



Certificate Policy


Certificate Practice Statement

Date	Rev	Description of changes
1-Mar-2019	01	First release
28-Mar-2019	02	3.5 – rewording and minor changes 5.2.1 – added RAO to trusted roles
17-May-2019	03	Support, documents and certificates sites URL changed
20-May-2020	04	3.2.3 – rewording 3.2.5 - rewording and addition of remote identification using notified eIDAS identification schemes
4-Jun-2021	05	4.9 - added retention period for revoked certificates and OIDs ExpiredCertsOnCRL, ArchiveCutOff
13-Jul-2021	06	4.9 – details about CRL publication in case of termination or key compromise
12-Feb-2022	07	7.1.7 – added certificate policies 0.4.0.194112.1.0 (QCP-n), 0.4.0.194112.1.1, (QCP-l), 0.4.0.194112.1.2 (QCP-n-qscd), 0.4.0.194112.1.3 (QCP-l-qscd)
10-Apr-2024	08	3.2.5 – rewording of the remote identification process to clarify that all identities are verified by an officer


	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public


1	INTRODUCTION	9
1.1	OVERVIEW	9
1.2	DOCUMENT NAME AND IDENTIFICATION	10
1.2.1	EFFECT	10
1.3	PKI PARTICIPANTS	11
1.3.1	TRUSTPRO QTSP CERTIFICATION AUTHORITY	11
1.3.2	REGISTRATION AUTHORITY AND LOCAL REGISTRATION AUTHORITIES	12
1.3.3	SUBSCRIBERS	13
1.3.4	RELYING PARTIES	14
1.3.5	OTHER PARTICIPANTS	14
1.4	CERTIFICATE USAGE	14
1.4.1	APPROPRIATE CERTIFICATE USES	14
1.4.2	PROHIBITED CERTIFICATE USES	15
1.5	POLICY ADMINISTRATION	15
1.5.1	ORGANIZATION ADMINISTERING THE DOCUMENT	15
1.5.2	CONTACT PERSON	15
1.5.3	ENTITY RESPONSIBLE FOR THE SUITABILITY OF THE PRACTICE STATEMENT FOR THE QUALIFIED SIGNATURE CERTIFICATE POLICY	15
1.5.4	CP-CPS APPROVAL PROCEDURES	16
1.6	DEFINITIONS AND ACRONYMS	16
1.6.1	DEFINITIONS	16
1.6.2	ACRONYMS	23
2	PUBLICATION AND REPOSITORY RESPONSIBILITIES	25
2.1	REPOSITORIES	25
2.2	PUBLICATION OF CERTIFICATION INFORMATION	25
2.2.1	SERVICE PROVIDER CERTIFICATES	26
2.2.2	END-USER CERTIFICATES	26
2.3	TIME OR FREQUENCY OF PUBLICATION	26
2.3.1	FREQUENCY OF THE PUBLICATION OF TERMS AND CONDITIONS	26
2.3.2	FREQUENCY OF THE CERTIFICATES DISCLOSURE	26
2.3.3	THE CHANGED REVOCATION STATUS PUBLICATION FREQUENCY	27
2.3.4	ACCESS CONTROLS ON REPOSITORIES	27
3	IDENTIFICATION AND AUTHENTICATION	28
3.1	NAMING	28
3.1.1	NEED FOR NAMES TO BE MEANINGFUL	28
3.1.2	ANONYMITY OR PSEUDONYMITY OF SUBJECTS	29
3.1.3	RULES FOR INTERPRETING VARIOUS NAME FORMS	29
3.1.4	UNIQUENESS OF NAMES	29
3.1.5	PROCEDURES TO RESOLVE DISPUTES RELATING THE NAMES	30
3.1.6	RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS	30
3.2	INITIAL IDENTITY VALIDATION	30

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public


3.2.1	METHOD TO PROVE POSSESSION OF PRIVATE KEY	30
3.2.2	VALIDATION OF AN ORGANIZATION IDENTITY	30
3.2.3	VALIDATION OF AN INDIVIDUAL IDENTITY	31
3.2.4	IN PRESENCE IDENTIFICATION	31
3.2.5	REMOTE IDENTIFICATION	32
3.2.6	ELECTRONIC CERTIFICATE IDENTIFICATION	32
3.2.7	NON-VERIFIED INFORMATION	33
3.2.8	VALIDATION OF AUTHORITY	33
3.3	IDENTIFICATION VALIDATION IN CASE OF CERTIFICATE RENEWAL REQUESTS	34
3.3.1	IDENTIFICATION WITH A VALID CERTIFICATE	34
3.4	IDENTIFICATION VALIDATION FOR CERTIFICATE MODIFICATION REQUESTS	34
3.5	IDENTIFICATION AND AUTHENTICATION FOR REVOCATION AND SUSPENSION REQUEST	34
4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	36
4.1	APPLICATION FOR A CERTIFICATE	36
4.1.1	WHO MAY SUBMIT A CERTIFICATE APPLICATION	38
4.1.2	ENROLMENT PROCESS AND RESPONSIBILITIES	38
4.2	CERTIFICATE APPLICATION PROCESSING	40
4.2.1	PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS	40
4.2.2	IDENTITY AUTHENTICATION WITH TWO AUTHENTICATION FACTORS	40
4.2.3	APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS	40
4.2.4	TIME TO PROCESS CERTIFICATE APPLICATIONS	41
4.3	CERTIFICATE ISSUANCE	41
4.3.1	CA ACTIONS DURING CERTIFICATE ISSUANCE	42
4.3.2	NOTIFICATION OF THE SUBSCRIBER ABOUT THE ISSUANCE OF THE CERTIFICATE	42
4.4	CERTIFICATE ACCEPTANCE	42
4.4.1	CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE	42
4.4.2	PUBLICATION OF THE CERTIFICATE BY THE CA	42
4.4.3	NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES	43
4.5	KEY PAIR AND CERTIFICATE USAGE	43
4.5.1	SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE	43
4.5.2	RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE	43
4.6	CERTIFICATE RENEWAL	44
4.6.1	CIRCUMSTANCES FOR CERTIFICATE RENEWAL	44
4.6.2	WHO MAY REQUEST RENEWAL	45
4.6.3	PROCESSING CERTIFICATE RENEWAL REQUESTS	45
4.6.4	NOTIFICATION ABOUT THE NEW CERTIFICATE ISSUANCE	46
4.6.5	CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWED CERTIFICATE	46
4.6.6	PUBLICATION OF THE RENEWED CERTIFICATE BY THE CA	46
4.6.7	NOTIFICATION OF OTHER ENTITIES ABOUT THE CERTIFICATE ISSUANCE	46
4.7	CERTIFICATE MODIFICATION	46
4.8	CERTIFICATE REVOCATION OR SUSPENSION	47
4.8.1	CIRCUMSTANCES FOR REVOCATION	47
4.8.2	WHO CAN REQUEST REVOCATION	49
4.8.3	PROCEDURE FOR REVOCATION AND SUSPENSION REQUEST	49
4.8.4	REVOCATION REQUEST GRACE PERIOD	49
4.8.5	TIME WITHIN WHICH CA WILL PROCESS THE REVOCATION REQUEST	49

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public


4.8.6	REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES	50
4.8.7	CIRCUMSTANCES FOR SUSPENSION	50
4.8.8	WHO CAN REQUEST SUSPENSION	50
4.8.9	PROCEDURE FOR SUSPENSION AND REINSTATEMENT REQUEST	50
4.8.10	CRL ISSUANCE FREQUENCY	51
4.8.11	MAXIMUM LATENCY FOR CRLs	51
4.8.12	ONLINE REVOCATION/STATUS CHECKING AVAILABILITY	51
4.8.13	SPECIAL REQUIREMENTS FOR KEY COMPROMISE	51
4.8.14	MAXIMUM DELAY FOR REVOCATION STATUS AVAILABILITY	51
4.9	CERTIFICATE STATUS SERVICES	51
4.9.1	OPERATIONAL CHARACTERISTICS	52
4.9.2	SERVICE AVAILABILITY	53
4.9.3	END OF SUBSCRIPTION	53
4.9.4	KEY ESCROW AND RECOVERY	53
5	FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS	54
5.1	PHYSICAL CONTROLS	54
5.1.1	SITE LOCATION AND CONSTRUCTION	55
5.1.2	PHYSICAL ACCESS	55
5.1.3	POWER AND AIR CONDITIONING	56
5.1.4	WATER EXPOSURES	56
5.1.5	FIRE PREVENTION AND PROTECTION	57
5.1.6	MEDIA STORAGE	57
5.1.7	WASTE DISPOSAL	57
5.1.8	BACKUP	57
5.2	PROCEDURAL CONTROLS	58
5.2.1	TRUSTED ROLES	58
5.2.2	ROLES REQUIRING SEPARATION OF DUTIES	59
5.3	STAFF CONTROLS	60
5.3.1	QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS	60
5.3.2	BACKGROUND CHECK PROCEDURES	60
5.3.3	TRAINING REQUIREMENTS	61
5.3.4	RETRAINING FREQUENCY AND REQUIREMENTS	61
5.3.5	JOB ROTATION FREQUENCY AND SEQUENCE	62
5.3.6	SANCTIONS FOR UNAUTHORIZED ACTIONS	62
5.3.7	INDEPENDENT CONTRACTOR REQUIREMENTS	62
5.3.8	DOCUMENTATION SUPPLIED TO STAFF	62
5.4	AUDIT LOGGING PROCEDURES	63
5.4.1	TYPES OF EVENTS RECORDED	63
5.4.2	FREQUENCY OF AUDIT LOG PROCESSING	63
5.4.3	RETENTION PERIOD FOR AUDIT LOG	64
5.4.4	PROTECTION OF AUDIT LOG	64
5.4.5	AUDIT LOG BACKUP PROCEDURES	64
5.4.6	AUDIT COLLECTION SYSTEM	65
5.4.7	NOTIFICATION TO EVENT-CAUSING SUBJECT	65
5.4.8	VULNERABILITY ASSESSMENTS	65
5.5	RECORDS ARCHIVAL	65

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

5.5.1	TYPES OF RECORDS ARCHIVED	65
5.5.2	RETENTION PERIOD FOR ARCHIVE	66
5.5.3	PROTECTION OF ARCHIVE	66
5.5.4	ARCHIVE BACKUP PROCEDURES	66
5.5.5	ARCHIVE COLLECTION SYSTEM	66
5.5.6	PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION	66
5.6	CA KEY CHANGEOVER	67
5.7	COMPROMISE AND DISASTER RECOVERY	67
5.7.1	CORRUPTION OF RESOURCES, SOFTWARE, AND DATA	67
5.7.1	ENTITY PRIVATE KEY COMPROMISE PROCEDURES	68
5.7.2	BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER	68
5.8	TERMINATION OF QUALIFIED TRUST SERVICES	68
6	TECHNICAL SECURITY CONTROLS	70
6.1	KEY PAIR GENERATION AND INSTALLATION	70
6.2	KEY PAIR GENERATION	70
6.2.1	PRIVATE KEY DELIVERY TO SUBSCRIBER	71
6.2.2	CA PUBLIC KEY DELIVERY TO RELYING PARTIES	71
6.2.3	KEY SIZES	72
6.2.4	KEY USAGE PURPOSES	72
6.2.5	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	72
6.2.6	CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS	72
6.2.7	PRIVATE KEY MULTI-PERSON CONTROL	73
6.2.8	PRIVATE KEY ESCROW	73
6.2.9	PRIVATE KEY BACKUP	73
6.2.10	PRIVATE KEY ARCHIVAL	73
6.2.11	PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE	73
6.2.12	PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE	73
6.2.13	METHOD OF ACTIVATING PRIVATE KEY	74
6.2.14	METHOD OF DEACTIVATING PRIVATE KEY	74
6.2.15	METHOD OF DESTROYING PRIVATE KEY	74
6.2.16	CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS	74
6.3	ACTIVATION DATA	75
6.4	COMPUTER SECURITY CONTROLS	75
6.4.1	SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS	75
6.5	LIFE CYCLE TECHNICAL CONTROLS	75
6.6	TIME ACCURACY	76
7	CERTIFICATE, CRL AND OCSP PROFILES	77
7.1	CERTIFICATE PROFILES	77
7.1.1	VERSION NUMBER	78
7.1.2	CERTIFICATE EXTENSIONS	78
7.1.3	ALGORITHM OBJECT IDENTIFIERS	78
7.1.4	NAME FORMS	78
7.1.5	NAME CONSTRAINTS	78
7.1.6	CERTIFICATE POLICY OBJECT IDENTIFIERS	78
7.1.7	END USER CERTIFICATE PROFILE DETAILS	79

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

7.2 CRLPROFILE	81
7.2.1 VERSION NUMBER(S)	81
7.2.2 CRLANDCRLENTRYEXTENSIONS	81
7.3 OCSP PROFILE	81
7.3.1 VERSION NUMBER(S)	82
7.3.2 OCSP EXTENSIONS	82
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS	83
8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT	83
8.1 IDENTITY/QUALIFICATIONS OF ASSESSOR	83
8.2 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY	83
8.3 TOPICS COVERED BY ASSESSMENT	84
8.4 ACTIONS TAKEN AS A RESULT OF DEFICIENCY	84
9 OTHER BUSINESS AND LEGAL MATTERS	85
9.1 FEES	85
9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES	85
9.1.2 CERTIFICATE ACCESS FEES	85
9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES	85
9.1.4 FEES FOR OTHER SERVICES AND REFUND POLICY	85
9.2 FINANCIAL RESPONSIBILITY	85
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION	85
9.3.1 SCOPE OF CONFIDENTIAL INFORMATION	86
9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION	86
9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION	86
9.4 PRIVACY OF PERSONAL INFORMATION	86
9.4.1 PRIVACY PLAN	86
9.4.2 INFORMATION TREATED AS PRIVATE	87
9.4.3 INFORMATION NOT DEEMED PRIVATE	87
9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION	87
9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION	87
9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS	87
9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES	87
9.5 INTELLECTUAL PROPERTY RIGHTS	87
9.6 REPRESENTATIONS AND WARRANTIES	88
9.7 LIMITATIONS OF WARRANTY	88
9.8 LIMITATIONS OF LIABILITY	88
9.9 INDEMNITIES	88
9.10 TERM AND TERMINATION	88
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS	88
9.12 AMENDMENTS	88
9.13 DISPUTE RESOLUTION PROVISIONS	88
9.14 GOVERNING LAW	88
9.15 COMPLIANCE WITH APPLICABLE LAW	89
9.16 MISCELLANEOUS PROVISIONS	89
9.16.1 SEVERABILITY	89
9.16.2 ENFORCEMENT	89

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public


9.16.3

FORCE MAJEURE

89

REFERENCES

90

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

1 Introduction

This document contains the integrated *Qualified Certificate Policy* and *Certification Practice Statement* concerning the qualified certification service of TrustPro QTSP Ltd Certification 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 electronic signatures and Certificates 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

This document summarizes all the information the *Clients* 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.

Furthermore it contains set of rules that specify a *Certificate's* usability for a community and/or a class of applications with common safety requirements and information to help the users and acceptors of *Certificates*, *Certificate* revocation lists and online *Certificate* status responses issued by the *Provider* in the clear identification of the ways they are managed, the level of security guaranteed as well as the relevant and related technical, commercial, financial guarantees and legal responsibility. The content and format of the present document complies with the requirements of the RFC 3647 [13] framework.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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

<i>Issuer</i>	TrustPro QTSP Ltd Certification Authority
<i>Document name</i>	Qualified Certificate Certification Practice Statement – Certificate Policy
<i>Code</i>	QTSP-CP/CPS
<i>Document version</i>	1.0
<i>Date of effect</i>	01-03-2019
<i>OID (Iana PEN)</i>	1.3.6.1.4.1.52969

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.

<i>Subject Scope</i>	This document is related to the provision and usage of the services concerning the issuance of certificates for digital signature.
<i>Temporal Scope</i>	The present version of this document is effective from the date of effect, until withdrawal. The effect automatically terminates at the cessation of services.
<i>Personal Scope</i>	The effect of this document extends each of the participants mentioned in section 1.3.
<i>Geographical Scope</i>	The present <i>Certification Practice Statement</i> includes specific requirements for services primarily provided for <i>European Clients</i> , operating by the European law. The <i>Provider</i> can extend the geographical scope of the service, in this case, it shall use not less stringent requirements than those applicable to European conditions.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

1.3 PKI Participants

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

- TrustPro QTSP Ltd Certification Authority and Registration Authority,
- The Local Registration Authorities in a contractual relationship with TrustPro QTSP Ltd Certification Authority,
- the Clients of TrustPro QTSP Ltd Certification Authority (Subscribers and Subjects),
- relying parties,
- other participants.


1.3.1 TrustPro QTSP Certification Authority

TrustPro QTSP Certification Authority (CA) is the entity that issues Certificates within the framework of TrustPro QTSP Trust Service Provider and performs the related tasks. TrustPro QTSP CA identifies the applicant person, manages records, accepts the changes related to the Certificates, and publishes the policies related to the Certificate, public keys and information on the current state of the Certificate (in particular about its possible revocation or suspension).

Provider data

<i>Name</i>	TrustPro QTSP Certification Authority
<i>Company</i>	TrustPro QTSP Ltd
<i>Head office</i>	Guinness Enterprise Centre Taylor's Lane, Dublin 8 Ireland, D08 N9EX
<i>Telephone number</i>	+353 14861130
<i>Internet address</i>	https://www.trustpro.eu
<i>Online H24 7x7 customer support</i>	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 Certification Authority has its own

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

Registration Authority and can operate also with a network of *Local Registration Authorities*.

TrustPro QTSP highlights the importance of *Client* experience and security. In order 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.

Subscribers certification services interface are Accessible to person with disabilities according to W3C standards.

The *Provider* provides the following trust services defined by the eIDAS regulation within the framework of the present *Certification Practice Statement*:

- Qualified certificates for Electronic Signatures (art. 28 eIDAS regulation) and related services. Supported policies: QCP-n and QCP-n-qscd
- Qualified certificates for Electronic Seals (art. 38 eIDAS regulation) and related services. Supported policies: QCP-l and QCP-l-qscd

1.3.2 Registration Authority and Local Registration Authorities


The *Registration Authority* operates as a part of the *Trust Service Provider*. The *Registration Authority* operates directly or through formally delegated Local registration Authorities. The *Trust Service Provider* is in all cases responsible for the proper operation of the *Registration Authority*.

The *Trust Service Provider* shall contractually oblige the *Local Registration Authority* to comply with the relevant requirements. The list of active Local Registration Authorities is available on TrustPro QTSP website.

Local Registration Authority will be formally trained by the *Trust Service Provider* and are subject to audit from the *Trust Service Provider*.

Tasks of the office:

- identification and registration of the *Subject* indicated on end user *Certificates*,
- administration and registration activity related to the issuing of *Certificates* and *Electronic Signature Creation Devices*

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

- maintaining contact with *Clients* (reception of questions, announcements, requests and complaints, and the initiation of their processing),
- performance of certificate actions (revocation, suspension, reinstallation, certificate renewal, certificate modification and re-key).

The *Provider* maintains a continuously available standby service for the initiation of revocation or suspension – 24 hours a day, every day of the week.

The *Registration Authority* and *Local Registration Authorities* may perform registration activities wherever is needed, including client premises

Any communication between Local Registration Authority, Registration Authority and Certification Authority is authenticated by a client certificate authentication issued by the Certification Authority.


1.3.3 Subscribers

Subscribers define the scope of *Subjects* using the service, and *Subscribers* also cover the service fees related to the usage of these services. The *Subject* is that natural person, whose data is indicated on the *Certificate*. Subject and Subscriber can be the same person.

In case of a *Certificate* for electronic signature purposes, the *Subject* is also the *Signatory*.

The *Clients* of the services provided by the *Provider*:

- Subscriber:
 - concludes a service agreement with the Provider,
 - defines the scope of the Subjects ,
 - responsible for the payment of the fees arising from the usage of the service.
- Subject: the Provider issues the Certificate for the Subject.
- Signatory: the electronic signature certification service user party, who can create electronic signature with the help of the issued Certificate.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

1.3.4 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.

1.3.5 Other Participants

The *Represented Organization*, whose name is indicated in a Certificate issued for a natural person.

The Trust Service Provider does not necessarily have a contractual relationship with the Represented Organization, but the Trust Service Provider shall not issue an Organizational Certificate without the approval of that Organization. The Trust Service Provider can revoke the Certificate at the request of the Represented Organization.

If a Certificate has been issued to the Subject in order to be used representing an Organization (Organizational Certificate issued to natural person) for signing or for its activity, the Represented Organization is the actual Organization also indicated within the Certificate.


The Provider defines reciprocal obligations in contractual relationship with companies providing services related to the CA activities.

1.4 Certificate Usage

The *Certificate* usability area is essentially determined by the *Certificate* attribute values set by the *Trust Service Provider*. The *Certificate Policy* and the *Certification PracticeStatement* may also contain additional restrictions.

1.4.1 Appropriate Certificate Uses

The private keys belonging to the end-user, bound to the *Certificates* issued by the *Provider* based on the present *Certification Practice Statement* can be only used for electronic signature creation or electronic seal creation according to the Certificate Policy of the Certificate. The certificate allows the verification that the document has been signed or sealed by the person described in the Certificate.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

In case of *Certificate Policies* requiring *Qualified Electronic Signature Creation Device* usage the private key belonging to the qualified *Certificate* is protected by a *Qualified Electronic Signature Creation Device*. *Certificates* issued according to these policies are suitable for *Qualified Electronic Signature* generation.

In case of *Certificate Policies* requiring *Qualified Electronic Seal Creation Device* usage the private key belonging to the qualified *Certificate* is protected by a *Qualified Electronic Seal Creation Device*. *Certificates* issued according to these policies are suitable for *Qualified Electronic Seal* generation.

1.4.2 Prohibited Certificate Uses

Provider Certificate

The provider root *Certificate*, and the associated private keys shall not be used for *Certificate* issuance prior to the disclosure of the provider *Certificate*.

End User Certificates

Certificates issued in accordance with the present *Certificate Policies*, and the private keys belonging to them use for other purposes than the generation and verification of electronic signature and electronic seal is prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The organization administering the present *Certification Practice Statement* is TrustPro QTSP Certification 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

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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


Certification Unit	A unit of the Trust Service Provider 's system that signs the Certificates. Always just one Certificate-Creation Data (signing key, signature-creation data) belongs to a Certification Unit. It is possible that a Certification Authority simultaneously operate several Certification Units
Advanced Electronic Signature	Means an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable
Applicant	The natural person who acts during the application for the given Certificate
Certificate	The electronic signature certificate, the electronic seal certificate and the Website Authentication Certificate, and all those electronic verifications 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

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public


	the issuance and during its validity period
Certificate Application	The data and statements given by the Applicant to the Trust Service Provider for Certificate issuance, in which the Applicant reaffirms the authenticity of data to be indicated on the Certificate
Certificate for Automatism	A <i>Certificate</i> in which the name of the IT device (application, system) that is applied by the <i>Subject</i> to use the <i>Certificate</i> is to be recorded among the <i>Subject's</i> data
Certificate for Electronic Signature	Means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person. In case of Certificates issued by the Trust Service Provider, it can be clearly concluded from the Certificate Policy related to the Certificates, whether the given Certificate is pseudonymous or not. The reference of the Certificate Policy is in the Certificate.
Certificate Policy	A Trust Service Policy which concerns the Certificate issued within the framework of the Trust Service
Certificate Repository	Data repository containing various Certificates. A Certification Authority has a Certificate Repository in which the issued certificates are disclosed, but the system containing Certificates available to the application (certificate manager system) on the computer of the Subject and the Relying Party is also called Certificate Repository
Certification Authority	A Trust Service Provider, who/which identifies the requester within the confines of the certification service, issues Certificates, keeps a record, receives the Certificate related data changes, and publishes the regulations belonging to the Certificate, the Certificate-Verifier Data and the information on the current state (especially on possible revocation or suspension) of the Certificate

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public


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 Centre	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 Document	Means any content stored in electronic form, in particular text or sound, visual or audio-visual recording
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 Signature Creation Data	Means unique data which is used by the signatory to create an electronic signature Typically, cryptographic private key, formerly known as the signature creation data
Electronic Signature Creation Device	Means configured software or hardware used to create an electronic signature. Formerly known as signature-creation device.
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 in the course of 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

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public


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
Local Registration Authority	Local organization formally delegated by the Registration Authority for Subject Subscriber identification and checks of the submitted data authenticity
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
Organizational Certificate	A Certificate, the Subject of which is the Organization, or which presents that the natural person Subject belongs to an Organization. In this case the name of the Organization is indicated in the "O" field of the Certificate
Private Key	In the public key infrastructure, the

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public


	<p>element of an asymmetric cryptographic key pair for an actor that the Subject shall keep strictly secret.</p> <p>In case of electronic signatures, the Signatory generates the signature with the help of the private key.</p> <p>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</p>
Public Key	<p>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.</p> <p>The authenticity of the Certificates can be verified with the public key of the Certification Unit</p>
Public Key Infrastructure, PKI	An infrastructure based on asymmetric cryptography, including the cryptographic algorithms, keys, certificates, the related standards and legislation, the underlying institutional system, a variety of providers and devices
Qualified Certificate for Electronic Signature	A Certificate for electronic signatures issued by a Qualified Trust Service Provider and meets the requirements laid down in Annex I of eIDAS [1].
Qualified Electronic Signature	An advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures
Qualified Electronic Signature Creation Device	Means an electronic signature creation device that meets the requirements laid down in Annex II of eIDAS [1]
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

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

	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
Registration Authority	Organization that checks the authenticity of the Certificate holder's data and verifies that the Certificate Application is authentic, and it has been submitted by an authorized person
Registration Claim	The data and statement given beforehand for the preparation of the Certificate Application and the provider contract to the Trust Service Provider by the Client in which the Client authorizes the Trust Service Provider for data management
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.
Revocation Status Records	The records of the revoked Certificates which includes the fact of the suspension or revocation and the time of the suspension or revocation maintained by the Certification Authority
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

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public


Server-Based Signature Service	A service in which the Signatory's private key can be found on a properly protected server in a secure cryptographic module that can be used by the Signatory after a properly secured authentication step
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
Signatory	A natural person who creates an electronic signature. A person with an identity or attribute verified by the Trust Service Provider with the certificate of the electronic signature
Subject	A person with an identity or attribute verified by the <i>Trust Service Provider</i> with the <i>Certificate</i> , so the signatory especially in case of an electronic signature certificate
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 <i>Trust Service Provider</i> , relying party or other person requires conditions for the usage of the <i>Trust Service</i> 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 particular

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public


	Trust Services
Trust Service Provider	A natural or a legal person who provides one or more <i>Trust Services</i> either as a qualified or as a non-qualified <i>Trust Service</i>
Trust Service Supervisory Body	The National Authority, the supervising authority monitoring the <i>Trust Services</i>
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

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

QCP	Qualified Certificate Policy
RA	Registration Authority
SCD	Secure Creation Device
TSP	Trust Service Provider

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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 Qualified 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 Publication of Certification Information

The *Provider* discloses on its webpage its CA *Certificates*. Subject certificates are not published.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

2.2.1 Service Provider Certificates

The *Certification Authority* discloses the root *Certificate* and the online certificate status service units it operates in the *Certification Practice Statement*. The information related to their change of status are available at the website of the *Certification Authority*.

2.2.2 End-User Certificates

The *Certification Authority* discloses status information related to the issued end-user *Certificates*:

- on revocation lists,
- within the confines of the online certification status response service.

The end-user *Certificate* revocation or suspension is disclosed by the *Provider*, and the *Subject's* consent is not required for it.

The *Certification Authority* discloses, in case of the *Subject's* consent the end-user *Certificates* in its *Certificate Repository* after issuance without delay.

2.3 Time or Frequency of Publication

2.3.1 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.

2.3.2 Frequency of the Certificates Disclosure

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

- the *Certificates* of the root certification units operated by it are disclosed

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

before commencing the service;


2.3.3 The Changed Revocation Status Publication Frequency

The status information related to the end-user *Certificates* issued by the *Provider* and the provider *Certificates* are available immediately within the confines of the online certificate status service.

The information related to the status of the *Certificates* are disclosed in the Certificate Repository on the certificate revocation lists. The practices related to the issuance of the certificate revocation lists are described in Section 4.10.

2.3.4 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.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

3 Identification and Authentication

This section describes subject and subscriber's identification and authentication practices used by the *Provider*.

Identification activities are performed in strict compliance with procedures hereby defined - by the Registration Authority of the *Provider* or by Local Registration Authorities in contractual relationship with the *Provider*.

3.1 Naming


The subject is identified in the certificate by the Distinguished Name (DN), in the field Subject, compliant with X.500 (ISO/IEC 9594) standard.

DN attributes comply with below ETSI EN standards and RFC 5280.

- ETSI EN 319 411-1 [2]: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements. ^[L]_[SEP]
- ETSI EN 319 411-2 [3]: 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. ^[L]_[SEP]
- ETSI EN 319 412-1 [4]: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures. ^[L]_[SEP]
- ETSI EN 319 412-2 [5]: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons. ^[L]_[SEP]
- ETSI EN 319 412-3 [6]: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons. ^[L]_[SEP]
- ETSI EN 319 412-5 [7]: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements. ^[L]_[SEP]

3.1.1 Need for Names to be Meaningful

The attributes of the Distinguished Name (DN) certificate uniquely identifies the subject to which it is issued the certificate.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

If the certificate subject is a Natural Person, the field *Subject* contains at least:

- countryName (OID: 2.5.4.6) ^[L]_[SEP]
- givenName (OID: 2.5.4.42) ^[L]_[SEP]
- surname (OID: 2.5.4.4) ^[L]_[SEP]
- commonName (OID: 2.5.4.3) ^[L]_[SEP]
- serialNumber (OID: 2.5.4.5) ^[L]_[SEP]
- dnQualifier (OID 2.5.4.46) ^[L]_[SEP]

If the certificate subject is a Legal Person, the field *Subject* contains at least:

- countryName (OID: 2.5.4.6) ^[L]_[SEP]
- organizationName (OID: 2.5.4.10) ^[L]_[SEP]
- organizationIdentifier (OID: 2.5.4.97) ^[L]_[SEP]
- commonName (OID: 2.5.4) ^[L]_[SEP]
- dnQualifier (OID 2.5.4.46)

The value of the field dnQualifier is a unique identification code generated by TrustPro QTSP CA and stored in CA database.

3.1.2 Anonymity or Pseudonymity of Subjects


The *Provider* will evaluate case by case the request for the use of a Pseudonym instead subject real data. If the request is accepted the field *Pseudonym* (OID 2.5.4.65) will be used while *givenName*, *surname* and *serialNumber* will be omitted.

3.1.3 Rules for Interpreting Various Name Forms

The *Provider* complies with the X500 standard.

3.1.4 Uniqueness of Names

The *Subject* has a unique name in the *Certificate Repository* of the *Provider*. In order to ensure the uniqueness a combination of subject country code, identity document type and identity document number is used.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

This combination is compliant with the Natural Person and Legal person semantic identifier as described ETSI EN 319 412-1 [4] standard.

3.1.5 Procedures to Resolve Disputes Relating the Names

The *Provider* makes sure of the *Client's* right to use the indicated names. The *Provider* is entitled to revoke the *Certificate* in question for the illegal use of the name or data.

3.1.6 Recognition, Authentication, and Role of Trademarks

In the fields of the end-user *Certificate* required by the *Subscriber* trademarks may occur. The *Provider* makes sure of their legitimate use, and in case of a complaint it is entitled to revoke the *Certificate*.

If the *Client* requests a *Certificate*, and asks for brand name or trademark indication, then the *Client* shall provide evidence of the legitimacy of its use, which the *Provider* verifies before *Certificate* issuance.

The *Provider* uses the TrustPro QTSP Ltd trademark during its service provision. The trademark is the property of TrustPro QTSP Ltd LP., for the usage of the trademark, the consent is given by the holder.

3.2 Initial Identity Validation

The Registration Authority can use any communication channel within the limits provided by law, for the verification of the identity of the Subject requesting the *Certificate*, and for checking the authenticity of the data provided.


The Registration Authority or the *Provider* may refuse the issuance of the required *Certificate* at its sole discretion, without any justification.

3.2.1 Method to Prove Possession of Private Key

The *Provider* establishes that the applicant has or controls the private key corresponding to the public key to be certified verifying that the certificate application contains a signed request signed with the private key corresponding to the public key to be certified. The signed request will be in PKCS#10 format (RFC 2314).

3.2.2 Validation of an Organization Identity

Legal Person identity is validated using country specific organization registries and document issued by these organizations.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

3.2.3 Validation of an Individual Identity

The natural person's identity shall be verified:

- if the *Subject* of the *Certificate* to be issued is a natural person;
- if a natural person is acting on behalf of an *Organization*

When issuing a qualified Certificate, the identity of the natural person shall be verified according to paragraph 1 of Article 24 of the eIDAS regulation by the physical presence or by a method providing equivalent security. Namely:

1. In presence identification: the natural person shall appear in person to the Registration Authority representative or Local Registration Authority delegate;
2. Remote identification using a system with equivalent assurance to physical presence;
3. Qualified Electronic certificate identification: the identity of the natural person is backed by a qualified electronic signature with a qualified certificate belonging to the natural person;


Each method is performed by a Registration Authority and is detailed in following paragraphs.

The Registration Authority can formally delegate the identification to a Local Registration Authority. In this case, a reference to the identity of the Local Registration Authority officer must be present in the *Certificate Application*.

3.2.4 In presence identification

The natural person identity is validated in presence.

- the natural person shall appear in person to the *Registration Authority* representative, delegate or Subscriber to perform the personal identification;
- the identity of the natural person is verified during personal identification based on a suitable official proof of identity card;
- accepted identity cards are defined in each country by local rules;
- the natural person shall verify the accuracy of the data for the registration and identity verification;
- the Registration Authority representative or delegate verifies whether any

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

alteration or counterfeiting happened to the presented identity documents.

The Registration Authority verifies the identity of foreign citizens with the help of their passport or other personal identification documents, in this case it can perform data reconciliation with the proper records of the country, if such records are available.

The *Provider* can also accept other documents and evidences, if it makes sure that the level of security is the same as of the above. Obtaining such evidence and submitting it to the *Provider* is the *Client's* responsibility.

The *Provider* only accepts valid documents and evidences not older than 3 months.

The *Provider* does not issue the *Certificate* if it considers that - based on its internal rules - it can't verify with corresponding confidence the certificate, document or the data of the foreign organization.

3.2.5 Remote identification

Registration Authority is authorized to use the remote identification system provided by the *Provider* and confirmed by a Conformity Assessment body.


Remote identification can be performed with one of following methods:

- a) A remote video identification system as per art. 24.1.d eIDAS [1]. TrustPro remote video identification is an application (<https://remoteid.trustpro.eu>) that collects a number of subject identity evidences - included a video record -, validates these evidences and submits to the Registration Authority or Local Registration Authority officer only successfully validated identities. All identities are verified by the Registration Authority or Local Registration Authority officer. If the identity is not properly verified by the officer, the certificate is revoked.
- b) A notified electronic identification scheme according to art. 8 eIDAS [1] using substantial and/or high assurance level for identification means.

3.2.6 Electronic certificate identification

The identity of the natural person is backed by a qualified electronic signature with a qualified certificate belonging to the natural person.

- The Subject submits the Certificate Application in electronic format with a qualified electronic signature based on a non-pseudonymous qualified certificate

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

- The electronically signed *Certificate Application* shall contain the data needed for the identification of the natural person.
- The authenticity and confidentiality of the *Certificate Application* shall be verified on the whole certification chain.
- The *Provider* may accept only those electronic signatures, which are based on a qualified certificate issued by a Trust Service Provider which is listed on the Trusted List of one of the EU member states and was valid at the time of the signature creation.

The *Provider* can use the data reconciled during a previous identification procedure, if the *Subject* requests new *Certificate* instead of an expired or a revoked one, or if he requests a new *Certificate* besides the existing one during the validity period of the service agreement. The authenticity of the *Certificate* application, the accuracy of the data to be in the *Certificate* and the identity of the person submitting the application shall also be checked.

3.2.7 Non-Verified Information

Some *Subject* or *Subscriber* informations, such as address, or telephone number may not be verified by the *Provider*. The *Provider* is not responsible for the accuracy of these informations.


3.2.8 Validation of Authority

The identity of the natural person representing the legal person is verified according to the requirements of Section 3.2.3 before issuing a *Certificate* for the legal person.

The right of representation of the natural person shall be verified. Persons entitled to act on behalf of an *Organization*:

- a person authorized to represent the given *Organization*,
- a person who is mandated for that purpose by an authorized person to represent the *Organization*,
- an *Organization* administrator appointed by an authorized person to represent the *Organization*.

The organization administrator can be appointed during *Certificate* application, or anytime later with the help of the corresponding form. The identifier information of the designated person(s) shall be given on the form, by which he/she can be identified in

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

later litigation. The form shall be electronically signed by the representative of the *Organization*, which is verified by the registration associate of the *Provider* when received. Appointing an organization administrator is not mandatory, and multiple organization administrators can be appointed too. If there is no appointed organization administrator, then the person entitled to represent the *Organization* can perform this task.

3.3 Identification validation in Case of Certificate Renewal Requests

Certificate renewal is the process when the *Provider* issues a certificate with unchanged *Subject* identification information but for new validity period to a *Subject*. *Certificate* renewal can only be requested during the validity period of the service agreement.

3.3.1 Identification with a valid Certificate

For *Certificate* renewal based on a valid certificate the following options are enabled by the *Provider*:

- electronically submitted request with an electronic signature based on the Certificate to be renewed;
- electronic form with an electronic signature of the Subject based on the non-pseudonymous Certificate with a security classification not lower than the Certificate to be renewed (see section 1.2.3.);

There is no need for further verification of the applicant's identity, or the authenticity of the application.


The certificate must be valid. Invalid certificate shall not be renewed.

3.4 Identification validation for Certificate Modification requests

Not applicable, because certificate modification is not permitted.

3.5 Identification and Authentication for Revocation and Suspension Request


The *Provider* receives and processes the requests related to the revocation or suspension of the Certificates, and the announcements (for example related to the private key compromise or to the improper use of the Certificate) concerning the

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

revocation of the Certificates.

The *Provider* accepts requests only from authorized parties before processing of the revocation or suspension requests.

The identity of the submitter persons and the authenticity of the applications are verified. The identification and authentication aspects of such requests are described in section 4.8.3.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

4 Certificate Life-Cycle Operational Requirements

All life-cycle certificate operations are managed through a trusted Registration Authority and are bound to a valid *Service Agreement* with the Subscriber.

Service agreement is in electronic form and can be part of - or is referenced by - the Certificate Application and Acceptance. Certificate Application is signed by Subscriber with advanced electronic signature.

Certificate Application is delivered to the Subscriber together with the Certificate in the enrolment process.

Service agreement shall contain the types of *Certificate* available for specific *Subjects* within the confines of the Agreement.

Certificate life-cycle operations managed by the Provider are:

- New certificate
- Certificate renewal
- Certificate revocation

The state of a *Certificate* can be valid or revoked.

The Provider provides *Certificate* maintenance only during the force of the related service agreement.


4.1 Application for a Certificate

For each new *Certificate*, *Certificate Application* submission is required. The *Subject* shall specify the data to be indicated in the *Certificate* and shall specify what kind of *Certificate* is requested, and he/she shall authorize the *Provider* for the management of their personal data.

The *Provider* informs the *Subscriber* about the *Certificate* usage terms and conditions prior to the conclusion of the contract.

If the *Subject* is not the same as the *Subscriber*, then the aforementioned information is also given to the *Subject* by email.

The *Provider* publishes the documents containing this information in a comprehensible

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

manner, made available in an electronically downloadable format.


In the *Certificate Application*, the *Subject* shall at least include below data:

- Subject data to be indicated in the *Certificate* (see section 3.1 for details);
- personal identification information of the *Subject* – in case of an *Organization* the *Organization* representative (at least birth date and place for natural person, full name for legal person)
- the contact of the *Subject* – in case of an *Organization* the *Organization* representative - (address, telephone number, e-mail address);
- in case of *Organization* Certificate application, the official data of the *Organization*
- *Subscriber's* data if *Subject* and *Subscriber* are not the same person;

In conjunction with the *Certificate Application* the Registration Authority representative or delegate asks for and checks at least the following documents, certifications, attorneys and declarations:

- documents necessary to identify the *Subject* – in case of an *Organization*, the *Organization* representative, according to Section 3.2.3;
- in case of *Organizational Certificate* application, the documents for the identification of the *Organization*, according to Section 3.2.2;
- if the *Subject* represents an *Organization*, then the certification or procuration delivered by the *Organization*, that the *Subject* is entitled to represent the *Organization*, according to section 3.2.5;
- if the *Subject* is a natural person requesting the indication of belonging to an *Organization*, the evidence of the consent of the *Organization*, identified according to section 3.2.2.;
- if the *Certificate* requested contains a trademark or a brand name, then a certification about the usage rights of the *Subject*, according to section 3.1.6.

The *Certificate Application* and the *Service Agreement* (or a reference to a standard *Service Agreement*) are electronic documents signed by *Subject* and the *Subscriber* (if the subscriber and the subject are different persons). The signature is:

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

- an advanced electronic signature authenticated by a dynamic authentication factor or
- an advanced electronic signature containing subject signature biometric informations such as speed, pressure and pen inclination, collected by an application authorized by the *Provider*.
- a qualified signature of the Subscriber if the subscriber performs the in presence identification of the Subject

4.1.1 Who May Submit a Certificate Application

Certificate Application may only be submitted by natural persons, requesting a *Certificate* for themselves or for the organization represented.

The *Subscriber* and the *Subject*, in case of an *Organization*, the *Organization* representative shall provide their contact information during the *Registration Application*.

4.1.2 Enrolment Process and Responsibilities

During the process of the application the *Registration Authority* representative or delegate verifies the identity of the person submitting the *Certificate Application* (see section 3.2.3.).


If the Subject is an Organization and the name of an Organization is indicated in the Certificate, then the Registration Authority identifies the Organization (see section: 3.2.2.) and it ensures that the Subject is entitled to represent the Organization (see section: 3.2.5.) and to request a Certificate related to the Organization (see section: 3.2.2.).

The Subscriber determines which Subject is entitled to request a Certificate according to which Certificate Policy.

The Subject – in case of an Organization, its representative – shall provide all the necessary information for the conduct of the identification processes.

If the certificate is requested with QCP-n-qscd policy the Registration Authority ensures that the private key is generated within a QSCD under the sole control of the Subject.

If the certificate is requested with QCP-l-qscd policy the Registration Authority ensures that the private key is generated within a QSCD under the sole control of the Subject.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

If the certificate is requested with QCP-n policy the Registration Authority ensures that the private key is generated under the control of the Subject.

If the certificate is requested with QCP-I policy the Registration Authority ensures that the private key is generated under the control of the Subject.

The *Provider* may perform data reconciliation with public registers (such as the personal data and address register or the company register). In case of a database if it can be arranged, the *Provider* performs the data reconciliation electronically.

The *Provider* registers all the necessary information on the identity of the Subject and the Organization for the provision of service and for keeping contact.

The *Provider* registers the service agreement signed by the Subscriber that shall contain the Subscriber's statement that the Subscriber is aware of its obligations and undertakes the compliance.


The *Provider* registers the Certificate Application which shall contain the following:

- a confirmation, that the data provided in the *Certificate Application* are accurate;
- a consent, that the *Provider* records and processes the data provided in the application;
- a statement that there's no brand name or trademark indicated in the requested *Certificate*, or it is indicated, and the applicant is entitled to use that.
- a reference to the service agreement used (or the signed service agreement)

The *Provider* keeps the aforementioned records for the time period required by law.

The *Provider* archives the Certificate Application document and every attestation that the Represented Organization, the Subject or the Subscriber handed in.

If the identity of the Subject – in case of an Organization, its representative – or in case of an Organizational Certificate the identity of the Organization or in case of an Organizational Certificate issued to a natural person, the Subject's inherency to the Represented Organization cannot be verified without a doubt or any of the indicated data on the Certificate application form is incorrect, then the *Provider* can, according to its inner regulations give the Client the opportunity to correct the missing or incorrect data, and to hand over the missing attestations within 3 months from the submission

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

of the Certificate Application.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The Registration Authority identifies the *Subject* according to Section 3.2, and it verifies the authenticity of the request.

The Registration Authority submits to the provider the Certificate Application and identification evidences.

In case of organization Certificate request, the Organization will be identified too, and the verification of the privileges takes place according to section 3.2. The Provider registers all the information used by the Subject or in case of an Organizational Certificate the Organization to certify its identity, including the registration number of the documentation used for the certification and the incidental limitations related to its validity.

4.2.2 Identity authentication with two authentication factors

The *Provider* generates and associate to each validated Subject data two authentications factors (one dynamic). A new certificate request can be submitted together with the two authentication factors. A new certificate is issued if:


- the verification of both authentication factors is successful;
- the identity evidences are not expired
- the request is in the boundary of the service agreement

4.2.3 Approval or Rejection of Certificate Applications

To avoid any conflicts of interests, the *Provider* ensures its personal and operational independence from the Subscriber. It does not constitute a breach of conflicts of interests, if the *Provider* issues Certificates for its associates.

The Registration Authority verifies the authenticity of all the information given in the Certificate Application to be indicated on the Certificate before issuing the Certificate.

If the Subject requests a Certificate containing an e-mail address, the Registration Authority verifies the e-mail address to be indicated in the Certificate.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

The *Provider* accepts or refuses to fulfil the Certificate Application after processing it.

If the identity of the natural person or the organization which is to be identified, or in case of a personal *Certificate*, the *Subject's* inherency to the *Represented Organization* cannot be verified without a doubt or any of the indicated data on the *Certificate Application* form is incorrect, and the *Client* did not correct it for the request of the *Provider*, then the *Provider* rejects the application.

In case of *Certificate Application* refusal, the *Provider* informs the *Subject* and the *Subscriber*, but the *Provider* does not have to justify its decision.

4.2.4 Time to Process Certificate Applications

The *Provider* undertakes the processing of the *Certificate Application* within 5 workdays if all the necessary data and document is available.


4.3 Certificate Issuance

Certification Authority uses high security HSM for certificate signature using a 4096 RSA Key. This guarantees a substantial protection against forgery.

The issued Certificate only contains the data that was indicated in the Certificate Application and that was verified by the Provider (or by the Registration Authority) during the evaluation process.

If the Certification Authority provides the Electronic Signature Creation Device to the Subject (within the framework of device provision service), as a part of the process, the issued Certificate is installed to the Electronic Signature Creation Device. The handover of the Electronic Signature Creation Device containing the private key takes place in a controlled environment in accordance with the safety regulations defined in section 6.1.2.

If the takeover of the Electronic Signature Creation Device containing the Subject's Certificate and private key to the Subject do not take place right after the personal identification related to the Certificate application, then the Subject (in case of a non-natural person, its representative) can take over their device after personal identification, in the course of they have to identify themselves with an identification document. The transferring party verifies, that the portrait of the Subject matches the one on his/her ID card, and the Signature of the Subject fits the one appears on the ID card.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

Along with the takeover of the Electronic Signature Creation Device, the Subject receives the activation codes necessary for activation, generated according to section 6.4. These codes are handed in a closed envelope, and it is mandatory for the Subject to open and verify whether the codes are readable.

4.3.1 CA Actions During Certificate Issuance

The *Certificate* issuance happens according to strictly regulated and controlled processes, the details are stated by the Provider 's inner regulations and requirements.

4.3.2 Notification of the Subscriber about the Issuance of the Certificate

The Certification Authority informs the *Subject* and the *Subscriber* on the issuance of the *Certificate* and enables the *Subject* to receive the *Certificate*.

A unique revocation code is associated to the certificate and transmitted to the Subject and the Subscriber.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance


The *Subject* – in case of a certificate issued to an Organization, the representative of the *Subject* - shall verify the accuracy of the data indicated in the *Certificate* during the takeover of the *Certificate*.

If the Certification Authority provides local *Qualified Electronic Signature Creation Device* to the *Subject*, after the reception of the *Qualified Electronic Signature Creation Device* containing the private key, the *Certificate* of the *Subject* and the code necessary for activation the *Subject* can test his/her device. The use of the device implies the acceptance of the certificate.

If the Certification Authority or a Registration Authority provides remote *Qualified Electronic Signature Creation Device* to the Subject the activation by the subject of the remote device implies the acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

If the service agreement allows certificate disclosure and the subject asks for it, after the *Certificate* receipt the *Provider* discloses the *Certificate* in its *Certificate* store.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

If the *Certificate* was issued for the *Subject* to create electronic signature on behalf of an *Organization* the contact of the *Represented Organization* is notified by the *Provider* on the *Certificate* issuance without delay.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The *Subject* shall only use its private key corresponding to the *Certificate* for electronic signature creation, and any other usage (for example, authorization and encryption) is prohibited.

A private key corresponding to an expired or revoked *Certificate* shall not be used for electronic signature creation.


The *Subject* is bound to ensure the adequate protection of the private key and the activation data (password and other static or dynamic authentication factors).

The limitations determined in Section 1.4. shall be followed during the usage.

4.5.2 Relying Party Public Key and Certificate Usage

To retain the level of security guaranteed by the *Provider*, in the course of accepting the electronic signature verified, the *Relying Party* is recommended to proceed prudentially particularly regarding to the following:

- the *Relying Party* shall verify the validity and revocation status of the *Certificate*;
- *Certificates* for electronic signatures and the corresponding public keys shall only be used for electronic signature validation;
- the verifications related to the *Certificate* should be carried out for the entire certificate chain;
- the electronic signature verification shall be performed with a reliable application, which complies with the related technical specifications, can be resiliently configured, and has been set correctly, and it runs within a virus-free environment;
- in case of personal *Certificates* related to an organization, it is recommended to

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

verify that the title of the Signatory by which it is entitled to sign the document can be identified by the certificate (for example indicated in the Title field);

- it is recommended to verify that the *Certificate* was issued according to the appropriate *Certificate Policy*;
- when accepting a qualified electronic signature, it is recommended to verify that the *Certificate* was issued based on a *Certificate Policy* requiring Qualified Electronic Signature Creation Device;
- it is recommended to verify the highest value of the obligation undertaken at one time indicated in the *Certificate* (the *Certification Authority* is not responsible for the claims arising from electronic documents issued and signed concerning transactions in excess of those limits and for the damage caused this way.);
- the *Relying Party* shall consider any restrictions indicated in the *Certificate* or in the regulations referenced in the *Certificate*.

The *Provider* makes available a service for its *Clients* and *Relying Parties* that they can use to verify the issued *Certificates*.

4.6 Certificate Renewal


Certificate renewal is the process when the *Provider* issues a new *Certificate* for a new validity period for the same public key with unchanged *Subject* identity information

The *Subject* shall initiate the *Certificate* renewal before the *Certificate* expiration date. The *Certificate* renewal technically means the issuance of a new *Certificate*, with the same *Subject* identification data, but new validity period. Other data can change in the *Certificate*, like the CRL, OCSP references or the provider key used for signing the *Certificate*.

4.6.1 Circumstances for Certificate Renewal

Certificate renewal is only permitted when all of the following conditions are met:

- the *Certificate* renewal request was submitted within the validity period of the *Certificate*;
- the *Certificate* to be renewed is not revoked;

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

- the private key corresponding to the *Certificate* is not compromised;
- the *Subject* identity informations are still valid.

The *Provider* shall only accept a *Certificate* renewal application within the effect of the service agreement.

If any of the *Subject* data indicated in the *Certificate* changed, then a *Certificate* shall be requested within the framework of *Certificate* modification (see section 4.8.).

During the *Certificate* renewal, the *Subject* is informed if the terms and conditions have changed since the previous *Certificate* issuance.

If the *Subject* is not the same as the *Subscriber*, then the information aforementioned is also provided to the *Subscriber*.

4.6.2 Who May Request Renewal

The *Certificate* renewal shall be initiated by a person who is entitled to submit an application for a new *Certificate* of the same type on behalf of the *Subject* at the time of the submission of renewal application.

The applicant shall state in the *Certificate* renewal application, that the *Subject* identification data indicated in the *Certificate* are still valid.


The *Provider* is entitled to initiate the renewal of the *Certificate* if the service signatory key used for the issuance of the *Certificate* shall be replaced.

The certificate renewal request is signed with the valid certificate to be renewed.

4.6.3 Processing Certificate Renewal Requests

During the evaluation of the *Certificate* renewal application, the *Provider* verifies that:

- the submitted *Certificate* renewal application is authentic;
- the submitter of the *Certificate* renewal application has the appropriate entitlement and authorization;
- the submitter of the *Certificate* renewal application stated that the data of the *Subject* to be indicated in the *Certificate* are unchanged and accurate;
- the identification evidences of the previous certificate are still valid

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

- the Certificate renewal application was submitted during the Certificate's validity period;
- the Certificate to be renewed exists is not revoked;
- based on currently available information about the cryptographic algorithms used, they still will be applicable even during the planned validity period of the Certificate to be issued.

4.6.4 Notification about the New Certificate Issuance

The *Provider* informs with an email the *Subject* and the *Subscriber* about the *Certificate* issuance. A unique revocation code is associated to the certificate and communicated to the *Subject* and *Subscriber*.

Current terms and conditions are communicated to the *Subject* and *Subscriber*.

4.6.5 Conduct Constituting Acceptance of a Renewed Certificate

During the *Certificate* renewal process, there is no key generation, thus there is no need to handover key to the *Subject*. The renewed *Certificate* can be received (downloaded) without personal encounter.

If the private key of the *Subject* is on an *Electronic Signature Creation Device*, then the *Subject* installs the *Certificate* into the device.

The subject accepts the *Certificate* by its usage without additional declaration.

4.6.6 Publication of the Renewed Certificate by the CA


The *Provider* discloses the renewed *Certificate* the same method as the original *Certificate*.

4.6.7 Notification of Other Entities about the Certificate Issuance

If the *Certificate* was issued for the *Subject* to create electronic signature on behalf of an *Organization* the contact of the *Represented Organization* is notified by the *Provider* on the *Certificate* issuance without delay.

4.7 Certificate Modification

Certificate modification is not allowed. A certificate with wrong data must be revoked.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

If the error has been caused by the Provider or by the Registration Authority the wrong certificate will be revoked and the new one will be issued without any additional charge for the client.

If the error has been caused by Subject and/or Subscriber, the certificate will be revoked and the new one will be issued with ordinary procedure.

4.8 Certificate Revocation or Suspension

Certificate revocation terminates the validity of the *Certificate* before expiration. The *Certificate* revocation is a permanent and irreversible status change; the revoked certificate will never be valid again.

The usage of the private key belonging to the revoked *Certificate* shall be terminated immediately.

If possible, the private key belonging to the revoked *Certificate* shall be destroyed immediately after revocation.

Suspension is a form of revocation that suspend the validity of the *Certificate* until:

- a revocation is requested or
- the suspension state is removed, and the certificate is reinstated


Responsibility regulations related to revocation:

- Before the revocation request is received by the *Provider*, the *Subject* and the *Subscriber* are responsible for the damages arising.
- If the *Provider* has already published the revoked state of the *Certificate*, the *Provider* does not take any responsibility, if the *Relying Party* considers the *Certificate* valid.

4.8.1 Circumstances for Revocation


Certification Authority takes action on the revocation of the end-user *Certificate* in the following cases:

1. *Certificate* modification because of data change referring to the *Subject*;
2. the *Provider* becomes aware that the data in the *Certificate* does not correspond

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

to reality;

3. if the *Provider* issued the *Certificate* based on a document from a third party, and the third party withdraws that document in writing;
4. the *Subject* or the *Subscriber* requests the revocation of the *Certificate* using the defined channels;
5. the *Provider* becomes aware that the private key is not in the exclusive possession of the *Subject* , or in case of the Remote Signature Service, does not have sole control over the private key;
6. the *Provider* becomes aware that the certificate was used illegally;
7. the *Subscriber* failed to fulfil any of its financial obligations according to the terms and conditions;
8. the termination of service;
9. the *Provider* becomes aware that the public key in the *Certificate* does not comply with the requirements defined in Section 6;
10. the *Provider* becomes aware that the *Certificate* was not issued according to the related *Qualified Signature Certificate Policy* and the *Certification Practice Statement*;
11. the *Provider* becomes aware that the private key of the *Certificate* issuer certification unit might be compromised;
12. the format and technical content of the *Certificate* presents an unacceptable risk to the *Relying Parties* (for example, if the used cryptographic algorithm or key size is no longer secure);
13. the *Provider* is no longer entitled to issue *Certificates*, and maintenance is not provided for the existing CRL and OCSP services;
14. the *Provider* has terminated its activities;
15. the law makes revocation mandatory;
16. the QSCD security certificate, monitored by the *Provider*, is not valid anymore.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

4.8.2 Who Can Request Revocation

The revocation of the *Certificate* may be initiated by:

- the Subscriber;
- the Subject;
- in case of *Organizational Certificate*, the *Organization's* authorized representative;
- the contact person specified in the service agreement;
- the Provider.

4.8.3 Procedure for Revocation and Suspension Request

The *Provider* ensures the following possibilities to submit a revocation request:

- in automatic electronic form - available 24/7 - using the certificate revocation code given to Subject and Subscriber when the certificate has been created. The *Provider* can further authenticate the request using data available in the certificate record.
- in electronic form on *Provider* web site. The *Provider* will verify the requester right to revoke the certificate using data available in certificate record (i.e. email, mobile phone).

The reason for revocation shall be stated. If the revocation was requested by the *Client* and it does not state the reason for revocation, then the *Provider* considers that the reason for revocation is that the *Subject* does not want to use the *Certificate* anymore.

In case of a successful revocation the *Provider* notifies the *Subject* and the *Subscriber* about the fact by e-mail.


The *Provider* logs every revocation or suspension request.

4.8.4 Revocation Request Grace Period

The *Provider* does not apply grace period during the fulfilment of revocation requests.

4.8.5 Time Within Which CA Will Process the Revocation Request

The *Provider* processes the revocation requests submitted in electronic form immediately if the revocation code is submitted or within 24 hours.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

The time of arrival is when the Client provides all the necessary data for revocation.

4.8.6 Revocation Checking Requirement for Relying Parties

To maintain the level of security guaranteed by the *Provider*, prior to the adoption and use of the information indicated in the *Certificate*, it is necessary for *Relying Parties* to act with proper carefulness. It is particularly recommended for them to verify all of the *Certificates* located in the *Certificate* chain according to the relevant technical standards. The verification should cover the verification of the *Certificates*' validity, the policy requirements and key usage, and the checking of the referenced CRL or OCSP based revocation information.

4.8.7 Circumstances for Suspension

The *Provider* ensures a possibility for the temporary suspension of the *Certificate*

The *Provider* is entitled for *Certificate* suspension for the following reasons:

- The *Subscriber* does not pay within the payment deadline.
- If the *Provider* presumes that the data indicated on the *Certificate* does not comply with reality. If the *Provider* becomes aware of those conditions, it initiates the suspension or revocation of the *Certificate*.
- If the *Provider* presumes that the private key belonging to the *Certificate* is not in the possession of the *Subject*, and it is confirmed by substantial evidence. If the *Provider* becomes aware of that the *Electronic Signature Creation Device* is possessed by an unauthorized person, the *Provider* suspends every *Certificate* it contains.

The *Provider* does not accept suspension requests related to a *Certificates* not valid, in addition to justify the reason for rejection. Suspended certificate can be reinstated.


4.8.8 Who Can Request Suspension

The suspension of a *Certificate* can be requested by the same persons eligible to initiate the revocation of the *Certificate* (see section 4.8.2.)

4.8.9 Procedure for Suspension and Reinstatement Request

The *Provider* ensures opportunity for certificate suspension or reinstatement using the same channel and timing used for revocation (see section 4.8.3).

The *Provider* logs every suspension or reinstatement request. In case of a successful

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

suspension, the *Provider* notifies the *Subject* and the Subscriber about the fact of the suspension by e-mail.

4.8.10 CRL Issuance Frequency

The *Provider* issues a new *Certificate Revocation List* (CRL) at least once a day.

The validity of these certificate revocation lists is to a maximum of 25 hours.

4.8.11 Maximum Latency for CRLs

At most 5 minutes elapse between the generation and disclosure of the revocation list (CRL).

4.8.12 Online Revocation/Status Checking Availability

The *Provider* provides online *Certificate* status (OCSP) service. The status service complies with the requirements of Section 4.9

4.8.13 Special Requirements for Key Compromise

In case any CA key is compromised, the *Provider* makes every reasonable effort in order to notify the *Relying Parties* about the incident. It publishes any status change on the provider *Certificates* on its webpage.

This event is addressed as a disaster. All subscribers and other entities with a relationship with the CA, other relying parties will be informed.

In case of compromised *Certificates* issued by the *Provider*, the *Provider* is able to revoke the end-user *Certificate* belonging to the compromised private key. The revocation reason information (reasonCode) in this case is set to "keyCompromise" value.


4.8.14 Maximum Delay for Revocation Status Availability

Revocation or suspension OCSP status will be available within 60 minutes after revocation or suspension is confirmed.

4.9 Certificate Status Services

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

- OCSP – online *Certificate* revocation status query service,

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

- CRL – certificate revocation lists.
- a REST service for Registration Authorities that lists all the certificate events (creation, revocation, suspension, reactivation) given the Certificate revocation code provided by Subject or Subscriber.

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 CA 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.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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

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

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

The OSCP service can be reached through the URLs indicated on the *Certificates*.

The OSCP responses always contain the current information listed in the revocation registry of the *Provider*, but if the "thisUpdate" time of the OSCP 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 OSCP 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 *Certificates* 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

The *Provider* may revoke the end-user *Certificates* in case of the termination of the contract concluded with the *Subscriber*.

4.9.4 Key Escrow and Recovery

The *Provider* does not provide key escrow service for a private key belonging to a signatory *Certificate*.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

- 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.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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 <i>Provider</i>	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 <i>Provider</i> . Responsible, for the reliable and continuous operation of the assigned system units, and for monitoring

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

	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 <i>Provider</i> , 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.
RAO	Registration Authority Officer and Local Registration Authority Officer: individuals who performs natural and legal person identification and authorize certificates emission

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

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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*.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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 occasion of the planned or special training for the specific form of education.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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

5.4 Audit Logging Procedures

In order 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.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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*.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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);

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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 CA Key Changeover

The *Provider* ensures that the used *Certification 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 *Certification Units* and inform its Clients in time. 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.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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* and *Subject*;
- 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 Qualified Trust Services

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 *Certificate* issuance shall be terminated;
- *Provider* 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

© TrustPro QTSP Ltd	Facility, Management and Operational Controls	68
---------------------	---	----

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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 Key Pair Generation and Installation

The *Provider* makes sure that the generation and management of all the private keys generated by it – for itself, for its departments (for example *Certificate Repository*, *Registration Authority*) and for the *Subjects* – is secure and complies with the regulatory requirements in force and with industry standards.


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 CA management application.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

- The creation of the keys is carried out in a protected environment with exclusively trusted role holder persons present.
- In case of *Certificate Policies* requiring the use of a *Qualified Signature Creation Device* the signing private key is generated in the user's *Subject Qualified Signature Creation Device* which makes the disclosure of the signing private key impossible.
- If the private key is handed over to the *Subject*: The signer keys generated outside a *Qualified Signature Creation Device* are stored in an adequately secure environment by the *Provider* to prevent the disclosure. After the documented handover of the signer private key to the *Subject* the *Provider* destroys every copy of the handed over private key stored by it, in such a way that its restoration and usage becomes impossible.

6.2.1 Private Key Delivery to Subscriber

If the *Provider* generates the *Subject* private key, then the following requirements are met:

- During the whole service, the *Provider* shall store the private keys generated by it for the *Subjects* and the activation data securely to prevent the key disclosure, copy, modification, damage and the usage by unauthorized people.
- The *Provider* shall use an identification procedure that ensures that the private keys can only be used by the *Subject*.


If *Provider* does not generate the *Subject* private key:

- In case of *Certificate Policies* not requiring the use of a *Qualified Signature Creation Device*, the *Client* generates the private key.
- In case of *Certificate Policies* requiring the use of a *Qualified Signature Creation Device*, the *Client* always generates the private key into the *Qualified Signature Creation Device*.

6.2.2 CA 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.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

The *Provider* publishes certificates at this address:

<https://docs.trustpro.eu>

6.2.3 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*.

6.2.4 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*.


6.2.5 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.

6.2.6 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

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

- 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.

6.2.7 Private Key Multi-Person Control

The *Provider* implements the "2 out of 5" at the activation of the private key related key management functions. 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.

6.2.8 Private Key Escrow

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

6.2.9 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.

6.2.10 Private Key Archival


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

6.2.11 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.

6.2.12 Private Key Storage on Cryptographic Module

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

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

6.2.13 Method of Activating Private Key

The *Provider* keeps its provider private keys in a secure *Hardware Security Module*. It can only be activated by the corresponding operator cards and the private keys within the *Hardware Security Module* cannot be used before activating the module. The *Provider* keeps the operator cards in a safe environment and those cards can be only reached by entitled employees of the *Provider*.

The *Provider* ensures that signatures can only be created with the private key of the root unit certificate in case of commands issued directly by the trust official duly authorized to do so.

In case of the end-user private keys generated by the *Provider* it ensures that the private keys and the private key activation data are generated and managed in a properly secure way that excludes the possibility of the unauthorized usage of the private key.

6.2.14 Method of Deactivating Private Key

The private key managed by the cryptographic devices becomes deactivated if the device is removed from active status. This can happen in the following cases:

- the user deactivates the key,
- the power supply of the device is interrupted (switched off or power supply problem),
- the device enters an error state.

The private key deactivated like this cannot be used until the module is in active state again.


6.2.15 Method of Destroying Private Key

The *Provider* destroys the provider private keys stored in the secure *Hardware Security Module* according to the procedures, requirements defined in the user guide and in the certification documents of the used *Hardware Security Module*.

The *Provider* destroys each backup copy of the private key in a documented way in such a way that its restoration and usage become impossible.

6.2.16 Certificate Operational Periods and Key Pair Usage Periods

The validity period of the *Provider* root certification unit certificates and the private keys

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

belonging to them shall not exceed the amount of time until which the used cryptographic algorithms can be used safely according to the algorithmic decision of the National Authority.

The CA certificates are valid for 20 years, and the standard end-user certificate is valid for 3 years. On *Subscriber* request the *Provider* can issue end-user certificates with different validity time.

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

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

- Operational security
- Security in software development
- Incident management
- Business continuity
- Network security

6.6 Time Accuracy

System time accuracy is guaranteed by NTP protocol. The external time source is a reliable and official metrology national institute.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

7 Certificate, CRL and OCSP Profiles


CA certificates have following structure:

Version	Version 3
Serial Number	Serial number of the certificates
Signature	sha256, RSA
Issuer ^(SEP) (ETSI 319 412-2 par. 4.2.3.1)	Issuer DN: ^(SEP) countryName : "IE" ^(SEP) 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	Issuer DN: ^(SEP) countryName : "IE" ^(SEP) organizationName : "TrustPro QTSP Ltd" organizationIdentifier : "NTRIE-637218" L ="Dublin", OU ="QTSP" commonName : [CA 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 ^(SEP) Path Length Constraint: 0
KeyUsage (critical)	CertSign, cRLSign
Policy Constraints	requireExplicitPolicy : 0

7.1 Certificate Profiles

The end-user *Certificates* issued by the *Provider* and the provider certification unit *Certificates* used 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]

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

- 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

The *Provider* uses a distinguished name – composed of attributes defined in the above Certificate profile standards for the Subject identification in the *Certificates* issued based on this *Certification Practice Statement*.

The *Certificate* contains the globally unique identifier of the *Subject* filled out as defined in Section 3.1.1.

The value in the "Issuer DN" field of the *Certificate* is identical to the value in the "Subject DN" field of the issuer *Certificate*.


7.1.5 Name Constraints

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

7.1.6 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.

Following Object Identifiers identify ETSI EN 319411-2 [3] policies.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

OID	Policy	Person	QSCD	SCD
1.3.6.1.4.1.52969.1.1	QCP-n	Natural	no	no
1.3.6.1.4.1.52969.1.2	QCP-l	Legal	no	no
1.3.6.1.4.1.52969.1.3	QCP-n-qscd	Natural	yes	no
1.3.6.1.4.1.52969.1.4	QCP-l-qscd	Legal	Yes	No

7.1.7 End user certificate profile details


For each certificate policy supported certificate fields details are described in this section.

7.1.7.1 Policy QCP-n: qualified certificate for natural person

Serial Number	Certificate serial number
Issuer ^[1] DN	CN =[CA NAME] C ="IE" ^[1] O ="TrustPro QTSP Ltd" OU ="QTSP" L ="Dublin" organizationIdentifier =" NTRIE-637218"
Subject DN	CN =[subject given name and subject surname], SN =[subject surname], G =[subject given name], email =[subject email], dnQualifier =[subject unique ID], C =[subject country], serialNumber =[according to ETSI EN 319 412-1 par. 5.1.3]
Validity Period	3 years or as defined in the contract with subscriber
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 ^[1] Path Length Constraint: none
KeyUsage	No repudiation
Certificate Policies	Policy OID 0.4.0.194112.1.0: qualified certificates issued to natural persons Policy OID ^[1] 1.3.6.1.4.1.52969.1.1 ^[1] CP URL: https://docs.trustpro.eu/trustpro-cpcps-en.pdf
CRL distribution point	http://ca.trustpro.eu/crls/[CANAME].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-pds-en.pdf , "en"

7.1.7.2 Policy QCP-l: qualified certificate for legal person

Serial Number	Certificate serial number
Issuer ^[1] DN	CN =[CA NAME] C ="IE" ^[1] O ="TrustPro QTSP Ltd" OU ="QTSP" L ="Dublin" organizationIdentifier =" NTRIE-637218"
Subject DN	CN =[subject common name], dnQualifier =[subject unique ID], C =[subject country], serialNumber =[according to ETSI EN 319 412-1 par. 5.1.4]
Validity Period	3 years or as defined in the contract with subscriber
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 ^[1] Path Length Constraint: none
KeyUsage	No repudiation

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public


Certificate Policies	Policy OID 0.4.0.194112.1.1: qualified certificates issued to legal persons Policy OID, ^[1] _[SEP] 1.3.6.1.4.1.52969.1.2, ^[1] _[SEP] CP URL: https://docs.trustpro.eu/trustpro-cpcps-en.pdf
CRL distribution point	http://ca.trustpro.eu/crls/[CANAME].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-pds-en.pdf , "en"; id-etsi-qct-esed 2 (OID 0.4.0.1862.1.6.2)

7.1.7.3 Policy QCP-n-qscd: qualified certificate for natural person on QSCD

Serial Number	Certificate serial number
Issuer ^[1] _[SEP] DN	CN =[CA NAME] C ="IE" ^[1] _[SEP] O ="TrustPro QTSP Ltd" OU ="QTSP" L ="Dublin" organizationIdentifier ="NTRIE-637218"
Subject DN	CN =[subject given name and subject surname], SN =[subject surname], G =[subject given name], email =[subject email], dnQualifier =[subject unique ID], C =[subject country], serialNumber =[according to ETSI EN 319 412-1 par. 5.1.3]
Validity Period	3 years or as defined in the contract with subscriber
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 ^[1] _[SEP] Path Length Constraint: none
KeyUsage	No repudiation
Certificate Policies	Policy OID 0.4.0.194112.1.2: qualified certificates issued to natural persons with private key on QSCD Policy OID, ^[1] _[SEP] 1.3.6.1.4.1.52969.1.3, ^[1] _[SEP] CP URL: https://docs.trustpro.eu/trustpro-cpcps-en.pdf
CRL distribution point	http://ca.trustpro.eu/crls/[CANAME].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-QcSSCD (OID 0.4.0.1862.1.4) id-etsi-qcs-QcPDS (OID 0.4.0.1862.1.5) = https://docs.trustpro.eu/trustpro-pds-en.pdf , "en"

7.1.7.4 Policy QCP-l-qscd: qualified certificate for legal person on QSCD

Serial Number	Certificate serial number
Issuer ^[1] _[SEP] DN	CN =[CA NAME] C ="IE" ^[1] _[SEP] O ="TrustPro QTSP Ltd" OU ="QTSP" L ="Dublin" organizationIdentifier ="NTRIE-637218"
Subject DN	CN =[subject common name], dnQualifier =[subject unique ID], C =[subject country], serialNumber =[according to ETSI EN 319 412-1 par. 5.1.4]
Validity Period	3 years or as defined in the contract with subscriber
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 ^[1] _[SEP] Path Length Constraint: none

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

KeyUsage	No repudiation
Certificate Policies	Policy OID 0.4.0.194112.1.3: qualified certificates issued to legal persons with private key on QSCD Policy OID, ^[16] 1.3.6.1.4.1.52969.1.4, ^[16] CP URL: https://docs.trustpro.eu/trustpro-cpcps-en.pdf
CRL distribution point	http://ca.trustpro.eu/crls/[CANAME].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-QcSSCD (OID 0.4.0.1862.1.4); id-etsi-qcs-QcPDS (OID 0.4.0.1862.1.5) = https://docs.trustpro.eu/trustpro-pds-en.pdf , "en"; id-etsi-qct-esel 2 (OID 0.4.0.1862.1.6.2)

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 <i>Certification Authority</i> 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 <i>Certificates</i> with the serial number of the <i>Certificate</i> 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.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

7.3.1 Version Number(s)

The *Provider* supports the online certificate status requests and responses conforming to the Version 1 according 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)".

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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.


	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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 customerservice.

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

See section: 9.1.

9.1.2 Certificate Access Fees

The *Provider* grants free of charge on-line access to its *Certificate Repository* for the *Relying Parties*.

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.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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:
 - private keys and activation codes,
 - certificate applications and Service Contracts,
 - 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

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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 PKI Disclosure Statement in: <https://docs.trustpro.eu/trustpro-pds-en.pdf>

9.8 Limitations of Liability

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

9.9 Indemnities

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

9.10 Term and Termination

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

9.11 Individual Notices and Communications with Participants

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

9.14 Governing Law

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

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

9.15 Compliance with Applicable Law

Refer to the PKI Disclosure Statement in: <https://docs.trustpro.eu/trustpro-pds-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*.

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

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

	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	10-Apr-2024		Public

	(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