once the request has been accepted and registered and proper checks are carried out, the TSU server processes it, generates the time stamp and sends it back to the Applicant.

4.1.2 Registration process and responsibility

In the process, the different figures involved have different roles and run parallel with the successful outcome of the issuance:

- The Applicant is responsible for submitting the request for time stamp issuance or verification.
- The Provider is ultimately responsible for the success of the time stamp generation process.

4.2 Processing the request

The request is processed as follows:

- The Applicant submits, through TSA's procedures, a time stamp request for the

electronic document to the TSU server, eventually viewing it;

- the request contains the imprint of the electronic document to be stamped using the SHA256 imprint algorithm (secure hash algorithm 256-bit).

4.3 Time Stamp creation

The time stamp is automatically issued by a secure electronic system (TSU server), managed by TSA, able to:

- accurately calculate the date and time of time stamp generation with reference to Coordinated Universal Time (UTC),
- generate the data record containing the specified information,
- digitally sign (in the technical meaning of the term) the data record.

Upon receipt of the request, the time stamp is issued as follows:

- The TSU, upon receipt of the time stamp request, generates the data record: this record contains, amongst the various information, the same imprint and the current date/time,
- The TSU server signs the generated data record, obtaining the time stamp,
- When the time stamp generation procedure has successfully completed, the latter is sent to the Subject.

4.4 Acceptance of the certificate

n/a

4.5 Key pair and certificate usage

n/a The pair of keys and stamp certificate are solely used to sign the association between the datetime and the imprint of the document.

4.6 Certificate renewal

n/a.

4.7 Re-issuing the certificate

A new certificate is issued for each TSU before the current certificate expires.

4.8 Certificate modification

n/a

4.9 Certificate Status Services

The *Provider* provides the following possibilities for the *Certificate* status query:

- OCSP – online *Certificate* revocation status query service,
- CRL – certificate revocation lists.

In case of revocation the new status of the *Certificate* appears instantly in the revocation records of *Provider* after the successful completion of the process. From that moment, the OCSP responses provided by the *Provider* shall contain the new revocation status of the certificate.

Certificate revocation status is maintained for 20 years after certificate revocation. CRL includes the OID "ExpiredCertsOnCRL" and OCSP response includes, for expired and revoked certificates, the attribute "ArchiveCutOff".

The *Provider* issues an extraordinary and last CRL with next update field value as defined in ETSI EN 319411-1 in case of *Certificate* revocation due to key compromise instantly after recording the event.

OCSP response issued by the *Provider* shall not contain "good" status information for *Certificates* that were not issued by the given certification unit (positive OCSP).

In case of Provider termination, the lists of revoked certificates will be kept online for a period of not less than five years.

4.9.1 Operational Characteristics

Each certification unit of the *Provider* issues revocation list with the frequency below:

- The "TrustPro QTSP Qualified TSA 1" certification unit issues a CRL once in at the most of 24 hours.

The effective date of the revocation lists "thisUpdate" marks also the time when the certification unit assembled and started signing the revocation list. After that, in case of long revocation lists the publication of the revocation list may even take 1 or 2 minutes. The appearance of the next revocation list ("nextUpdate") marks the next time, from what the list is publicly available. Accordingly, the time interval between the date of the revocation list entering into force, and the date of publication of the next revocation list can be longer than the time intervals above, but this does not affect the time interval between the appearance of the CRLs is at most 24 hours, and (in case of a CRL related to Certification Authority Certificates) 1 month.

Since the fastest and the easiest way to determine the validity of the certificate is the OCSP service, the *Certification Authority* recommends the use of OCSP to its *Client*s.

The *Provider* provides OCSP service according to the RFC 6960 "authorized responder" principle, so its every certification unit certifies separately an OCSP responder, which provides information on the revocation status of the *Certificate*s issued by the certification unit (section 1.3.1.).

The OCSP service is publicly and freely available to anybody. There is no need for authentication.

The OCSP service can be reached through the URLs indicated on the *Certificate*s.

The OCSP responses always contain the current information listed in the revocation registry of the *Provider*, but if the "thisUpdate" time of the OCSP response is earlier than the time for which the verification is carried out – which is either earlier or coincides with the time of the query –, then the OCSP response is not clear evidence for a third party regarding the revocation status of the *Certificate*.

4.9.2 Service Availability

The *Provider* ensures that the availability of the *Certificate Repository* and the terms and conditions pertaining to the *Certificate*s issued by the *Provider* is at least 99.95% per year, and the length of downtime shall not exceed at most 3 hours.

The *Provider* ensures that the availability of the revocation status information and the revocation management service is at least at least 99.95% per year, and the length of downtimes shall not exceed at most 3 hours on any occasion.

The response time of the revocation status service in case of normal operation is less than 10 seconds.

4.9.3 End of Subscription

n/a.

4.9.4 Key Escrow and Recovery

n/a.

5 Facility, Management and Operational Controls

The *Provider* applies physical, procedural, and staff security precautions that comply with acknowledged standards, along with the administrative and governance related procedures that enforce these.

The *Provider* keeps a record of the system units and resources related to the service provision and conducts a risk assessment on these. It uses protective measures proportional to the risks related to the individual elements.

The *Provider* monitors the capacity demands and ensures that the adequate processing power and storage are available for the provision of the service.

5.1 Physical Controls

The *Provider* takes care that physical access to critical services is controlled and keeps physical risk of the assets related to critical services at a minimum.

The purpose of physical precautions is to prevent illegitimate access, damage, and unauthorized access to the *Provider*'s information, and physical zones.

Services that process critical and sensitive information are implemented in a secure area provided by a selected supplier.

The provided protection is proportional to the identified threats of the risk analysis that the *Provider* has performed.

In order to provide adequate security:

- The *Provider* implements the strongly protected services in a protected computer room. This computer room has been designed and constructed specifically for this purpose, by its design uniform enforcement of various aspects of protection (the placement and structure of the site, physical access (access control and supervision), power supply, air conditioning, protection against water leakage and flooding, fire prevention and protection, media storage etc.) took place.
- The Customer Service office of the *Provider* was designed, to be able to meet the requirements for registration services under realistic costs.

- The *Provider* constructed its mobile registration units, so that they comply with the requirements imposed on the registration service.
- The *Provider* requires its external offices and mobile units to have the same security level as the security of the *Provider* registration office and mobile units. The conditions and the expectations of the *Provider* are recorded in the contract with the *Local Registration Authority*.
- The *Provider* implements every critical service and every necessary tool in a separate security zone. All the devices necessary for this are placed in a protected computer room.

5.1.1 Site Location and Construction

The IT system of the *Provider* is located and operated within a properly secured *Data Centre* with physical and logical protection that prevents illegitimate access. Defensive solutions – as for example guarding, security locks, intrusion detection systems, video surveillance system, access control system – are applied.

5.1.2 Physical Access

The *Provider* protects devices and equipment that take part in the service provision from unauthorized physical access in order to prevent tampering with the devices.

Provider ensures that:

- each entry to the *Data Centre* is registered;
- persons without independent authorization can only stay in the *Data Centre* in justified cases, for the time required and accompanied by the staff with appropriate rights;
- the entry logs shall be archived continuously and available for evaluation

In the presence of unauthorized persons:

- data media containing sensitive information are physically out of reach;
- the logged-in terminals are not left without supervision;
- no work process is carried out during which confidential information may be revealed.

When leaving the computer room, the administrator shall verify that:

- every equipment of the Data Centre is in an adequately secure operation state,
- there's no terminal left logged-in,
- physical storage devices are locked properly,
- systems, devices providing physical protection operate properly,
- the alarm system has been activated.

There are appointed responsible people to carry out regular physical security assessments. The results of the examinations are recorded in the appropriate log entries.

5.1.3 Power and Air Conditioning

The *Supplier* applies an uninterruptible power supply unit in the *Data Centre* that:

- has adequate capacity to ensure power supply for the *Data Centre*'s IT and subsidiary facility systems,
- protects IT equipment from voltage fluctuations in the external network, power outages, spikes and other,
- in case of lasting power outage has its own power generation equipment, which – by allowing refuel – is able to provide the necessary energy for any period of time.

The air of the outer environment does not get into the *Data Centre* directly. The *Data Centre* air purity is ensured with adequate filter system to detect a variety of contaminants from the air (dust, pollutants, and corrosive materials, toxic or flammable substances). The ventilation system provides the necessary amount of fresh air with adequate filtration for the safe working conditions of the operators.

The humidity is reduced to the level required by the IT systems.

The *Supplier* uses cooling systems with proper performance to provide the necessary operating temperature, to prevent overheating of IT devices.

5.1.4 Water Exposures

The *Data Centre* of the *Supplier* is adequately protected from water intrusion and flooding.

The total area of the security zone is free from sanitary facilities, there is not any drain or water pipe close to it. The total area of water security zone is monitored by an intrusion detection system. In the protected computer room security is further increased by the use of a raised floor.

5.1.5 Fire Prevention and Protection

In the *Data Centre* of the *Supplier*, a fire protection system approved by the competent fire headquarters operates. Smoke and fire detectors automatically alert the fire brigade. Water vapor based, automatic fire extinguishing system has been installed in the computer room, which is not hazardous to human life, and does not damage the IT equipment.

There is the type and quantity of manual fire extinguishers in accordance with the relevant regulations at clearly visible locations in each room.

5.1.6 Media Storage

The *Provider* does not use removable physical media storage.

5.1.7 Waste Disposal

The *Supplier* ensures the environmental standards compliant disposal of the superfluous assets, and media.

The Provider does not use the electronic storage media containing information classified as confidential even for storing data classified as not confidential after deleting their content and devices like that shall not be taken outside of the premises of the *Provider*. The *Provider* physically destroys – according to the rules of disposal – the defective for any other reason unusable, redundant media storages containing confidential classified information:

5.1.8 Backup

The *Provider* creates a backup daily from which the whole service could be restored in case of a fatal error. The backups – at least including the last full backup – are stored in an external location that's physical and operational protection is identical to the primary site. The secure data transmission from the primary to the backup locations is resolved.

5.2 Procedural Controls

The *Provider* takes care that its systems are operated securely, according to the rules, and with a minimal risk of defects.

Procedural precautions have the objective of supplementing, and at the same time intensifying the effectiveness of physical safeguards, along with those applicable to the staff, by means of appointing and isolating trusted roles, documenting the responsibilities of various roles, as well as specifying the personnel headcounts and exclusion roles necessary for the various tasks, moreover identification and authentication expected in the various roles.

The *Provider*'s internal governance system ensures that its operation complies with legal, as well as its internal regulations. In its system a responsible person shall be clearly assigned for every given system unit and process.

Individuals responsible for a given system element or process are assigned unambiguously to every system element and every process in its system. Development and operations related tasks are sharply segregated in the *Provider*'s system. The auditing activity of the independent system auditor and the *Provider* 's internal auditor ensures the system's appropriate operation.

5.2.1 Trusted Roles

The *Provider* creates trusted roles (in the wording of the regulation, scope of activities) for the performance of its tasks. The rights and functions are shared among the various trusted roles in such a way that one user alone shall not be able to bypass the security protection measures.

The *Provider* defines the following trusted roles, with the following responsibilities:

Manager with overall responsibility for the IT system of the *Provider*	The individual responsible for the IT system
Security officer	Senior security associate, the individual with overall responsibility for the security of the service.
System administrator	Infrastructure administrator. The individual with the task to install, configure and maintain the systems of the *Provider*. Responsible, for the reliable and continuous operation of the assigned system units, and for monitoring

	the development of technology, and for the detection and proposing of development solutions of the vulnerabilities of each system component.
System Operator	System operator, individual performing the IT system's continuous operation, backup and restore.
System auditor	Individual who audits the logged, as well as archived dataset of the *Provider*, responsible for verifying the enforcement of control measures the service provider implements in the interest of operation that complies with regulations, moreover for the continuous auditing and monitoring of existing procedures.

For the provision of trusted roles, the manager responsible for the security of the *Provider* formally appoints the Provider's employees.

Only those persons may hold a trusted role who are in employment relationship or commission contract with the *Provider*.

Up to date records are kept of the trusted roles and in case of any change, the national authority is notified without delay.

5.2.2 Roles Requiring Separation of Duties

Employees of the *Provider* can hold multiple trusted roles at the same time, but the *Provider* ensures that:

- the security officer and the registration officer shall not hold the independent system auditor role,
- the system administrator shall not hold the security officer and the independent system auditor role,
- the manager with overall responsibility for the IT system shall not hold the security officer and the independent system auditor role.

In addition to the aforementioned, the *Provider* seeks the complete separation of trusted roles.

5.3 Staff Controls

The *Provider* takes care that its staff policy, and its practices applicable to employing staff members intensify and support the reliability of the *Provider* 's operation. The objective of precautions applicable to staff is to reduce the risk of human errors, theft, fraud and cases of misuse.

The *Provider* addresses staff security already during the hiring stage, including the conclusion of contracts, as well as their validation when they are being employed. In the case of all trusted roles, applicants have valid certificate of no criminal record at the time of the application. Every employee in a trusted role and external parties – who get in contact with the *Provider*'s services shall sign a non-disclosure agreement.

At the same time, the *Provider* ensures for its employees obtaining a common, general know-how along with the specialized professional knowledge necessary for performing the various jobs.

5.3.1 Qualifications, Experience, and Clearance Requirements

The *Provider* requires at least intermediate education degree, as hiring requirement and the *Provider* continues to take care that employees receive appropriate training. Immediately after recruitment, the *Provider* grants a training for its new employees, under the course of which they acquire the knowledge necessary to carry out the job. The *Provider* usually supports the professional development of the employees, but it also expects employees to independently develop their skills in their respective fields.

Trusted roles can be held at the Provider only by persons, who have no external influence and possess the necessary expertise validated by the *Provider*.

5.3.2 Background Check Procedures

The *Provider* only hires employees for trusted or leading roles, who

- have a clean record and there's no proceeding in progress against them
- are not subject to professional disqualifications prohibiting to exercise electronic signatures related services.

The *Provider* verifies the authenticity of the relevant information given in the applicant's CV during the hiring process.

5.3.3 Training Requirements

The *Provider* trains the newly recruited employees, over the course of which they acquire

- basic PKI knowledge,
- the specifics and the way of handling the *Provider* 's IT system,
- the necessary special knowledge for fulfilling their scope of activities,
- processes and procedures defined in the public and inner regulations of the *Provider*,
- the legal consequences of the individual activities,
- the applicable IT security regulations to the extent necessary to the specific scope of activities,
- the data protection rules.

The *Provider* trains the employees concerned with registration about the dangers and risks related to the verification of the data to be indicated on the Certificate.

The employees concerned with registration take and pass an exam on the knowledge of the related requirements and procedures for data verification before their appointment, and this fact is documented by the *Provider*.

Only employees having passed the training shall gain access to the he production IT system of the *Provider*.

5.3.4 Retraining Frequency and Requirements

The *Provider* ensures that the employees have the necessary knowledge continuously, so, if needed, further or repeater type of training is held.

Further training is held if there's a relevant change within the processes or the IT system of the *Provider*.

The training is adequately documented, from what the syllabus and the scope of the participator employees can be clearly determined.

5.3.5 Job Rotation Frequency and Sequence

The *Provider* does not apply mandatory rotation between individual work schedules.

5.3.6 Sanctions for Unauthorized Actions

The *Provider* regulates the prosecution possibilities of the employees in an employment contract in case of failures, errors, accidental or intentional damage. If the employee – due to negligence or intentionally – violates their obligations, sanctions could be taken against him by the *Provider*, which it sets out having regard to the offense and the consequences.

5.3.7 Independent Contractor Requirements

The *Provider* selects persons employed with engagement contract or subcontract to perform the other tasks, choosing if possible, from the list of qualified suppliers. The *Provider* concludes a written contract before working with suppliers.

Each contracting party – before the start of the active work – signs a confidentiality statement in which he agrees that the business / corporate secrets learned later on will not be covered up to unauthorized persons and will not be exploited in any other way. The confidentiality statement includes sanctions in case of violation. External employees employed under the contract are expected to have appropriate technical skills, and the *Provider* does not hold any trainings for them.

5.3.8 Documentation Supplied to Staff

The *Provider* continuously provides for the employees the availability of the current documentation and regulations necessary to perform their roles.

Each employee in trusted role receives the following documents:

- the organizational security regulations of the Provider,
- the signed confidentiality agreement,
- educational materials on the planned or special training for the specific form of education.

All employees are informed in a written notice about any changes in the organizational safety regulations.

5.4 Audit Logging Procedures

To maintain a secure IT environment, the *Provider* implements and operates an event logger and control system covering its full IT system.

5.4.1 Types of Events Recorded

The *Provider* logs every security-related event that can provide information on changes happened in the IT system or in its physical environment according to the generally accepted information security practice. For every log entry, it stores the following data:

- the time of the event,
- the type of the event,
- the success or failure of the implementation (if applicable),
- the identification of the user or the system who/that triggered the event.

All the essential event logs are available to the independent system auditors, who examine the compliance of the *Provider*'s operation.

5.4.2 Frequency of Audit Log Processing

The independent system auditors of the *Provider* evaluate the generated log files with the frequency defined in security procedures.

During the evaluation, the authenticity and integrity of the examined logs is ensured, the error messages in the logs are checked and if needed, document the differences and take measures to eliminate the cause of the deviation.

For the IT system evaluation, the *Provider* uses automated evaluation tools too, that are used to monitor the resulting log entries according to pre-set criteria and, where necessary, alert the operational staff.

The fact of the investigation, the results of the investigation and the measures undertaken to avert deficiencies found are properly documented.

5.4.3 Retention Period for Audit Log

Before the deletion from the on-line system, the logs are archived, and their secure preservation is ensured by the Provider for 6 months.

For that time period, the *Provider* ensures the readability of archived data, and maintains the necessary software and hardware tools necessary for that.

5.4.4 Protection of Audit Log

The *Provider* protects the created logs for the required preservation time. During the whole preservation time, the following properties of the logs' data is ensured:

- protection against unauthorized disclosure: only authorized persons – primarily the independent system auditors – access the logs;
- availability: authorized persons are granted access to the logs;
- integrity: any data alteration, deletion in the log files and change in the order of the entries, etc. is prevented.

The *Provider* protects the log records with qualified *Time Stamps*, and they are stored in a way excluding the seamless insertion and deletion of the log entries.

The log files are protected against accidental and malicious damage by backups. In case of log entries containing personal data, the *Provider* makes sure of the confidential storage of the data. Only those individuals are entitled to access to the log entries, who absolutely need it for their work. The *Provider* verifies the accesses in a secure way. The *Provider* preserves the log files in a secure environment. Keeps copies of the files at the second operation site.

5.4.5 Audit Log Backup Procedures

Daily log files are created from the continuously generated log entries during the operation in each system.

The daily log files are archived in two copies after the evaluation and stored physically apart from each other, at separate sites for the required time.

The exact process of backups is defined in the backup regulations of the *Provider*.

5.4.6 Audit Collection System

Each application automatically collects and sends the records to the logging system.

The logging functions start automatically at the time of the system launch and they are run continuously during the entire period of system operation.

In case of any anomaly in the automatic examiner and logging systems, the operation of the related areas is suspended by the *Provider* until the incident is resolved.

5.4.7 Notification to Event-causing Subject

The persons, organizations and applications that caused the error event are not always notified, but if necessary, the *Provider* involves them in the investigation of the event. The *Clients* affected by triggering the event has the duty to cooperate with the *Provider* to explore the event.

5.4.8 Vulnerability Assessments

The *Provider* periodically review extraordinary events and perform analysis of vulnerability, based on which the *Provider* if necessary, takes measures to increase the security of the system.

5.5 Records Archival

5.5.1 Types of Records Archived

The main record types archived for long-term by the *Provider* are:

- every document related to the accreditation of the *Provider (document)*;
- all issued versions of the Certificate Policies and Certification Practice Statements (documents);
- all issued versions of the *Terms and Conditions (*documents*)*;
- contracts related to the operation of the *Provider* (documents);
- all informations related to the Subject and Subscriber registration (records);
- information related to the Certificate for the whole lifecycle (records);

5.5.2 Retention Period for Archive

The *Provider* preserves the archived data for 20 years after related certificate expiration date.

5.5.3 Protection of Archive

The *Provider* stores all archived data in two copies at locations physically apart from each

other. Authentic paper or electronic copy is made in accordance with the applicable law from the only authentic paper-based copy of the document available.

Each of the two locations fulfils the requirements for archiving security and other requirements. During the preservation of the archived data, it is ensured that:

- their integrity is preserved,
- they are protected against unauthorized access,
- they are available,
- they preserve authenticity.

The archived electronic documents are provided with a qualified electronic signature or seal and a qualified *Time Stamp*.

5.5.4 Archive Backup Procedures

The *Provider* stores the paper documents in a single original copy and makes an authentic electronic copy of the original in accordance with the relevant legislation. Electronic copies are stored according to the same rules as other protected electronic documents.

5.5.5 Archive Collection System

The log entries are generated in the *Provider*'s protected computer system, and only the log files that are electronically protected with qualified timestamps can leave it.

One original copy of the documents created during the service provision is stored and protected by the *Provider* in an inner data storage operated by it.

5.5.6 Procedures to Obtain and Verify Archive Information

The archived documents are protected from unauthorized access.

Controlled access to the archived documents is only available to the eligible persons:

- *Clients* are eligible to see the data stored about them;
- in legal litigation in order to provide evidence the necessary data shall be provided.

5.6 TSU Key Changeover

The *Provider* ensures that the used *Time Stamping Units* are continuously possessing a valid key and Certificate for their operation. For that purpose, sufficient time before the expiration of their Certificates, and the usage expiration of the keys related to them, it generates a new key pair for the *Time Stamping Units*. The new provider key is generated and managed according to this regulation.

5.7 Compromise and Disaster Recovery

The *Provider* maintains a Disaster Recovery site, at a safe distance from the primary location with a replica of production hardware and software infrastructure. A fully backup of data is maintained between primary and disaster recovery infrastructure.

In case of disaster, the *Provider* takes all necessary measures in order to minimize the damage resulting from the unavailability of the service and restores the services as quickly as possible.

Based on the assessment of the incident that occurred, the Provider takes the necessary amendments, corrective measures to prevent future occurrence of the incident.

Once the problem is resolved, the event is reported to the National Authority, as the supervisory authority.

The *Provider* periodically tests the changeover to the Disaster Recovery system and reviews its business continuity plans.

5.7.1 Corruption of Resources, Software, and Data

The IT systems of the *Provider* are built of reliable hardware and software components. The critical functions are implemented using redundant system elements so that in the event of an item failure they are able to operate further.

The business continuity plan of the *Provider* includes accurate requirements for the tasks to be performed in case of critical system component failure.

5.7.1 Entity Private Key Compromise Procedures

In case of the *Trust Service Provider* 's private key compromise, the following steps will be taken without delay:

- all of the affected Certificates of the *Trust Service Provider* shall be revoked,
- new provider private key shall be generated for the restoration of the services,
- the revoked provider Certificate's data shall be disclosed according to the regulated method in Section 2.2,
- the information related to the compromise shall be disclosed for every *Subscriber*,
- the *Provider* publishes a notice about the provider public key revocation.

5.7.2 Business Continuity Capabilities After a Disaster

The tasks to be performed in case of service failure due to natural or other disaster, are defined in the *Provider*'s business continuity plan.

The Provider has a supplier that performs the disaster recovery plan for the IT systems.

5.8 Termination of Time Stamp Service

In termination phase the Provider shall perform activities defined in its Termination Plan:

- the National Authority, the Relying parties and the *Subscribers* shall be notified about the planned termination in time (at least 90 days before),
- the *Trust Service Provider* shall make every effort to ensure that before the service termination another provider takes over the records and service obligations,
- new *Time Stamp* issuance shall be terminated,
- *Provider* TSU Certificates shall be revoked, and provider private keys shall be destroyed,
- after the termination of the service, a full system backup and archiving shall be carried out, including the last issued CRL,
- archived data shall be handed over to the provider that takes over the services,
- In case no other provider can be found at any condition all end user certificates shall be revoked and a final CRL shall be maintained until the expiration date of the last end user certificate issued.

6 Technical Security Controls

The *Provider* uses systems consisting of reliable, and safety technically assessed equipment for the provision of its services. The *Provider* manages the cryptographic provider keys during their whole lifecycle within a *Hardware Security Module* that has appropriate Certification.

Both the *Provider* and the system supplier and execution contractors have significant and long-term experience with PKI products, technologies and standards

6.1 TSU Key Pair Generation and Installation

The time stamp is signed with an asymmetric algorithm from a private key stored on a secure hardware device and the corresponding public key certified by the Provider Certification Authority dedicated to this service (TSA).

The pair of asymmetric keys is generated within a hardware encryption device (HSM) compliant with the security requirements provided by ETSI 319 421 [21].

The TSU asymmetric key pair generation devices can only be activated by authorised operators, working in pairs. One operator with administrative rights creates the TSU slot in the HSM and the procedure sends an activations code to another operator authorized to create the key pairs and the certificate.

6.1.1 Key algorithm and length

The pair of asymmetrical certification keys is generated inside the hardware encryption device mentioned above. The RSA asymmetrical algorithm with key length no less than 2048 bits is used.

6.1.2 Public key quality controls and generation

The devices used are certified according to high security standards (see § 6.2.1) and ensure that the public key is correct and random. The TSA, before issuing the certificate, verifies that the public key has not been used yet.

6.2 Key Pair Generation

The *Provider* uses key generation algorithms which comply with the requirements set out in the following normative:

ETSI TS 119 312 [8];

The *Provider* in case of the generation of a key pair of its own ensures:

- The creation of the private key of the provider is carried out in a protected environment (see section 5.1), with two trusted role holder (see section 5.2.1) authorized person simultaneously, excluding the presence of other unauthorized persons.
- The creation of the provider private key is carried out in compliant devices (see section 6.3)
- The production of provider private key is performed using the core TSA management application.
- The creation of the keys is carried out in a protected environment with exclusively trusted role holder persons present.

6.2.1 TSA Public Key Delivery to Relying Parties

The *Trust Service Provider* shall make available its top-level provider Certificates to the *Relying Parties* in such a way, that makes attacks targeting key modification impossible.

The public key is contained in the Certificate.

The *Provider* publishes certificates at this address:

https://docs.trustpro.eu

6.2.2 Key Sizes

The *Provider* uses algorithms and minimum key sizes, which comply with the requirements set out in the following standard:

ETSI TS 119 312 [8];

The *Provider* uses at least 4096 bit RSA keys in every currently active root *Certificate*.

6.2.3 Key Usage Purposes

The *Provider* root certification unit private key may only be used for the following purposes:

- issuance of the self-signed *Certificate* of the root certification unit itself,
- issuance of end user certificates
- to sign the OCSP responder *Certificate* or the OCSP response,
- to sign CRLs.

The *Provider* includes the Key Usage extensions in the end-user certificates defining the scope of the Certificate usage and in the X.509v3 [30] compatible applications technically restrict the usage of the Certificates.

6.2.4 Private Key Protection and Cryptographic Module Engineering Controls

The *Provider* ensures the secure management of the private keys held by it and prevents the private key disclosure, copy, deletion, modification and unauthorized usage. The *Provider* will preserve the private keys only as long as the provision of the service definitely requires.

6.2.5 Cryptographic Module Standards and Controls

The systems of the *Provider* issuing *Certificate*, signing OCSP responses and CRL lists store the private keys in hardware devices that are compliant with the following:

- the requirements of ISO/IEC 19790 [9], or
- the requirements of FIPS 140-2 [10] 3, or the requirements of a higher level, or
- the requirements of CEN 14167-2 [11] task force agreement, or
- they are such reliable systems that are evaluated at a guarantee level 4 or higher according to ISO/IEC 15408 [12] or an equivalent security criteria system. The assessment either shall be based on the appropriate security system plan that meets the requirements of the present document, or on security appropriations.

6.2.6 Private Key Multi-Person Control

The *Provider* implements the "2 out of 5" at the generation of the TSA private key. The parameters are determined so that the simultaneous presence of at least two

trusted role holder employees is needed for the critical operations carried out with its provider private keys.

6.2.7 Private Key Escrow

The *Provider* does not escrow its own provider private key.

6.2.8 Private Key Backup

The *Provider* makes security copies of its provider private keys, before putting the private key into service in a protected environment, in the simultaneous presence of at least two people holding trusted roles, with the exclusion of other people.

The same strict safety standards are applied to the management and preservation of backups as for the operation of the production system.

6.2.9 Private Key Archival

The *Provider* does not archive its private keys and the end-user signer private keys.

6.2.10 Private Key Transfer Into or From a Cryptographic Module

All of the provider private keys of the *Provider* are created in a *Hardware Security Module* that meets the requirements.

6.2.11 Private Key Storage on Cryptographic Module

The *Provider* keeps its private keys used for service provision in *Hardware Security Module*s.

6.3 Activation Data

The employees of the *Provider* manage the private key activation devices and the activation data securely, protect them using technical and organizational measures and passwords are stored in encrypted form only.

6.4 Computer Security Controls

6.4.1 Specific Computer Security Technical Requirements

During the configuration and operation of its IT system of the *Provider* ensures the compliance with the following requirements:

- the user identity is verified with two-factor authentication controls,
- roles are assigned to users and it ensures that all users only have permissions appropriate for his or her roles,
- a log entry is created for every transaction, and the log entries are archived,
- for the security-critical processes it is ensured that the internal network domains of the Provider are adequately protected from unauthorized access.

6.5 Life Cycle Technical Controls

The provider has defined as supplier company with an Information Security management system certified against the ISO 27001 [14] standard.

- The fundamental security control provided by the supplier, are:
- Access control
- Security of assets
- Operational security
- Security in software development
- Incident management
- Business continuity
- Network security

6.6 Time Accuracy

System time accuracy is guaranteed by paired time servers getting time from two distinct satellite constellations (Galileo and GPS). Time servers in the pair are in continuous reciprocal control, to ensure that the time difference is under one second. If the difference is one second or above one second the timestamp is not issued.

7 Certificate, CRL and OCSP Profiles

TSA certificates have following structure:

Version	Version 3
Serial Number	Serial number of the certificates
Signature	sha256, RSA
Issuer (ETSI 319 412-2 par. 4.2.3.1)	Issuer DN: **countryName**: "IE" **organizationName**: "TrustPro QTSP Ltd" **L**="Dublin" **OU**="QTSP" **organizationIdentifier** : "NTRIE-637218" **commonName** : [ROOT CA NAME]
Validity Period	20 Years (expire 20 years from the date of issue)
Subject	Subject DN: **countryName**: "IE" **organizationName**: "TrustPro QTSP Ltd" **L**="Dublin" **OU**="QTSP" **organizationIdentifier** : "NTRIE-637218" **commonName** : [TSA NAME]
SubjectPublicKeyInfo	Public Key 4096 bit Algorithm: RSA
Extensions	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
Basic Constraint (critical)	Subject Type: CA Path Length Constraint: 0
KeyUsage (critical)	CertSign, cRLSign
Policy Constraints	requireExplicitPolicy : 0

7.1 TSU Certificate Profiles

The TSU (Time Stamping Unit) *Certificates* issued by the *Provider* during the service comply with the following recommendations and requirements:

- ITU X.509 V3 Information technology - Open Systems Interconnection - The Directory: Public- key and attribute certificate frameworks [15]
- RFC 5280 [16]
- RFC 6818 [17]
- ETSI EN 319 411-1 [2]
- ETSI EN 319 411-2 [3]
- ETSI EN 319 412-1 [4]
- ETSI EN 319 412-2 [5]
- ETSI EN 319 412-3 [6]
- ETSI EN 319 412-5 [7]

7.1.1 Version Number

The provider certification unit *Certificates* used by the *Provider* and the end-user *Certificates* issued by the *Provider* are "v3" *Certificates* according to the X.509 V3 specification [15].

7.1.2 Certificate Extensions

The *Provider* only uses the certificate extensions according to the X.509 specification [15] and to the IETF RFC 3739 [18] (clause 3.2.6). The usage is performed according to standard ETSI 319 412-5 [7].

7.1.3 Algorithm Object Identifiers

The denomination of the algorithm that has been used to certify the *Certificate*. The following algorithms are used by the *Certification Authority* for sealing the end-user *Certificates*:

SHA256WithRSAEncryption

7.1.4 Name Forms

TSU certificate contains a unique serial number.

7.1.5 Name Constraints

The *Provider* does not use name constraints with the use of the "nameConstraints" field.

7.1.6 TSU Certificate Policy Object Identifiers

The Provider includes the not critical (Certificate Policy) extension in the Certificates according to the requirements of the Section 7.1.2 with following OID: 1.3.6.1.4.1.52969.2.1

7.1.7 TSU certificate profile details

TSU fields details are described in this section.

Serial Number	Certificate serial number
Issuer DN	**CN**=[TSA NAME] **C** ="IE" **O**="TrustPro QTSP Ltd" **OU**="Qualified Time Stamping Authority" **L**="Dublin" **organizationIdentifier**=" NTRIE-637218"
Subject DN	**CN**=[TSU NAME], **C**=IE, **l**=Dublin, 2.5.4.97=NTRIE-637218, **O**="TrustPro QTSP Ltd" OU=Qualified Time Stamping Authority
Validity Period	10 years
SubjectPublicKeyInfo	Public Key 2048 bit Algorithm: RSA
Extensions	

Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
Basic Constraint	Subject Type: NO CA Path Length Constraint: none
KeyUsage	Digital Signature
Extended KeyUsage	Time Stamping
Certificate Policies	Policy OID: 0.4.0.194112.1.3 Policy OID, 1.3.6.1.4.1.52969.1.2, CP URL: https://docs.trustpro.eu/trustpro-tsa-cpcps-en.pdf
CRL distribution point	http://ca.trustpro.eu/crls/[TSANAME].crl
Authority Information Access	OCSP, http://ca.trustpro.eu/ocsp/
QC Statements	id-etsi-qcs-QcCompliance (OID 0.4.0.1862.1.1); id-etsi-qcs-QcRetentionPeriod (OID 0.4.0.1862.1.3) = 20; id-etsi-qcs-QcPDS (OID 0.4.0.1862.1.5) = https://docs.trustpro.eu/trustpro-tds-en.pdf, "en"

7.2 CRL Profile

7.2.1 Version Number(s)

The *Certification Authority* issues Version 2 certificate revocation lists according to the RFC 5280 [16] specification.

7.2.2 CRL and CRL Entry Extensions

The revocation lists issued by the *Certification Authority* shall include the following fields:

Version	2
Signature Algorithm Identifier	sha256WithRSAEncryption
Signature	Issued by TrustPro QTSP Qualified CA private key
Issuer	the unique identifier of the revocation list issuer certification unit.
This Update	The date of the entry into force of the revocation list. Value according to UTC with encoding according to RFC 5280 [16]. In case of the revocation lists issued by the *Certification Authority* this is the same as the issuance time.
Next Update	The issuance time of the next revocation list (see Section 4.10.). Value according to UTC with encoding according to RFC 5280 [16].
Revoked *Certificates*	The list of the suspended or revoked *Certificates* with the serial number of the *Certificate* and with the suspension or revocation time.
CRL number	not critical, The consecutive serial numbers of the revocation lists are in this field.

7.3 OCSP Profile

The *Provider* operates an online certificate status service according to the RFC 6960 [20]

standard. The OCSP response is signed by TrustPro QTSP CA private key.

7.3.1 Version Number(s)

The *Provider* supports the online certificate status requests and responses conforming to the Version 1according to the standards RFC 6960 [20].

7.3.2 OCSP Extensions

The *Provider* may optionally include the following OCSP extension:

- ArchiveCutoff – not critical

  The *Certification Authority* may indicate with a standard notation according to the RFC 6960 [20] specification that it retains revocation information beyond the *Certificate*'s expiration.

The *Provider* may include the following OCSP registration extension:

- Reason Code – not critical – with the reason of the revocation.

  In case of suspended certificates, it is a mandatory field, its value shall be: "certificateHold (6)".

8 Compliance Audit and Other Assessments

The operation of the *Provider* is supervised by a National Authority in line with European Union regulations. The National Authority can hold site inspections at the *Provider* location. Before the site inspection, the *Provider* has a screening of its operations by an external auditor and sends the detailed report of the screening to the National Authority within 3 days from its receipt. The screening verifies whether the operation of the *Provider* meets the requirements of the eIDAS Regulation [1] and the related national legislation.

8.1 Frequency or Circumstances of Assessment

The *Provider* has the conformance assessment carried out yearly on the IT system performing the provision of the services.

8.1 Identity/Qualifications of Assessor

The *Provider* performs the internal audits with the help of employees and contractor with independent system auditor role.

The eIDAS and ETSI conformity assessment can be performed by an organization with a qualifying mandate issued by the national accreditation organization of an EU Member State.

8.2 Assessor's Relationship to Assessed Entity

External audit is performed by a CAB, which:

- is independent from the owners, management, and operations of the examined *Provider*,
- is independent from the examined organization, namely neither himself or herself nor his or her immediate relatives have any employment or business relationship with the *Provider*,
- remuneration is not dependent on the findings of the activities carried out during the audit.

8.3 Topics Covered by Assessment

The CAB performs the external audit to evaluate the conformity to this document, European standards and to applicable standards.

8.4 Actions Taken as a Result of Deficiency

The *Provider* shall answer the problems stated by the independent auditor in writing, reporting the measures taken to avert them at the occasion of the next authority review.

9 Other Business and Legal Matters

9.1 Fees

The *Provider* publishes fees and prices on its webpage and makes them available for reading at its customer service.

The *Provider* may unilaterally change the price list. The *Provider* publishes any modification to the price list 30 days before it becomes effective. Modifications will not affect the price of services paid in advance.

9.1.1 Certificate Issuance or Renewal Fees

N/A.

9.1.2 Certificate Access Fees

N/A.

9.1.3 Revocation or Status Information Access Fees

The *Provider* provides free of charge on-line access to CRL and OCSP service.

9.1.4 Fees for Other Services and Refund Policy

See section: 9.1.

9.2 Financial Responsibility

The *Provider* has signed an appropriate insurance to cover the risks of the activity and any damage deriving from the certification service.

9.3 Confidentiality of Business Information

The *Provider* manages clients' data according to legal regulations. The *Provider* has a data processing regulation (see section 9.4), which addresses the processing of personal data in particular.

9.3.1 Scope of Confidential Information

The *Provider* treats as confidential:

- all *Client* data, with the exception of those that qualify as information not considered confidential in section 9.3.2;
- besides the *Client* data:
  - transaction related data and log data,
  - non-public regulations,
  - all data whose public disclosure would have an adverse effect on the security of the service.

9.3.2 Information Not Within the Scope of Confidential Information

The *Provider* considers all data public that can be obtained from a public source, or to the disclosure of which the *Subscriber* gave its consent in writing beforehand.

9.3.3 Responsibility to Protect Confidential Information

The *Provider* is responsible for the protection of the confidential data it manages.

The *Provider* shall oblige its employees, subcontractors, affiliated partners to protect all confidential data by signing declaration of confidentiality or by contract.

9.4 Privacy of Personal Information

The *Provider* takes care of the protection of the personal data it manages, the operation and regulations of the *Provider* comply with the requirements of the applicable legislation.

The *Provider* preserves upon expiry of the obligation to retain the registered personal data and information on the Client in accordance with the legal requirements.

9.4.1 Privacy Plan

The *Provider* has a Privacy Policy for data processing that contains detailed requirements for the personal data management. The Privacy Policy for data processing is published on the webpage of the TrustPro QTSP Ltd Certification Authority on the following URL: https://docs.trustpro.eu

9.4.2 Information Treated as Private

The *Provider* protects all personal data related to the data subject or containing conclusions on the data subject that cannot be accessed publicly from the Certificate or other public data source.

9.4.3 Information Not Deemed Private

The *Provider* may disclose the data of the *Subjects* indicated in the *Certificate* based on the written consent of the *Subject*. The *Provider* may indicate the unique provider identifier assigned to the *Subject* in the Certificate.

9.4.4 Responsibility to Protect Private Information

The *Provider* stores securely and protects the personal data related to the *Certificate* issuance and not indicated in the *Certificate*.

9.4.5 Notice and Consent to Use Private Information

The *Provider* only discloses personal data indicated in the *Certificates* with the written consent of the *Client*.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

In cases defined in the Authority the *Provider* may disclose the stored personal data about the *Client* without notifying the *Client*.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

During its business operation, the *Provider* shall not harm any intellectual property rights of a third person.

The present document is the exclusive property of the *Provider*. The *Clients*, *Subjects* and other *Relying Parties* are only entitled to use the document according to the requirements of the present *Certification Practice Statement* and any other use for commercial or other purposes is strictly prohibited.

9.6 Representations and Warranties

Refer to the contractual agreement between CA, RA, Applicants and Subjects for details of the guarantees and responsibilities to each subject.

9.7 Limitations of warranty

Refer to the TSA Disclosure Statement in: https://docs.trustpro.eu/trustpro-tds-en.pdf

9.8 Limitations of Liability

Refer to the TSA Disclosure Statement in: https://docs.trustpro.eu/trustpro-tds-en.pdf

9.9 Indemnities

Refer to the TSA Disclosure Statement in: https://docs.trustpro.eu/trustpro-tds-en.pdf

9.10 Term and Termination

Refer to the TSA Disclosure Statement in: https://docs.trustpro.eu/trustpro-tds-en.pdf

9.11 Individual Notices and Communications with Participants

Refer to the TSA Disclosure Statement in: https://docs.trustpro.eu/trustpro-tds-en.pdf

9.12 Amendments

The *Provider* reserves the right to change this document in a controlled way in case of the change of normative rules, safety requirements, market conditions or other circumstances.

9.13 Dispute Resolution Provisions

Refer to the TSA Disclosure Statement in: https://docs.trustpro.eu/trustpro-tds-en.pdf

9.14 Governing Law

Refer to the TSA Disclosure Statement in: https://docs.trustpro.eu/trustpro-tds-en.pdf

9.15 Compliance with Applicable Law

Refer to the PKI Disclosure Statement in: https://docs.trustpro.eu/trustpro-tds-en.pdf

9.16 Miscellaneous Provisions

9.16.1 Severability

Should some of the provisions of the present document become invalid for any reason, the remaining provisions will remain in effect unchanged.

9.16.2 Enforcement

The *Provider* is entitled to claim payment for damages and attorney fees for reimbursement of the damages, losses, expenses caused by its partners. If in a particular case the *Provider* does not exercise its claim for damages that does not mean that in similar cases in the future or in case of violation of other provisions of the present document, it would waive the enforcement of claims for damages.

9.16.3 Force Majeure

The *Provider* is not responsible for the defective or delayed performance of the requirements set out in this document if the reason for failure or delay was a condition that is outside the control of the *Provider*.

References

Num.	Reference
[1]	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
[2]	ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[3]	ETSI EN 319 411-2 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
[4]	ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[5]	ETSI EN 319 412-2 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[6]	ETSI EN 319 412-3 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
[7]	ETSI EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[8]	ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
[9]	ISO/IEC 19790 Information technology -- Security techniques -- Security requirements for cryptographic modules
[10]	FIPS 140-2 Security requirements for cryptographic modules
[11]	CEN 14167-2 Cryptographic Module for CSP Signing Operations with Backup — Protection Profile
[12]	ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security
[13]	RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[14]	ISO 27001 Information technology -- Security techniques -- Information security management systems -- Requirements
[15]	ITU X.509 V3 Information technology - Open Systems Interconnection - The Directory: Public- key and attribute certificate frameworks
[16]	RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[17]	RFC 6818 Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List

	(CRL) Profile
[18]	RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile
[19]	RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
[20]	RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
[21]	ETSI TS 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
[22]	ETSI TS 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
[23]	RFC 3161 Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)
[24]	RFC 5816 ESSCertIDv2 Update for RFC 3116