Trust Service Practice Statement

Ver. 2.1

November 11, 2026

History

Changes	Rev.	Data	Author	Verifier	Approval
First release	1.0	07/04/17	F.Barcellini	G.Damiano	P.Sironi
Clause 4.8 updated to include the maximum delay for certificate status publication	1.1	21/05/2017	F.Barcellini	G.Damiano	P.Sironi
General revision of the document. Added Advanced Electronic signature certificates and qualified certificates	1.2	07/07/17	F.Barcellini	G.Damiano	P.Sironi
Corrected title, general index, some inaccuracies	1.3	02/08/17	F.Barcellini	G.Damiano	P.Sironi
Correction on tables in paragraph 7	1.4	15/09/17	F.Barcellini	G.Damiano	P.Sironi
General revision of the document	1.5	22/11/17	F.Barcellini	G.Damiano	P.Sironi
Formatting correction. Modification to paragraph 1.3.1; 1.3.4; 3.1.4; 3.2.4; 3.2.5; 4.2; 4.5.3; 6.2.2; 6.2.8; 6.2.9; 6.2.10; 7; 8.6.	1.6	20/12/17	F.Barcellini	G.Damiano	P.Sironi
Modification to paragraph 3.1.4.	1.7	17/01/18	F.Barcellini	G.Damiano	P.Sironi
Modification to paragraphs 3.1.3, 3.2.3, 3.2.6 and 3.2.7.	1.8	13/03/18	F.Barcellini	G.Damiano	P.Sironi
Modification to paragraphs 3.4, 9.3.3 e .94	1.9	20/07/18	F.Barcellini	G.Damiano	P.Sironi
Modification to paragraphs 4.2, 6.1.1.2, 6.1.2	1.10	08/07/2019	F.Barcellini	G.Damiano	P.Sironi
Modification to paragraphs 1.3, 1.3.2, 1.3.6, 1.4, 1.6, 2.2, 3.1.1, 3.1.2, 3.1.3, 3.1.6, 3.1.7, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 4.1.2, 4.3.1, 4.4.1, 4.4.2, 4.9.1, 4.9.2, 5.1,5.2, 5.3, 5.4.1, 5.8, 6.1.5, 6.1.6, 6.2.1, 6.2.2, 6.6, 8. Added paragraphs 1.3.7, 3.2.8, 4.3.1.1, 4.3.2, 7.1.7, 7.1.8, 7.2.1, 7.2.2, 7.2.3, 7.2.4	1.11	09/03/2020	F.Barcellini V. Manaila	G.Damiano	P.Sironi
Added paragraph 3.2.9	1.12	12/01/2021	F.Barcellini	F.Barcellini	P.Sironi
Added paragraph 6.9	1.13	30/03/2021	F.Barcellini	F.Barcellini	P.Sironi
Changes to 1.1, 1.3.2, 1.4, 1.5, 3.1.4, 3.2.6, 3.2.8, 3.2.10, 4.1.1, 4.5.1.1, 4.6, 4.9.1, 6.8, 9.4	1.14	04/01/2021	B.Tafini	F.Barcellini	P.Sironi
Changes to 1.3, 3.2.3, 3.2.9, 3.2.10, 3.2.11. 3.2.12, 4.1.2, 4.2, 4.3, 4.9.15	1.15	25/06/2024	F.Barcellini	F.Barcellini	P.Sironi

Added paragraph 4.3.4, 4.11, 7,1 Modified paragraph: 1.3.1, 1.4, 3.2.5, 3.2.7, 4.6, 4.9.1, 4.9.3.3, 4.11, 9.12	1.16	10/03/2025	D. Saccò, M. Menghini	F. Barcellini	P.Sironi
Adaption for “management of remote qualified electronic signature creation devices” and “Identity Proofing Identity Provider” Adaption for Modified paragraph: 1.4, 3.2, 5.1, 6.1.5, 6.2.1, 6.5, 6.7, 7.1	2.0	04/03/2026	D. Saccò, M. Menghini	F. Barcellini	P.Sironi
Modification to paragraph 3.3.3, 5.4.3, 5.5.2, 6.1.1.2, 9.6.1, 9.6.6, 9.11	2.1	11/11/2026	D. Saccò	F. Barcellini	P.Sironi

Index

1 INTRODUCTION 11
1.1 Overview 11
1.2 Document Name and Identification 12
1.3 PKI participants 12
1.3.1 Intesi Group as Time Stamping and Certification Authority 12
1.3.2 Local Registration Authority 13
1.3.3 Subscribers or applicants 14
1.3.4 Subjects 14
1.3.5 Holders 14
1.3.6 RAO (Registration Authority Officer) 14
1.3.7 Relying parties or users 14
1.3.8 Other participants 14
1.4 Applicable Policies 15
1.4.1 Issuance of Certificates, Electronic Seals and Time Stamps 15
1.4.2 Management of Electronic Signature Creation Devices 16
1.5 Policy Administration 16
1.6 Abbreviations 17
2 PUBLICATION AND REPOSITORY 17
2.1 Repository management 17
2.2 Published information 18
2.3 Time and frequency of publications 18
2.4 Access control 18
3 IDENTIFICATION AND AUTHENTICATION 18
3.1 Naming 19
3.1.1 Types of names 19
3.1.2 Need for names to be meaningful 19
3.1.3 Subject's anonymity 19
3.1.4 Professional qualifications, role and organization 19

3.1.5 Rules for interpreting names 20
3.1.6 Uniqueness of names 20
3.1.7 Recognition, authentication, and role of trademarks 20
3.2 Initial Identity Proofing - eIDAS 21
3.2.1 Proving possession of private key 21
3.2.2 Authentication of organization identity 21
3.2.3 Identification and authentication requirements for an individual 21
3.2.4 Identification Data Acquisition 23
3.2.5 Face-to-face identification and registration 24
3.2.6 Identification through LRA process 25
3.2.7 Identification and registration through IDentify Web 25
3.2.8 Identification and registration through qualified signature verification 26
3.2.9 Identification by anti-money laundering regulation 26
3.2.10 Identification using SPID Identity 26
3.2.11 Identification using CIE Identity 27
3.3 Initial Identity Proofing – eIDAS2 27
3.3.1 Identification Methods and Associated OIDs 28
3.3.2 Verification Requirements and Procedures 28
3.3.3 Evidence Management and Retention 29
3.4 Identification and Authentication for Re-Key Requests 29
3.5 Identification and Authentication for Revocation Requests 29
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 29
4.1 Certificate Application 29
4.1.1 Who can submit a certificate request 29
4.1.2 Enrolment process and responsibilities 30
4.2 Application processing 30
4.2.1 Subject information required 31
4.2.2 Registration and authentication 31
4.3 Certificate Issuance 32
4.3.1 Qualified certificate issuance for remote signature 32
4.3.2 Qualified certificate issuance on physical QSCD device 33
4.3.3 TSA certificate issuance 34
4.3.4 Test certificate issuance 34

4.4 Certificate Acceptance 35
4.4.1 Certificate acceptance 35
4.4.2 Publication of the certificate by the QTSP 35
4.4.3 Notification of Certificate issuance by the QTSP to other entities 35
4.5 Key Pair and Certificate Usage 35
4.5.1 Subscriber private key and certificate usage 35
4.5.2 Relying Party public key and Certificate usage 36
4.5.3 User notice 36
4.6 Certificate Renewal 37
4.6.1 Procedure to process renewal request 37
4.6.2 Notification to the subscriber 37
4.6.3 Certificate acceptance 38
4.6.4 Publication of the certificate by the CA 38
4.6.5 Notification of Certificate issuance by the QTSP to other entities 38
4.7 Certificate Re-key 38
4.8 Certificate Modification 38
4.9 Certificate Revocation and suspension 38
4.9.1 Circumstances for revocation 38
4.9.2 Who can request revocation 39
4.9.3 Procedure for revocation request 39
4.9.4 Revocation request grace period 41
4.9.5 Time within which QTSP must process the revocation request 41
4.9.6 Revocation checking requirement for Relying Parties 41
4.9.7 CRL issuance frequency / OCSP response validity period 41
4.9.8 Maximum latency for CRLs 41
4.9.9 On-line revocation status checking availability 41
4.9.10 Other forms of revocation advertisements available 41
4.9.11 Special requirements regarding key compromise 41
4.9.12 Circumstances for suspension 41
4.9.13 Who can request suspension 42
4.9.14 Procedure for suspension and un-suspension requests 42
4.9.15 Limits on suspension period 42
4.10 Certificate Status Service 42
4.10.1 Service Availability 42

4.11 Timestamp Verification Services 42
4.12 End of Subscription 43
4.13 Key Escrow and Recovery 43
5 FACILITIES, MANAGEMENT, AND OPERATIONAL CONTROLS 43
5.1 Physical security 43
5.2 Procedural controls 44
5.3 Personnel security controls 45
5.4 Audit logging procedures 46
5.4.1 Type of events recorded 46
5.4.2 Frequency of processing log 46
5.4.3 Retention period for audit log 46
5.4.4 Protection of audit log 46
5.4.5 Audit log backup procedures 47
5.4.6 Audit collection system (internal vs. external) 47
5.4.7 Notification to event-causing subject 47
5.4.8 Vulnerability assessment 47
5.5 Record Archival 47
5.5.1 Type of records archived 47
5.5.2 Retention period for audit log 47
5.5.3 Protection of archive 47
5.5.4 Archive backup procedures 48
5.5.5 Requirements for timestamping of records 48
5.5.6 Procedure to obtain and verify archive information 48
5.6 Renewal of CA Key 48
5.7 Compromise and disaster recovery 48
5.7.1 Incident and compromise handling procedures 48
5.7.2 Computing resources, software, and/or data are corrupted 48
5.7.3 Entity private key compromise procedures 49
5.7.4 Business continuity capabilities after disaster 49
5.8 CA termination 49
6 TECHNICAL SECURITY CONTROLS 49

6.1 Key pair generation and installation 50
6.1.1 Key Pair Generation 50
6.1.2 Private key delivery to holder 51
6.1.3 Public key delivery to certificate issuer 51
6.1.4 CA public key delivery to Relying Parties 51
6.1.5 Key sizes 51
6.1.6 Public key parameters generation and quality checking 51
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 51
6.2 Private Key Protection and Cryptographic Module Engineering Controls 52
6.2.1 Cryptographic module standards and controls 52
6.2.2 Private key (n out of m) multi-person control 52
6.2.3 Private key escrow 52
6.2.4 Private key backup 53
6.2.5 Private key archival 53
6.2.6 Private key transfer into or from a cryptographic module 53
6.2.7 Private key storage on cryptographic module 53
6.2.8 Method of activating private key 53
6.2.9 Method of deactivating private key 53
6.2.10 Method of destroying private key 53
6.2.11 Cryptographic module rating 54
6.3 Other Aspects of Key Pair Management 54
6.3.1 Public key archival 54
6.3.2 Certificate operational periods and key pair usage periods 54
6.4 Activation data 54
6.5 Computer Security Controls 54
6.6 Life cycle technical controls 55
6.7 Network security controls 55
6.8 CA and Timestamping 55
6.9 Asset inventory 56
7 CERTIFICATE AND CRL PROFILE 56
7.1 Certificate profile 56
7.1.1 CA for Time-stamp certificate 56

7.1.2 CA for Qualified Electronic Signature 57
7.1.3 CA for Qualified Electronic Seal 58
7.1.4 Certificate for TSU 58
7.1.5 End User Certificate for Qualified Electronic Signature 59
7.1.6 Certificate for Qualified Electronic Seal 61
7.1.7 OCSP Certificate for Qualified Electronic Signature 63
7.1.8 OCSP Certificate for Qualified Electronic Seal 64
7.2 CRL profile 65
7.2.1 CRL issuing parameter 65
7.2.2 CRL for the Qualified Timestamp certificate 65
7.2.3 CRL for the Qualified Electronic Qualified certificate 66
7.2.4 CRL for the Qualified Electronic Seal certificate 67
7.3 Timestsamp Profile 67
8 COMPLIANCE AUDIT 68
8.1 Frequency or circumstances of assessment 68
8.2 Identity and qualification of assessor 69
8.3 Assessor's relationship to assessed entity 69
8.4 Topics covered by assessment 69
8.5 Actions taken as result of deficiency 69
8.6 Communication of results 69
9 OTHER BUSINESS AND LEGAL MATTERS 69
9.1 Service fees 70
9.2 Financial responsibility 70
9.3 Confidentiality of Business information 70
9.3.1 Confidential information 70
9.3.2 Non-confidential information 70
9.3.3 Responsibility for the protection of confidential information 71
9.4 Privacy of personal information 71
9.5 Intellectual Property Rights 71

9.6 Representation and warranties 71
9.6.1 Certification Authority 71
9.6.2 Registration Authority 72
9.6.3 Subscribers 72
9.6.4 Relying parties 72
9.6.5 Timestamp Authority 72
9.6.6 External suppliers 72
9.7 Disclaimer of warranties 72
9.8 Limitations of Liability 73
9.9 Indemnities 73
9.10 Term and Termination 73
9.11 Amendments 73
9.12 Dispute Resolution Provisions 73
9.13 Governing Law 74
9.14 Compliance with Applicable Law 74
9.15 Miscellaneous Provisions 74

1 INTRODUCTION

1.1 Overview

This Trust Service Practice Statement (TSPPS) describes the technical, security and organizational requirements implemented by Intesi Group S.p.A. (hereafter referred to also as “Intesi Group” or “QTSP” or “CA”) applicable to all the Trust Services that it provides and the trust service tokens that it issues:

- qualified signature certificates issued to natural persons;
- qualified seal certificates issued to legal persons;
- Time Stamping Unit certificates issuing qualified Timestamp Tokens;
- certificates and the CRLs issued by the Cas listed in the paragraph 1.3.1 and the related OCSP services;
- qualified timestamp tokens generation;
- management of remote qualified electronic signature creation devices;
- management of remote qualified electronic seal creation devices;

The qualified trust services comply with the relevant requirements of the eIDAS2 regulation (Regulation (EU) 2024/1183 amending Regulation (EU) 910/2014) and conforms to the following standards:

- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI EN 319 411 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates.
- ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles.
- ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.
- ETSI TS 119 431-1 Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev.
- ETSI TS 119 461 Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects.

The structure of this TSPPS conforms to the public specification [RFC 3647] and refers to the Certificate Policy whose OIDs are specified in subsection 7.1.3, hereafter referenced as “related TSPPs”. This TSPPS applies to the following certificates issued by Intesi Group:

- The CA root certificate dedicated to issue qualified signature certificates.
- The CA root certificate dedicated to issue certificates for qualified electronic seals.
- The CA root certificate dedicated to issue time stamp certificates.

- Time Stamp Server certificates.
- Time Stamp Tokens.

1.2 Document Name and Identification

Name and version of this document are indicated on the first page of this document.

This document is public and freely downloadable from the Intesi Group web site (https://www.intesigroup.com/it/qtsp/documenti/) and published on the AgID website (http://www.agid.gov.it).

1.3 PKI participants

Intesi Group is a Trust Service Provider that issues different types of certificates under this TSPPS. Intesi Group operates one or more Certification Authorities (CAs) which create and sign end entity digital certificates for electronic signatures, time stamps, electronic seals, according to EU eIDAS2 Regulation. Intesi Group uses various PKI services and its CAs are hosted in highly secured data centers. All equipment for running PKI services, including but not limited to CAs, OCSPs, RA servers, Server Signing Application (SSA as defined in [CEN/TS 419 241]), HSMs enjoy the same controls described in Section 5 and 6 for physical, personnel, procedural and technical security. The location and construction of the facility housing the CAs and equipment are consistent with facilities used to house high value, sensitive information.

1.3.1 Intesi Group as Time Stamping and Certification Authority

Intesi Group as QTSP acts as time stamping and certification authority and is fully identified as follows:

Company name: Intesi Group S.p.A.

Registered Office: Via Torino, 48 – 20123 Milano (MI) – ITALY

Legal representative: Paolo Sironi (Board of Directors)

VAT Reg. No. and Tax Code: IT02780480964

Telephone: +39 02 6760641

ISO Object Identifier (OID): 1.3.6.1.4.1.48990

Company web site: http://www.intesigroup.com

Company e-mail address: intesi@intesigroup.com

The Intesi Group PKI (Public Key Infrastructure) that issue qualified certificates is based upon a one-level hierarchy. The CA keys currently in use by Intesi Group and covered by this CPS are indicated with the following subjectDistinguishedName:

SubjectDistinguishedName	Use
CN=Intesi Group EU Qualified Electronic Signature CA G2, OrganizationIdentifier=VATIT-02780480964,	Used for qualified certificates for electronic signature

SubjectDistinguishedName	Use
OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., C=IT	
CN=Intesi Group EU Qualified Electronic Signature CA G3 ECC, OrganizationIdentifier=VATIT-02780480964, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., C=IT	Used for qualified certificates for electronic signature
CN=Intesi Group EU Qualified Electronic Seal CA G2, OrganizationIdentifier=VATIT-02780480964, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., C=IT	Used for qualified electronic seal certificates
CN=Intesi Group EU Qualified Electronic Seal CA G3 ECC, OrganizationIdentifier=VATIT-02780480964, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., C=IT	Used for qualified electronic seal certificates
CN=Intesi Group Qualified Time-Stamp CA G2, OrganizationIdentifier=VATIT-02780480964, O=Intesi Group S.p.A., OU=Qualified Trust Service Provider, C=IT	Used for qualified certificates for timestamp

1.3.2 Local Registration Authority

A Local Registration Authority (RA) is a third party that operates on behalf of Intesi Group, after agreements stipulated with Intesi Group, to carry out:

- Identification and Authentication (I&A) of the subjects requiring qualified certificates.
- Transmission (and if necessary, Conservation) to the QTSP of the identified subject information.
- registration of the applicant data and authorization to certificate issuance using tools made available by Intesi Group.
- validation and management of any suspension, unsuspension and revocation request.

Personal identification of Subjects applying for a certificate may take place at Intesi Group premises or at any of the LRAs used for this purpose. Personal identification of Subjects applying for a certificate may also be performed by at other locations by officers operating on behalf of Intesi Group.

LRAs are subject to periodical assessment by Intesi Group to verify the compliance with this TSSPS and to the agreements taken.

Intesi Group reserves the right to interrupt or suspend the identification service if, as a result of the assessment, found that the identifications were not carried out following the procedures provided during the RAO courses and/or do not comply with current regulations.

1.3.3 Subscribers or applicants

In this TSPPS subscribers and applicants are:

- Natural person holding the qualified certificate
- Natural person authorized to represent a legal person.
- Legal person.

1.3.4 Subjects

Subjects are:

- natural persons holding qualified electronic signature certificates.
- legal persons holding qualified seal certificates.

1.3.5 Holders

The holders are person using the private keys relating to a qualified signature certificate or qualified seal certificate. For qualified signature certificate is the subject, for qualified seal certificate is the person identified by the RAO and who has in use the credentials.

1.3.6 RAO (Registration Authority Officer)

RAOs are individuals involved in the process of identifying, collecting and recording personal data and responsible for the transmission (and if necessary, Conservation) of the documentation to the CA.

RAOs can be part of the QTSP or LRA staff and can operate after a mandate with the QTSP and only after having attended a training course.

At the end of the training course, operators are given access privileges to web applications made available by Intesi Group to carry out RAO activities. The assignment of the access privileges is under the control of the CA.

1.3.7 Relying parties or users

The "Relying Parties" are all the subjects that rely on the information contained in the certificates. They are all the subjects that verify electronic signatures and electronic seals through the qualified certificates issued according to this TSPPS.

1.3.8 Other participants

The activities carried out by the Intesi Group as QTSP are under the supervision of AgID (Agenzia per l'Italia Digitale) in accordance with article 17 of eIDAS2 Regulation.

Where Intesi Group engages external suppliers to support the provision of the trust services covered by this TSPPS, their assigned activities and responsibilities are defined in contractual agreements. Their obligations are described in section 9.6.6.

1.4 Applicable Policies

1.4.1 Issuance of Certificates, Electronic Seals and Time Stamps

The policy of qualified certificates for signatures and seals issued under this TSPPS are identified by the OIDs specified below.

Intesi OID	ETSI OID	AgID OID	Description
1.3.6.1.4.1.48990.1.1.1.1	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons using Remote QSCD.
1.3.6.1.4.1.48990.1.1.1.3	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons using Remote QSCD - Customer user notice.
1.3.6.1.4.1.48990.1.1.1.4	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons using Local QSCD.
1.3.6.1.4.1.48990.1.1.1.5	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons using Local QSCD - Customer user notice..
1.3.6.1.4.1.48990.1.1.1.6	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons identified with qualified signature using Remote QSCD
1.3.6.1.4.1.48990.1.1.1.7	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons using Remote QSCD used only to sign agreement with Intesi Group
1.3.6.1.4.1.48990.1.1.1.8	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons issued using the eID based on National ID card (CIE).
1.3.6.1.4.1.48990.1.1.2.1	QCP-l-qscd	agIDcert	Qualified Certificates for Qualified Seal using remote QSCD
1.3.6.1.4.1.48990.1.1.5.1	baseline-ts-policy	agIDcert	Qualified TSA
1.3.6.1.4.1.48990.1.3.2.1	QCP-n-qscd	agIDcert	Qualified remote signature Certificates issued only for test purposes
1.3.6.1.4.1.48990.1.3.3.1	QCP-n-qscd	agIDcert	Qualified automatic signature Certificates issued only for test purposes
1.3.6.1.4.1.48990.1.3.4.1	QCP-l-qscd	agIDcert	Qualified remote seal Certificates

			for issued only test purposes

Where:

1. QCP-n-qscd is 0.4.0.194112.1.2 defined into the standard ETSI EN 319 411-2;
2. QCP-l-qscd è 0.4.0.194112.1.3 defined into the standard ETSI EN 319 411-2;
3. baseline-ts-policy is 0.4.0.2023.1.1 Best Practices Policy for Timestamp defined into the EN 319 421 and is included in the time stamps to claim conformance to it;
4. agIDcert 1.3.76.16.6 to indicate the adherence to AgID "Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate" (Technical Rules and Recommendations relating to the generation of qualified electronic certificates, qualified electronic seals and qualified electronic time stamps);

1.4.2 Management of Electronic Signature Creation Devices

The remote qualified signature and seal creation management service is compliant with the requirements defined in ETSI 119 431-1 and, therefore, references the following policy OID EUSPv2:

OID	Descrizione
0.4.0. 19431.1.1.2	Normalized SSAS Policy
0.4.0.19431.1.1.4	EU SSAS Policy

The remote signing system used for this service is PkBox version 3.4, certified as a QSCD by A-Sit. The corresponding certificate of conformity is publicly available on Intesi Group's institutional website in the company section (https://www.intesigroup.com/en/company/) and can also be accessed on the A-Sit website at the following address: https://www.a-sit.at/wp-content/uploads/2025/06/VIG-25-036_QSCD-Certificate_Intesi_PkBox34-Update1_Final_sig-HL.pdf

1.5 Policy Administration

This TSPPS is developed, reviewed and updated by Intesi Group authorized staff and is published only after being approved by the Intesi Group management and by the Supervisor Body (AgID – Agenzia per l'Italia digitale).

For further information or explanations about this TSPPS, please write an e-mail to the following address: **tsp@intesigroup.com.**

1.6 Abbreviations

Abbreviation	Definition
CA	Certification Authority
CAO	Certificate Authority Officer
CRL	Certificate Revocation List
ETSI	European Telecommunications Standards Institute
eIDAS2	Regulation (EU) No 2024/1183 of the European Parliament and of the council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework
HSM	Hardware Security Module
OTP	One Time Password
PKI	Public Key Infrastructure – componente per l'emissione dei certificati
QTSA	Qualified Time-Stamping Authority
RAO	Registration Authority Officer
RFC	Request For Comments
TIN	Tax Identification Number
TLS	Transport Layer Security
TSA	Time-Stamping Authority
TSP	Trust Service Provider
TSPP	TSP Policy
TSPPS	TSP Practice Statement
TSU	Time-Stamping Unit

2 PUBLICATION AND REPOSITORY

2.1 Repository management

Intesi Group public repositories consist of the following websites:

- **http://www.intesigroup.com**

- **http://www.time4mind.com**

Intesi Group manages the repositories and is responsible for their maintenance and the publication and update of their content.

The repositories are available 24 hours a day, 7 days a week and are designed to guarantee 99.8% service levels (SLAs). In case of system failures or any events that can interrupt the service, Intesi Group will activate all the procedures aimed to restore the service as soon as possible.

2.2 Published information

On the Web repositories are published the following documents:

[1] TSP Practice Statement (TSPPS).
[2] PKI Disclosure Statement (PDS)
[3] Identity Proofing Service Practice Statement (IPPS)
[4] Terms & Conditions of the services.
[5] All CAs certificates.
[6] CRL – Liste di revoca dei certificati per tutte le CA.
[7] Various forms.

2.3 Time and frequency of publications

The frequency of updating and publication of the documentation is established by Intesi Group's internal processes. The version valid is the latest version available on the certification service website (www.intesigroup.com) or, where applicable, the documentation published on the AgID website (https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia).

For the CRL issuance frequency refer to section 4.

2.4 Access control

Access to documentation and CRLs is free and does not require authentication.

3 IDENTIFICATION AND AUTHENTICATION

The I&A procedures followed by Intesi Group comply with ETSI EN 319411-1 requirements and eIDAS2 Regulation.

3.1 Naming

3.1.1 Types of names

All the qualified certificates issued by Intesi Group comply with EU eIDAS2 Regulation, the Italian laws and the profile specified in the applicable parts of ETSI EN 319 412, namely part 2 for certificates issued to natural persons, part 3 for legal persons, part 5 for qualified certificates.

All the TSU certificates issued by “Intesi Group Qualified Time-Stamp CA G2” comply with the profile specified in ETSI EN 319 412-3 and the requirements specified in ETSI EN 319 422.

Intesi Group generates and signs only certificates that contain a non-null subject Distinguish Name (DN) complying with the X.500 standard. Certificates may also include other name forms in the subject alternative name forms field.

3.1.2 Need for names to be meaningful

Unless pseudonyms are used, the names used under this TSPPS and the applicable TSPP shall be meaningful as identifying certificate Subjects (physical and legal persons) or TSUs.

Intesi Group will determine the subscriber’s DN to make it compliant with common standards, practices and regulations requirements. The name should have commonly understood semantics (full name, company’s name, Internet e-mail address) for the relying parties to determine identity of the person and/or organization. However, the subscriber can choose a pseudonym instead of the real name in the qualified certificate. Intesi Group will issue such pseudonymized certificate.

3.1.3 Subject's anonymity

During a face-to-face identification (cfr.3), or at the moment of certificate request, the subscriber may request the use of a pseudonym instead of personal data to be inserted in the subjectDistinguishedName's pseudonym field of the qualified certificate. The use of a pseudonym is clearly indicated by the usage of a dedicated field “PSEUDO”.

The use of pseudonym is allowed only for certificates issued to a natural person. The use of pseudonyms is not applicable to digital seals and TSU certificates Intesi Group records subject personal information associated with the pseudonym for twenty (20) years from the issuance of the certificate in accordance with current legislation. This information is retained confidential and can never be disclosed to third parties unless foreseen by law.

3.1.4 Professional qualifications, role and organization

The certificate holder, independently or with the permission of a "Third Party", can require the insertion in the certificate of information on its qualifications, such as membership of professional colleges, the qualification of a public official, the possession of professional qualifications, information on powers of representation.

This information is inserted in the "title" attribute of the certificate's Subject field. In this case, the Applicant, in addition to the documentation and the required identification information, must also present documentation to demonstrate the possession of the specific role or professional qualification.

The QTSP includes into the certificate information about the organization only after having received an authorization from the organization and after having checked the formal regularity of the documentation submitted by the Applicant.

3.1.5 Rules for interpreting names

Names respect X.500 standard.

3.1.6 Uniqueness of names

The full combination of the Subject Attributes (SubjectDistinguishedName) grants the uniqueness of the names. For certificates issued to a natural person the information granting the uniqueness are:

- the Givenname (OID 2.5.4.44) containing the subject's first name.
- the Surname (OID 2.5.4.44) containing the subject's surname.
- the SerialNumber (OID 2.5.4.44) containing the subject's tax identification number or alternatively a code taken from the identity document used for the identification process.

The same Subject may have different certificates, all bearing the same subject DN, but no two separate subjects may share a common DN and be issued by the same CA. To avoid conflict, Intesi Group add a unique registration number into the DNQualifier field of the subjectDistinguishedName.

When the subject uses a pseudonym the names uniqueness is guaranteed by the uniqueness of DNQualifier .

For certificates issued to a legal person the uniqueness is guaranteed by the combination of the fields:

- OrganizationName (OID 2.5.4.10) containing the full registered name of the subject (legal person).
- Organization Identifier (OID 2.5.4.97) containing an identification of the subject organization different from the organization name. This field is valued according to ETSI EN 319 412-1 [i.4].

For TSU certificates the uniqueness is granted by Intesi Group's internal procedures.

3.1.7 Recognition, authentication, and role of trademarks

The Subscribers must guarantee to operate in the full compliance with national and international intellectual property laws.

Intesi Group does not check the use of trademarks and may refuse to issue or force the revocation of certificates involved in a legal dispute. Intesi Group is not responsible for resolving name claim disputes among subscribers.

3.2 Initial Identity Proofing - eIDAS

These methods will be gradually phased out and replaced by the processes described in the following section. They will no longer be used from 22 May 2026 and will be fully discontinued by 19 August 2027.

3.2.1 Proving possession of private key

The proof-of-possession of the private key corresponding to the requested certificate is based on the cryptographic verification of the CSR (Certificate Signing Request) sent to the CA. In fact, the subscriber, using Intesi Group application managing secure connection, sends its own public key to the QTSP in the form of a CSR in PKCS#10 format [RFC2314]. The QTSP shall verify that the digital signature in the CSR is valid.

If Intesi Group generates within its premises the private key belonging to the qualified certificates of the Subject, verification is done through an internal process.

3.2.2 Authentication of organization identity

The application for qualified certificate issued to a legal person (electronic seal) is done by a natural person representing the legal person and who is identified according to the same procedures used for natural persons (see par. 3.2.3).

The legal person's powers of attorney must be demonstrated providing to QTSP (or to RAO) appropriate documentation issued by an authoritative body such as, for example, an official certification issued by a chamber of commerce, a competent official register in which the organization is listed (or a comparable document) .

Governmental or administrative authorities must supply documents which reflect their relationship to the next higher entity (e.g., a superior authority) with official letterhead, stamped with an official stamp or seal, and signed by an authorized officer.

The documentation must include:

- full name and legal status of the associated legal person or other organizational entity,
- relevant existing registration information (e.g., company registration) of the associated legal person or other organizational entity.

3.2.3 Identification and authentication requirements for an individual

Intesi Group supports all mechanisms for identity verification, as defined by EU eIDAS2 Regulation, art.24 requiring that the identity and any specific attributes of the natural or legal person to whom the qualified certificate is issued is verified by Intesi Group either directly or by relying on a third party in accordance with national law:

a. by the physical presence of the natural person or of an authorized representative of the legal person; or

b. remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorized representative of the legal person was

ensured and which meets the requirements set out in Article 8 of eIDAS2regulation with regard to the assurance levels 'substantial' or 'high'; or

c. by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or

d. by using other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.

The identification process is executed by RAOs (see 1.3.6) or LRA or by a public official (in accordance with the provisions governing their activities) which must operate according to EU eIDAS2 Regulation and to the identification procedures applied by Intesi Group:

"In-person identification through the physical presence of the natural person or of an authorised representative of the legal person and a RAO

- In-person identification through the physical presence of the natural person or of an authorised representative of the legal person and an authorized RAO
- Identification through a Video meeting with a RAO (IDentify Web process).
- Identification through customers procedures with an LRA mandate.
- Identification through Corporate Identity[1].
- For the following identification processes, RAO validation is replaced with automatisms to validate the data source: Identification by means of a certificate of a qualified electronic signature.
- Identification by anti-money laundering regulation.
- Identification by notified digital identity schemes of level substantial or high (SPID/CIE for Italian citizens)

.

Intesi Group guarantees every identification procedure applied adhere to article 24 of the (EU) regulationeIDAS2 and to corresponding ETSI standards.

In order to proof identity, the subscriber shall present an identification document. For Italian citizens are allowed the following identification documents:

- identity card;
- passport;
- driving licence;

For subscriber with citizenship of an EU countries the following identification documents:

- Passport
- National identity card.

[1] Corporate IDentity must be intended as the personal authentication credentials of a corporate account holder.

For citizens with non-EU citizenship:

- Passport

For Citizens with residence in the United States are also allowed:

- National Government-issued Picture ID that asserts the holder's identity (e.g. National ID card, Passport, Global Entry Card, PIV card or comparable), two Non-National Government IDs, one of which shall be a photo ID (e.g. Driver's License)[2].

Any document presented shall bear an expiration date and must be unexpired.

When the identification process occurs using notified digital identity schemes (e.g. SPID or CIE), the acquisition of identity documents is replaced by the acquisition of SAML assertions (or equivalent) received from the identity providers.

When the identification process occurs by means of a certificate of a qualified electronic signature only the digitally signed document is acquired.

3.2.4 Identification Data Acquisition

To facilitate operators in the acquisition and verification of identification documents, Intesi Group has introduced a tool that, subject to obtaining the user's consent and displaying the privacy notice, uses artificial intelligence algorithms for the biometric verification of applicants, enabling the following:

1. The real-time capture of document images through live photo acquisition and the immediate verification of the authenticity of the acquired documents.
2. The verification of the match between the individual undergoing identification and the photograph extracted from the presented identity document.
3. The verification of the physical presence of the signatory during the image acquisition process and proof that they are in possession of the presented identity document.

The acquired data are processed by an automated validation service that, based on predefined thresholds, determines whether they can be accepted, must be rejected, or require re-assessment by an Intesi Group officer.

The RAO operator responsible for the process is informed of the outcome of the assessment and, in the event of a negative result, cannot proceed with the approval of the identification.

[2] Examples of acceptable identity documents can be found at: https://www.fedidcard.gov/document/acceptable-forms-id

3.2.5 Face-to-face identification and registration

This identification method is carried out by an operator qualified as an RAO and requires the physical presence of the applicant, who must identify themselves by presenting valid (non-expired) identity documents. These documents may be acquired manually by the RAO operator or through the tool defined in Section 3.2.4.

The identification documents shall contain:

- full name (including surname and given names),
- date of birth and place of birth,
- a serial number or other attributes which may be used to distinguish the person from others with the same name.

It is also permitted to check the identity of the applicant indirectly using means which provide equivalent assurance to physical presence (for example if the applicant already possesses a qualified certificate, which implies that the applicant has been already identified).

If the subscriber is requesting:

- a qualified certificate for electronic seal.
- a certificate, containing membership/affiliation with the company, with the approval of a third party.
- the inclusion of professional qualifications, role and organization.

They must present documentation to demonstrate the authorization to request the certificate or to use the qualifications required.

The RAO must verify the acquired documentation and, if deemed sufficient and/or found to be valid also on the basis of the automated assessments returned by the service described in Section 3.2.4, may proceed with the process:

- Registration of the subscriber's personal data through the Intesi Group RAO portal. A detailed list of the information entered is shown in section 4.2.1.
- Digitization of a copy of the identification documents presented.
- Printing a copy of the contract with terms and conditions.

The RAO must keep the signed copy which will deliver to Intesi Group and must sent the digital copies to Intesi Group through the RAO portal. Intesi Group will keep digital and paper copies according to the Italian regulation.

Intesi Group will keep digital and paper copies as required by current legislation.

The information recorded for the issuance of each certificate is set forth below:

- The identity of the RAO, LRA or TA.
- A signed declaration by the RAO or TA that he or she has verified the identity of the applicant.

- The date and time of the verification.
- A declaration of the identity signed by the applicant using a handwritten signature or appropriate electronic signature.

If the subscriber provides incomplete information, invalid or missing identification documents or does not sign a copy of the contract, the RAO will not be able to approve the issue of the signature or seal qualified certificate.

3.2.6 Identification through LRA process

Intesi Group can accept methods of identification different from those established by its own processes and adopted by customers authorized to perform RA activities after having carefully verified that the procedure is adequate and conforms to the procedure defined by EU eIDAS2 Regulation, by AgID and from this TSPPS.

3.2.7 Identification and registration through IDentify Web

This identification procedure is carried out by a RAO operator via videoconference with the certificate applicant. The videoconferencing system is provided by Intesi Group, which makes available to the applicant all the necessary instructions for access, the privacy notice, and the contractual documentation, for which consent is obtained by the operator during the video interview.

The subscriber shall own a device (PC, Smartphone or Tablet) equipped with a webcam and an audio system.

On the agreed date, the applicant is contacted by the RAO through the IDentify Web platform. The RAO conducts a guided video interview aimed at verifying the applicant's actual presence and the authenticity of the documents presented.

The RAO carrying out the identification verifies the identity of the Holder by checking one or more identification documents, which may have been previously acquired either through manual entry by the user or through the tool described in Section 3.2.4.

The RAO conducting the identification may reserve the right to consider a document presented by the Holder as inadmissible if they believe it does not meet the requirements of validity and authenticity and/or if the process described in Section 3.2.4 returns a negative assessment.

Furthermore, the RAO may not start or interrupt the identification process if the audio and video quality is poor or not adequate to meet the requirements of Article 32 paragraph 3, letter a) of the Italian "Codice Amministrazione Digitale" (Digital Administration Code).

At the starting of the video conference the operator asks to the user its decision about the privacy policy and the acceptance of the qualified digital signature service terms and conditions.

The user is informed by the RAO with proper documentation about the digital signature service and relating Terms and Conditions.

Without the acceptance, the video conference and the identification process are interrupted by the RAO.

At the end of the videoconference, if the RAO deems the recognition process successful, it will approve the certificate issuance otherwise it will reject the request informing the user.

The recording data, consisting of the audio-video file and metadata structured in electronic format, are stored securely according to the art. 32, paragraph 3, letter j) of the Italian "Codice Amministrazione Digitale" (Digital Administration Code).

3.2.8 Identification and registration through qualified signature verification

A user can be identified by means of a qualified digital signature verification applied on the certificate request form. For this kind of identification, a user must:

1. Fill the certificate request form with its personal data and digitally sign it using its qualified certificate.
2. Send it to Intesi Group by means of a RAO or through one of the Intesi Group's available encrypted communication channel.

On document reception, Intesi Group verifies the signature validity and verifies that the data contained into the qualified certificate used to sign the document match with the data contained into the certificate request form.

In case of positive verification, the certificate request will be accepted, and the certificate issuance will be approved. Otherwise, the certificate request will be reject informing the user with a suitable message this case Intesi Group will safely keep a copy of the request form for twenty years as required by the Italian legislation.

3.2.9 Identification by anti-money laundering regulation

The identification procedure is carried out by credit and financial institutions with the anti-money laundering regulation in application of Directive 815/2015 and Directive 843/2018.

With specific reference to Italy in accordance with Legislative Decree no. 231 of November 21, 2007, as amended by Legislative Decree no. 90 of May 25, 2017, and by the "*Disposizioni in materia di Adeguata Verifica della Clientela per il contrasto del riciclaggio e del finanziamento del terrorismo"* of July 30, 2019.

These parties must proof the identify in accordance with the above provisions. In any case, the identy proofing process adopted by the Banking/Financial Institution must be agreed in advance with Intesi Group QTSP.

The Banking/Financial Institution, acting as Local Registration Authority, undertakes to collect all the information and consents required by QTSP Intesi Group to issue qualified signature certificates.

In any case, the QTSP Intesi Group reserves the right to verify and adopt different processes than the above in accordance with the provisions and regulations governing such services.

3.2.10 Identification using SPID Identity

This identification process requires an authentication on the Intesi Group portal using a Level2 (LoA3 of the ISO/IEC DIS 29115) or Level 3 (LoA4 of the ISO/IEC DIS 29115) SPID electronic identity.

Access to the authentication could be gained by the subscriber through a unique and non-reusable link generated by an operator or an application integrated with Intesi Group services.

SPID is the Italian eID, the credential requested for this kind of must be at least level 2 corresponding to the Level of Assurance LoA3 of the ISO/IEC DIS 29115 standards.

Upon receiving the SAML authentication response from the SPID Identity Provider server, Intesi Group service checks:

1. the absence of error messages and the presence of authentication assertion;
2. the signature validity against the certificate contained in the metadata;
3. the presence of all data required to issue the certificate;
4. compliance with the "SPID Technical Rules".

If the response is valid, it is saved and stored as identification data, the user is registered and is directly redirected to the certificate issuance page.

The qualified certificate will contain the OID 1.3.76.16.5 and the following user notice: "Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity."

If the response is not valid, the user is showed a message with the error cause and, if it is possible, instructions on how to solve it.

3.2.11 Identification using CIE Identity

This mode of identification requires an authentication on the Intesi Group portal using the Electronic Identity Card (CIE) and CieID portal.

Access to the authentication page could be gained through a unique and non-reusable link generated by the portal itself at the request of an operator or an application integrated with Intesi Group services.

Upon receiving the SAML authentication response from the CieID server, Intesi Group service checks:

1. the absence of error messages and the presence of authentication assertion;
2. the answer signature validity against the certificate contained in the metadata;
3. the presence of all data required to issue the certificate;

If the response is valid, it is saved and retained as identification data, the user is registered, and invited to proceed with the certificate generation process.

If the response is not valid, the user is shown a message explaining the reason for the error and providing any guidance on how to resolve it.

The same process generally applies to digital identity schemes notified at the EU level, subject to the technical specifications of the Identity Provider delivering the service within a specific scheme and Member State.

3.3 Initial Identity Proofing – eIDAS2

Intesi Group acts as an Identity Proofing Service Provider (IPSP), delivering identity verification services as a component of the qualified trust service for the issuance of digital certificates.

All practices, technical and organizational measures, and operational procedures relating to the identity verification of subjects (natural and legal persons) are described in a separate document entitled the "Identity Proofing Service Practice Statement" (IPSPS) [3], which is publicly available and downloadable from the official Intesi Group website at the following URL: https://www.intesigroup.com/it/qtsp/documenti/

The Identity Proofing service, named **IG Persona**, is designed to ensure the *Extended Level of Identity Proofing (LoIP)*, in compliance with article 24 of the Regulation (EU) 2024/1183 (eIDAS 2) and the ETSI TS 119 461 standards.

These identification processes will be introduced from 22 May 2026 and will become the sole methods used for identity verification from 19 August 2027.

3.3.1 Identification Methods and Associated OIDs

The policies applied to each identification method adopted by Intesi Group are identified by the following Object Identifiers (OIDs), as detailed in the Identity Proofing Service Practice Statement (IPSPS) [3].

Identification Method Description	Intesi OID
Attended identity proofing with hybrid manual and automated operation (ref. ETSI TS 119 461, clause 9.2.1.3).	1.3.6.1.4.1.48990.1.1.9.1
Unattended remote identity proofing with hybrid manual and automated operation (ref. ETSI TS 119 461, clause 9.2.3.3)	1.3.6.1.4.1.48990.1.1.9.2
Identity proofing by authentication using eID means with "High" level of assurance (e.g. SPID and Carta d'Identità Elettronica Level 3) (ref. ETSI TS 119 461, clause 9.2.4).	1.3.6.1.4.1.48990.1.1.9.3
Identity proofing using digital signature with certificate (Ref. ETSI TS 119 461 par. 9.2.5).	1.3.6.1.4.1.48990.1.1.9.4
Identity proofing of legal person (Ref. ETSI TS 119 461 par. 9.3).	1.3.6.1.4.1.48990.1.1.9.5
Identity proofing of natural person representing legal person (Ref. ETSI TS 119 461 par. 9.4).	1.3.6.1.4.1.48990.1.1.9.6

3.3.2 Verification Requirements and Procedures

For details regarding the following phases of the identity verification process, reference is made to the corresponding sections of the IPSPS:

- **Preliminary phase:** applicant information and consent collection.
- **Data collection:** types of accepted identity evidence (physical documents, notified eIDs, qualified certificates) and acquisition methods.
- **Validation:** document security checks, authenticity verification, liveness detection, video identification, and anti-fraud controls.

- **Binding to the Applicant:** procedures to establish a reliable link between the verified identity and the applicant.
- **Result issuance:** generation of the reliability score and final approval of the identification process.

3.3.3 Evidence Management and Retention

The evidence collected during the identity verification process — including, but not limited to, extracted data, multimedia recordings, and operator logs — is stored using Intesi Group archive that grants appropriate technical and organizational measures to ensure its security, integrity, authenticity, and immutability over time.

In compliance with the applicable regulations governing qualified trust services, such evidence is retained for a period of 20 years from the completion of the identification process, after which the data is deleted.

3.4 Identification and Authentication for Re-Key Requests

Re-key requests are not available for any certificate issued by Intesi Group CA.

3.5 Identification and Authentication for Revocation Requests

.

A user can request certificate suspension or revocation into time4mind portal after having logged in using username and password set during the first registration.

If the user does not remember or has lost the authentication information, he can submit a revocation request to an enabled authorized RAO or TA, or to the Intesi Group support as described in paragraph 4.9.

The revocation of TSU certificate shall be authorized by the Security Officer according to the procedure described in 4.9.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate request

Request for a qualified certificate issued to a natural person may be requested by a subscriber (see 1.3.4) applying to the QTSP or to an authorized LRA. If requested by the subscriber or third party, the qualified electronic signature certificate may contain the following information: subscriber qualifications (e.g. work title, professional orders or colleges membership etc.) and powers of representation.

Request for a qualified certificate issued to a legal person may be requested by a natural person who is authorized to represent the legal person by submitting the application accompanied by appropriate documentation to the QTSP or to an authorized LRA.

Finally, the certificate for time stamps (TSU) can only be requested by Intesi Group internal staff as part of the key ceremony of the keys.

4.1.2 Enrolment process and responsibilities

The registration process must be carried out after the identification process (see par.3) and includes the following different steps:

- the Subscriber shall:
  1. reads and accepts the privacy policy;
  2. provides the required data for registration and presents the require documentation for the identity proofing;
  3. signs a copy of the contract with Terms and Conditions;
  4. reads and accepts this TSPPS;
  5. Issues certificate following the process described into this QTSP;
- Where required, the RAO must:
  1. Identify the user as described in paragraph 3.2 and 3.3;
  2. Approve the issuance of the signature certificate or the seal;
  3. Where applicable, send a copy of the collected documents to the QTSP.
- the QTSP shall:
  1. issues qualified certificate or seal;
  2. archives the identification data and all the information collected during the registration process for the issuance of certificates;
  3. disseminates information on the certificates and seals status;

As indicated in the previous paragraphs the registration functions can also be performed by third parties (LRA) based on agreements with Intesi Group.

4.2 Application processing

The procedure for issuing certificates to natural and legal person takes place through the following steps:

1. Subscriber is identified according to one of the processes described in section 3.2 and 3.3
2. QTSP validates user data and documentation and notifies the user (e.g., through e-mail) of the approval to issue the certificate.
3. Subscriber issues certificate as described 4.3 within 7 days. If the issuance takes longer, the user shall contact Intesi Group support team

The procedure for issuing qualified certificates can only be executed by the subscriber or by the RAO in the presence of the holder user.

The procedure for issuing TSA certificates is described in the internal procedures of Intesi Group.

4.2.1 Subject information required

To request a qualified certificate the subject or the subscriber must provide the following mandatory information:

- Name and surname;
- Birth date, birth city, birth state and birth country;
- Country of residence;
- mobile phone number;
- email address;
- Tax Identification or equivalent;

If the subscriber represents a legal person must also provide

- organization name;
- organization tax code;
- organization address (country, state, city, address);
- organization email and organization phone number;
- information aimed to demonstrate power of attorney.

4.2.2 Registration and authentication

The registration and validation of the data are described in the 'Identity Proofing Service Practice Statement' (IPSPS) [3], paragraphs 3.2, 3.3 and 3.4.

4.2.2.1 Subject authentication credentials

To issue a certificate, the holder must authenticate to the Intesi Group's user portal (reachable at the URL https://user.time4mind.com) or must authenticate, to the IG You Mobile App using its basic credential.

The registration request to the Time4Mind portal is notified to the user through an e-mail containing a link that the user must click to confirm the registration request.

The basic credentials are not enough to start the certificate issuance process because for this it is necessary that the user also insert the security code received at the end of the registration.

4.2.2.2 RAO authentication credentials

Every RAO must have basic credentials enabled to access the PkRA reachable at the url https://pkra.time4mind.com portal and must be provided with remote signing credentials to perform the registration procedure.

Login credentials may already be in the user's possession or they may be generated automatically during the registration process. In the latter case, when the user first logs in, the system will ask the user to set a new password.

The generation of RAOs credentials is carried out by allowed Intesi Group staff and is executed following procedures defined by Intesi Group.

4.2.2.3 LRA authentication credentials

Intesi Group's customers authorized to do LRA Identification by means of their processes can do the registration using webservices exposed by the Time4Mind portal.

Communication between LRA client and Intesi Group server is protected by a secure TLS channel and requires: a certificate authentication to get access to services.

Authentication certificates are generated and distributed by Intesi Group staff following the procedures for the assignment of LRAs defined by Intesi Group.

4.3 Certificate Issuance

4.3.1 Qualified certificate issuance for remote signature

Users requesting remote signature must verify to have the required tools to generate OTP tokens. In particular:

- Users who use SMS tokens must ensure to have the mobile device associated with the phone number provided during the identification.
- Users who use physical OTP tokens must be sure to have the device provided by the RAO upon registration.
- Users who use OTP tokens generated by the Mobile IG You App, before starting the certificate issuance procedure must be sure that the App is installed on their mobile device (during installation they receive instruction how to install it). The App is freely downloadable from the Google Play Store for Android devices and from the Apple App Store for iOS devices.

The certificate issuance procedure can be performed through the Intesi Group Time4Mind portal or directly from the IG You mobile app.

To start the certificate issuance procedure through the user portal of Time4Mind the user must log in to the portal using its basic credentials and select the menu item "Enroll Certificate".

Then, the user must select the credential to be issued and enter the "security code" received via e-mail to complete the authentication phase. The e-mail address or telephone number used for sending security codes are those verified during the identification of the subject.

Alternatively, the user can skip these steps by clicking on the link received with the confirmation email. In both cases, if the authentication completes successfully, the procedure to generate the signing credential can be started. At this point, depending on the type of certificate to be issued and the type of token associated, the procedure will continue in different ways.

For automatic signature certificates it is necessary to define a PIN that, combined with the alias automatically generated and displayed to the user, will constitute the authentication credential.

For remote signature certificates using OTP SMS, in addition to the PIN is required to enter the OTP that the procedure automatically send to the phone number provided during the identification. In this case the combination of alias, PIN and OTP SMS will be the credentials to unlock the signing credential.

For remote signature certificates using physical OTP, in addition to the PIN is required to enter the OTP generated by the device provided by the RAO. In this case the combination of alias, PIN and OTP are the credentials to unlock the signing credential.

Finally, for remote signature certificates coupled with OTP tokens generated by App IG You for which the procedure, once started, will continue within the App after logging in using a username and password (see 4.2.2.1) and using the security code sent by email. The App will require only the definition of a PIN and then autonomously and in safety mode will start the certificate issuance procedure by communicating with the Time4Mind portal.

Upon receipt of the information, the Time4Mind server starts the key pair generation process on the QSCD device and receive a certificate request in PKCS#10 format in response. This request is then sent to the internal certificate generation system (PKI) which will validate the request and will issue an X.509 certificate.

The certificate generated will be returned to the caller who will save it on the QSCD device coupled with the private key completing the signing credential.

The certificate issuance process is completed with a message sent by email to the email address verified during identification confirming successful issuance.

Intesi Group verifies the accuracy and validity of all necessary data for the issuance of a qualified certificate, according to EU eIDAS2 Regulation and corresponding ETSI standards. Intesi Group will either issue the subscriber's certificate upon successful completion of the process above, or will inform the subscriber about any problems or inconsistencies.

4.3.1.1 Shot-term certificates

For short-term cloud-based certificates, the identification process, the credential issuance and the document signature take place at the same time. The credential is issued, and a document is signed only after the user inserts an OTP code received via SMS or email on the telephone number provided during identification.

4.3.2 Qualified certificate issuance on physical QSCD device

For qualified certificates issued on physical device (smartcard or USB token), Intesi Group will supply directly or through selected suppliers, only devices that are approved and published on the Compilation of Member States QSCDs list, available here:

https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD.

The QSCD customization process is carried out using software developed by Intesi Group includes a check on the serial code to verify its presence in QSCD certified devices list. If the device is not included in these lists, the personalization process is interrupted.

Users requesting qualified certificate on a QSCD device (smartcard or USB token) must first install on their PC the required software to handle the device and issue the qualified certificate. Information on where to

download the software package and the installation instructions will be provided by the QTSP or RAO or TA at the end of the identification process. The procedure for customizing the signature token and issuing the certificate is done through the following steps:

1. The user must insert the QSCD device into the smartcard reader or in the USB port of its PC and then start the IG Desk software to manage the QSCD device.
2. The user must then start the personalization procedure of his / her signature token by selecting the appropriate menu. At the beginning of the procedure the user will be asked to enter the authentication credentials and the "security code", received by SMS, that he / she has received after the identification procedure.
3. The user authentication starts the key pair generation, inside the QSCD device, and the PkCS#10 certificate request generation. The PkCS#10 certificate request and the authentication credentials are sent to the QTSP through a secure channel protected by the TLS (Transport Layer Security) protocol.
4. Upon receipt of the request, Intesi Group will verify the accuracy and validity of all the necessary data for the issuance of a qualified certificate according to the (EU) eIDAS2 Regulation and the corresponding ETSI standards.
5. If the verification process successfully completes, Intesi Group will issue the certificate that will return to the caller. In case of unsuccessfully verification Intesi Group will return an error message containing problems or inconsistencies that have caused the rejection.
6. Upon receipt of the certificate, the client software will install the certificate into the signature token completing the customization procedure.

The certificate issuance process is completed with a message sent by email to the email address verified during identification confirming successful issuance.

4.3.3 TSA certificate issuance

The certificate request is executed manually by a TSP operators after informing the TSP Operation Officer who supervises the whole activity. The process is carried out as follows:

- TSP operator using the timestamping software, generates the key pair on the HSM partition dedicated to the time stamp keys and generates the certificate request in PKCS # 10 format.
- TSP operator proceeds with the issuance of the certificate operating on the Intesi Group PKI administration panel.
- TSP operator install the certificate on the HSM and activates the time stamp service.

4.3.4 Test certificate issuance

Upon TSP Officer approval, Intesi Group can issue qualified certificates for test purposes. This kind of certificates are identified by specific certificate policy OID (see paragraph 1.4) and the user notice: "Le firme apposte con questo certificato sono valide solamente a scopo di test. Signatures created with this certificate are only valid for testing."

In addition, the Common Name field of the subjectDistinguishedName is filled with string “[TEST] {NAME} {SURNAME} for testing purpose only” that helps to quickly identify signatures applied with test certificates.

Every test certificate should be revoked at the end of the testing session.

4.4 Certificate Acceptance

4.4.1 Certificate acceptance

4.4.1.1 Subscriber Certificate acceptance

On receiving a certificate, the subscriber is committed to check its contents. If the certificate has any faults that cannot be accepted by the subscriber, the subscriber must inform Intesi Group without any delay. Intesi Group will then revoke the certificate and take the appropriate measures to reissue a new certificate.

If a certificate is not rejected within 7 days of the reception of the certificate, the certificate is considered accepted.

4.4.1.2 TSA Certificate acceptance

In case of erroneous certificates, the TSA Officer will request the security officer authorization to revoke the certificate according to the described procedure in 4.8.

4.4.2 Publication of the certificate by the QTSP

Qualified certificates are not published and are stored into the QTSP database.

4.4.3 Notification of Certificate issuance by the QTSP to other entities

An e-mail containing a confirmation e-mail message is sent to the subscriber. No notification is sent for TSA certificates.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

4.5.1.1 Keys and certificates of digital signature and seal

The holder must:

- be the sole user of the private key.
- Use the private key only to generate digital signatures or seals depending on the associated certificate. It is not possible to use the keys for other purposes (e.g. data encryption).
- maintain exclusively the knowledge of the authentication data (PIN, PUK and/or OTP), keeping them with the maximum diligence.
- keep the OTP device with the maximum diligence.
- use credentials respecting any user notice contained in the certificate.
- refrain from using improper or fraudulent keys and certificates in its possession.
- inform Intesi Group of any changes to the data not included in the certificate but communicated during the registration process.

- request the revocation of the certificate if there is reason to believe that the authentication data (e.g. PIN code) have been compromised.
- request the revocation of the certificate if there is reason to believe that the private key has been compromised.
- ask for the revocation of the certificate if the data contained in it are changed or incorrect.

4.5.1.2 Keys and certificates for TSU

TSU keys and certificates are generated and issued internally by authorized personnel and following Intesi Group's internal procedures. The keys and certificates are used only for generating time stamps (see rfc3161). Each private key is used for a maximum of 3 months.

4.5.2 Relying Party public key and Certificate usage

Who relies on the information contained in the certificates (see 1.3.7) must verify that the certificate has not been expired, suspended or revoked. The validity can be verified using the CRLs or the OCSP service referenced in the CRLDistributionPoints and AuthorityInformationAccess extensions of the certificate.

The verification must consider the certificate status at the relevant date and time based on the context. The current date and time, if there is no way of knowing when the signature was generated, or the date and time when the signature was generated if is demonstrable by a time stamp included in the signed document.

In addition, any user notice restriction should be checked.

Users can avoid the above checks only in the case of a "verified signature" certificate, according to the AgID Determination n. 63/2014; this kind of certificates can be detected analyzing the OID contained into CertificatePolicies extension. For more details on users' obligations, please refer to par 7.3.

4.5.3 User notice

Qualified certificates for server-side signature contain the user limit set by the Italian Conformity Assessment Body – Agid - as additional Certificate Policy:

Il presente certificato è valido solo per firme apposte con procedura automatica.	The certificate may only be used for unattended/automatic digital signature.

Conforming to the Italian regulation, the Subscriber can also request to the Certification Authority the inclusion into the certificate of one of the following user notices:

I titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato.	The certificate holder must use the certificate only for the purposes for which it is issued.
L'utilizzo del certificato è limitato ai rapporti con (indicare il soggetto).	The certificate may be used only for relations with the (declare the subject).

Furthermore, the Subscriber can also request the inclusion of custom user notice which must be evaluated by the CA.

The subscriber can also request limitation on the value of transaction for which a certificate can be used and is responsible to verify the compliance with the limits of use inserted into the certificate. The QTSP is not responsible for damage caused using a certificate that does not comply with the user notice contained into the certificate itself.

4.6 Certificate Renewal

The renewal of a certificate can only be carried out by the Holder and only if:

- The certificate is valid, meaning it has not expired, been revoked, or suspended.
- The personal data contained in the certificate have not changed.

The renewal procedure can be initiated only within thirty days prior to the certificate's expiration and always involves the generation of a new key pair.

The renewal procedure for a TSU certificate is carried out every three months by a TSP Operator following Intesi Group's internal procedures.

4.6.1 Procedure to process renewal request

Subjectcan start the procedure from its IG You Mobile App or from the Intesi Group portal and only after having:

1. done a successfully login using basic authentication credentials.
2. Signed with the expiring certificate the contract with terms and conditions.
3. Inserted certificate access PIN.

After obtaining this information, the QTSP generates a new key pair and a new certificate using the same procedure used for the first generation (see 4.3).

The TSU certificate renewal procedure is executed by two TSP operators who can generate a new key pair and issue a new certificate. The renewal of TSU keys is carried out following a specific internal procedure and is recorded on a KeyCeremony document which must be approved by the TSP Officer and which is kept for a period of 20 years.

4.6.2 Notification to the subscriber

The notifications sent to the holder are:

- Thirty days before the expiration, the server sends to the subject an e-mail containing a reminder about the certificate expiration and the instructions on how to proceed with the certificate renewal.
- The certificate issuance process is completed with a message sent by email to the email address verified during identification confirming successful issuance.

4.6.3 Certificate acceptance

Refer to section 4.4.1.

4.6.4 Publication of the certificate by the CA

Refer to section 4.4.2.

4.6.5 Notification of Certificate issuance by the QTSP to other entities

Refer to section 4.4.3.

4.7 Certificate Re-key

Certificate re-key is not allowed by Intesi Group qualified CA.

4.8 Certificate Modification

The certificate modification is not allowed by Intesi Group qualified CA. To modify a certificate a user must revoke the certificate to be modified and issue a new certificate following the procedure described in section 4.9 and 4.3.

4.9 Certificate Revocation and suspension

4.9.1 Circumstances for revocation

The circumstances to request a certificate revocation are those provided by the regulations and by the TSPP. A certificate shall be revoked when the binding between the Subject (holder) and the Subject's Public Key defined within the certificate is no longer considered valid. Examples of circumstances that invalidate the binding include, but are not limited to:

- Identifying information or affiliation components of any names in the certificate becomes invalid.
- Subject can be shown to have violated the stipulation of its respective Subscriber Agreement, or the stipulations of this TSPPS.
- Subscriber or another authorized agent asks for his/her certificate to be revoked.
- Reports from authorities.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on a CRL. Revoked certificates are published on all new publications of the certificate status information.

After certificate revocation, the key pair can no longer be used to generate signatures or seals and can no longer be used to issue a new certificate or seal.

If a private key used to approve requests for one or more certificates may have been compromised, all certificates authorized since the date of actual or suspected compromise and directly or indirectly chaining back to that private key will be either revoked or be verified to be appropriately issued.

The revocation operation is unrecoverable.

4.9.2 Who can request revocation

The certificate may be revoked on request of:

1. Certificate holder.
2. Third party, when present.
3. QTSP.

For certificates that bind an organizational affiliation, Intesi Group accepts revocation requests from the designated organization's Contact Point. The organization shall inform Intesi Group of any changes in the subscriber affiliation. If the affiliated organization no longer authorizes the affiliation of a subject (holder), Intesi Group will revoke any certificate issued to that subject containing the organization affiliation.

For TSU certificates, revocation can be required by TSP Operators after having informed and obtained approval from the TSP Security Officer.

4.9.3 Procedure for revocation request

The form and/or procedure to be used for applying for the suspension, unsuspension or revocation of a certificate can be obtained by the subject:

- from the Time4Mind user portal;
- making a request to a RAO;
- making a request to Intesi Group's customer care;

Applications and reports relating to a revocation are processed on receipt, are authenticated and are confirmed through the following processes:

4.9.3.1 Revocation with Time4Mind portal

To revoke its certificates through the time4mind portal (https://user.time4mind.com) the holder must:

1. Successfully login to the Time4Mind user portal;
2. search for the certificate to be revoked from those listed by the application using the "Credential" menu;
3. invoke the "revocation" function and confirm the request.

The request is immediately taken in charge and executed as soon as possible. The result of the operation is shown on the user screen and confirmed with an email sent to the holder and, when applicable, to the third party.

4.9.3.2 Revocation by means of Intesi Group RAO

The Revocation of a certificate can be made by any RAO operator using the PkRA RAO in response to a request from:

- Certificate holder;
- Third party, when applicable;
- QTSP;

The holders and third parties who wish to request a certificate revocation to a RAO, must present the revocation form, downloadable from the Time4Mind portal, filled in all its parts and a copy of the identification document.

Using the supplied information, the RAO, by means of the PkRA web portal, can:

1. search the user;
2. Compare the data provided with those recorded in the portal to authenticate the applicant. if the RAO consider that the information is wrong or incomplete, it will proceed with the certificate suspension waiting for the applicant providing clarification or additional information.;
3. request the certificate revocation or the certificate suspension.

The request is immediately taken in charge and executed as soon as possible. The result of the operation is shown on the RAO screen and confirmed with an email sent to the subject.

4.9.3.3 Customer care revocation

Only in the event of unavailability of Intesi Group's revocation services can users and RAOs request a revocation through Intesi Group's customer support by opening a ticket at:

https://support.intesigroup.com

When a revocation request is submitted by a RAO, the ticket must be opened within eight hours from the moment the revocation request is received from the subject.

Each request must include a completed revocation form, which must also contain the revocation code, or a digital copy of the identification document. If the user is unable to provide either of these documents, the certificate will only be suspended. The user then has ten days to proceed with the revocation or reactivation of the certificate, after which, if no action has been taken, the certificate will be automatically reactivated.

Upon receiving the email, an Intesi Group operator takes charge of the request and verifies the accuracy of the information provided. If all checks are positive, the RAO proceeds with either the revocation or the suspension of the certificate.

The outcome of the operation is confirmed by an email sent to the Subject.

4.9.3.4 TSA certificate revocation

According to clause 4.8 of the QTSP policy, the certificate revocation is executed by TSP Operator with the approval of the Security Officer following TSP Internal Procedure.

After the certificate revocation, the TSP operator will proceed with the deletion of the related private keys from the HSM.

4.9.4 Revocation request grace period

Intesi Group performs revocation on a best effort basis, to ensure that the time needed to process the revocation request and to publish the revocation status (updated CRL) is as reduced as possible.

4.9.5 Time within which QTSP must process the revocation request

When the QTSP receives a revocation request, it tries to immediately executes the operation. Intesi Group shall process revocation requests within 24 hours of the receipt of the request. If the operation is successfully executed, the revoked certificate is inserted in the CRL within 6 hours of the revocation and in any case not later than 24 hours after the operation. If the revocation fails the status of the certificate is not changed and the subject , is informed by an email.

4.9.6 Revocation checking requirement for Relying Parties

Refer to section 4.5.2.

4.9.7 CRL issuance frequency / OCSP response validity period

4.9.7.1 CRLs

The CRL is re-generated and re-published every 6 hours, even in the absence of new revocations. In some circumstances, the QTSP can force a new CRL issuance before of the 6h.

4.9.7.2 OCSP

OCSP service is available for certificate status validation. The fields “this update” and “next update” reflect the validity period of an OCSP (see section 7 of the TSPPS).

4.9.8 Maximum latency for CRLs

The time between the request for revocation or suspension and the confirmation with the issuance of a new CRL is at maximum six hours.

4.9.9 On-line revocation status checking availability

The QTSP makes available Certificate status checking services including CRLs and OCSP. See section 4.10 of this document.

4.9.10 Other forms of revocation advertisements available

Not available.

4.9.11 Special requirements regarding key compromise

Not available.

4.9.12 Circumstances for suspension

The certificate suspension can be executed under these circumstances:

1. QTSP receive a revocation request without necessary information to authenticate the requester.

2. QTSP, owner, subscriber or certification authority acquire elements of doubt about the validity of the certificate;
3. there are doubts about the safety of the key storage device or the authentication system;
4. is required an interruption of the validity of the certificate.

The suspension for the TSU certificate is not available.

4.9.13 Who can request suspension

Who can request a certificate suspension is listed in paragraph 4.9.2 of this TSPPS.

4.9.14 Procedure for suspension and un-suspension requests

Tools and procedures available are the same used to invoke the revocation of certificates (see paragraph 4.9.3).

4.9.15 Limits on suspension period

The suspension has a period of ten days after that the certificate can be automatically revoked or un-suspended depending on the customer configuration.

The suspension is maintained for a period of at least thirty days, after which the certificate is automatically reactivated. Intesi Group can extend the suspension period at the request of the authorities, the supervisory body or if it considers it necessary for matters of investigation.

4.10 Certificate Status Service

The status of the qualified certificates is made available through the publication of CRLs, in conformance to RFC 5280, via HTTP protocol [RFC7230] on the server **crl.time4mind.com**.

The status of the certificate is also available through a status checking service based on OCSP (On-line Certificate Status Protocol) in compliance with the specification [RFC2560].

The revocation services addresses are inserted into the certificates, the CRL address is inserted in the CRLDistributionPoints extension, and the OCSP server address is inserted in the AuthorityInformationAccess extension. The Certificate status services are public.

4.10.1 Service Availability

Access to the CRL and OCSP service is continuously available (24 x 7).

4.11 Timestamp Verification Services

Timestamps issued by Intesi Group are qualified in accordance with the eIDAS Regulation (EU Regulation No. 910/2014) and comply with the updated eIDAS2 framework.

They fully meet the technical specifications defined by RFC 3161 and the ETSI EN 319 422 standard, and can therefore be verified:

- Using the tools provided by Intesi Group, such as PkBox;
- Or through any other verifier that supports the verification of qualified timestamps according to EU regulations.

4.12 End of Subscription

The contract between the QTSP and the holder ends when the certificate expires or is revoked, unless there are different conditions that may be stipulated in contracts signed with customers.

4.13 Key Escrow and Recovery

The key recovery is available for CA and TSU keys in the case of unintentional cancellation or HSM fault. To allow key recovery, the QTSP keeps a backup of CA and TSU key pair and recovery is performed according to the HSM procedures and under dual operator control.

5 FACILITIES, MANAGEMENT, AND OPERATIONAL CONTROLS

The management, operational, procedural, personnel and physical (non-technical security) controls that are used by Intesi Group S.p.A. with regards to its qualified service is compliant with the technical standards EN 319 411-1 for non-qualified certificate issuing, EN 319 411-2 for qualified certificate issuing EN 319 421 for timestamp issuing and Intesi Group ISO/IEC 27001 certified Information Security Management System.

Intesi Group information security policy as well as documentation on security controls and operating procedures are available in the security plan (Piano della Sicurezza) and other reserved documents that are available only to authorized Intesi Group personnel, to auditors and to the Italian Supervisory Body.

5.1 Physical security

To ensure physical security, all systems used for QTSP activities are physically separated from other Intesi Group systems, so that access is granted only to personnel with the System Administrator role and in possession of a badge authorized to open the rack.

Private keys used for issuing certificates or signing certificate status responses are not vulnerable to physical penetration (HSM and server anti tampering). These keys are stored in tamper-resistant secure signature creation devices which are confirmed to fulfill the requirements of the EU eIDAS2 Regulation and corresponding ETSI standards.

The devices are protected from unauthorized access while installed and activated. Physical access controls are implemented to reduce the risk of device tampering even when is not installed and activated.

Regular security checks are made to ensure that all these controls function properly. Access to any physical area where information or equipment sensitive to QTSP operations is located is restricted and monitored by the integrated alarm system.

All computer systems used for the provision of the qualified trust services herein described are housed in the Intesi Group data centers that guarantee:

- a **physical access control** system, so that access to the building is only possible to authorized personnel;
- access to the TSP services is only possible for authorized personnel holding a personal badge and the corresponding PIN;
- From a video surveillance system that allows only authorized personnel to verify the integrity of QTSP devices.
- a **fire protection system** including **smoke detection** (VEWASD) **and** dedicated extinguishing system;
- a **power supply system** fully redundant at all levels (transformers, power centers, generators, UPS's, distribution panels, etc.)
- an **air conditioning** system (HVAC) which guarantees optimal working conditions;
- redundant **Internet connectivity**, with a capacity of at least twice the minimum necessary.

5.2 Procedural controls

Intesi Group S.p.A. carries out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. This risk analysis performed with the full support and collaboration of all component services providers and is regularly reviewed and revised if necessary. This risk analysis is part of the reserved documentation. Appropriate systems, infrastructures and measures for quality and information security management are implemented and maintained always. Any changes that would impact on the level of security provided must be approved by the Security Officer.

Development and testing facilities are physically separated from operational facilities. Procedures exist and are followed for reporting software malfunctions. Procedures exist and are followed to ensure that faults are reported and corrective actions are executed. Users of QTSP systems are required to note and report observed or suspected security weaknesses and threats to systems or services. System documentation is protected from unauthorized access.

Capacity demands are monitored and projections of future capacity requirements are made to ensure that adequate processing power and storage are always available.

Detection and prevention controls to protect against viruses and malicious software and appropriate user awareness procedures are implemented.

A formal reporting procedure exists and is followed, together with an incident response procedure, setting out the action to be taken on receipt of an incident report. Incident management responsibilities and procedures exist and are followed to ensure a quick, effective, and orderly response to security incidents.

Operational procedures are documented under the company's Quality Management System, certified in accordance with the ISO 9001 standard and into the QTSP operative procedures.

5.3 Personnel security controls

All members of the personnel staff that involved for the provision of the trust services are either employees of Intesi Group S.p.A. or authorized and qualified personnel. All members are subject to personnel and management practices that Intesi Group follows to provide reasonable assurance of the trustworthiness and competence of the staff members within the fields of electronic signature-related technologies and time stamping related technologies.

Personnel involved in the service development and management time stamp service have been adequately trained on the procedures and tools to be used during the various operational phases.

All personnel must have proper knowledge and experience related to QTSP operations and must have demonstrated security consciousness and awareness regarding its duties at Intesi Group. Periodic reviews occur to verify the continued trustworthiness of all personnel.

No unauthorized users have access to systems storing sensitive data. All systems storing such data are located inside a protected area. In addition, access to rooms inside the protected area is controlled by an access control system; access to systems is permitted to authorized persons only.

Employees sign a confidentiality (nondisclosure) agreement as part of their initial terms and conditions of employment. All employees of the organization and, where relevant, third-party users receive appropriate training in organizational policies and procedures.

A formal disciplinary process exists and is followed for employees who have violated organizational security policies and procedures. Intesi Group's policies and procedures specify the sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems.

Appropriate and timely actions are taken when an employee is terminated so that controls and security are not impaired by such an occurrence.

The trusted roles assigned to personnel are defined in accordance with the ETSI EN 319 401 and are:

1. TSP Officer: responsible for the information security and the compliance with the company's security policy.
2. TSP Operation Officer: responsible for the certification and validation service.
3. System Administrator: administers the systems of the TSP service.
4. System Operation Officer: responsible for technical and logistic services.
5. System Operator: reporting to the System Operation Officer manages the operation of the TSP systems.
6. System Auditor: verifies the compliance of the TSP services with regulatory requirements and standards.
7. Registration Officer - individual authorized to request or approve certificates or certificate revocations. These individuals do not hold any other roles.

All staff has received a mandate through a letter of engagement.

5.4 Audit logging procedures

5.4.1 Type of events recorded

The main events relevant to the certification service operations are registered in electronic form. The events logged are:

- All events relating to the life-cycle of CA keys;
- All events relating to the identification operation.
- Logging systems events related to certificate life cycle operations including but not limited to:
    - Subject key generation;
    - Certificate issuance;
    - Certificate revocation;
    - Certificate suspension;
    - Publishing of a CRL;
- All other certification services are equipped with event logging systems that record events related to any operation performed.
- Physical access to the data center.
- Physical access to the QTSP server area.
- Logical access to all TSP systems.
- Events related to the certificate life cycle.
- Events related to clock synchronization.
- Events related to the release and updating of software.

For each event, information about the type, date and time of occurrence is also logged. The time source used is the system clock that is kept aligned by a NTP service.
No single person may modify or even delete audit trails or system log files, and access to them is strictly restricted. These provisions are implemented using the features of a secure B1 operating system requiring the simultaneous login of two persons.

5.4.2 Frequency of processing log

Audit logs are processed continuously and/or following any alarm or anomalous event. Audit logs are archived daily.

5.4.3 Retention period for audit log

Log files are kept for 20 years, after which the data is deleted.

5.4.4 Protection of audit log

The archive system has a daemon that checks the consistency and the immutability of the stored log files. In case of inconsistencies fires an alarm to the monitoring system.

The access to the log can Intesi Groups personnel with role of “System Administrators” and “System Auditors”.

5.4.5 Audit log backup procedures

Log files are backed up according to internal procedures.

5.4.6 Audit collection system (internal vs. external)

Audit systems are an integral part of the CA.

5.4.7 Notification to event-causing subject

If required, Intesi Group notifies the originator of the audit event.

5.4.8 Vulnerability assessment

Vulnerability assessment related to the audit log systems is part of the risk analysis carried out by Intesi Group S.p.A. and available as a separate internal and confidential document.

5.5 Record Archival

5.5.1 Type of records archived

The TSP keeps the following information related to the certificate issuing and management processes:

- Event logging;
- All the logging files of the systems involved in the QTSP service;
- Identifications data, digital copy of identification document and contract approval.

The archive system has a daemon that checks the consistency and the immutability of the stored log files. In case of inconsistencies fires an alarm to the monitoring system.

The access to the log can Intesi Groups personnel with role of “System Administrators” and “System Auditors”.

5.5.2 Retention period for audit log

Archived records are kept for 20 years, after which the data is deleted.

5.5.3 Protection of archive

The archive system has a daemon that checks the consistency and the immutability of the stored information. In case of inconsistencies fires an alarm to the monitoring system so that a "System Administrator" is immediately informed and can treat the problem according with Intesi Group internal procedures.

The access to the log can Intesi Groups personnel with role of “System Administrators” and “System Auditors”.

5.5.4 Archive backup procedures

Ref. Paragraph 5.5.3.

5.5.5 Requirements for timestamping of records

Intesi Group ensures that the precise time of archiving all events, records and documents listed in section 5.4 and 5.5 is recorded obtained through NTP synchronization of all systems. NTP service grants the time accuracy within a few milliseconds of Coordinated Universal Time.

5.5.6 Procedure to obtain and verify archive information

Archives are only accessible to the Intesi Group's authorized personnel as described in internal documents. Records are retained only in electronic format.

The Certificate holder and third party may access to records and other information related to the certificates by contacting Intesi Group writing an e-mail to the e-mail address defined in the paragraph 1.5.

5.6 Renewal of CA Key

The Key ceremony procedure in force shall be applied.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

The applicable and appropriate incident and/or compromise reporting and handling procedures, disaster recovery procedures and Business Continuity Plan have been established and are available as a separate internal document.

All such procedures are compliant against ISO/IEC 27001 standard. All incident and/or compromise events are documented, and any associated records are archived as described in section 5.5 of the TSPPS.

5.7.2 Computing resources, software, and/or data are corrupted

Intesi Group S.p.A. establishes the necessary measures to ensure full and highly automated recovery of the certification services in case of a disaster, corrupted servers, software or data. Any such measures are compliant against the ISO/IEC 27001 procedure.

Disaster recovery resources are established at sufficient distance from the original resources to avoid that a disaster would corrupt resources at both sites. Sufficiently fast communications are established between original and remote sites to ensure the alignment and data integrity. Secured communications infrastructures are established from both sites to the RAs, the Internet, the certificate revocation status and repository services.

Disaster recovery infrastructure and procedures are fully tested at least once a year with witnessing of at least one member of Intesi Group.

5.7.3 Entity private key compromise procedures

Compromise of the CA private key(s) implies immediate revocation of the certificate of the key(s) compromised. The QTSP will additionally take the following measures:

- stop the affected qualified services.
- revoke all certificates that became unreliable because of the event;
- immediately publish the CRL with revocation information;
- Notifies customers and end users of the key compromise.
- Informs the Conformity Assessment Body.

Only after having assessed the reasons of the problem and put in place all the necessary measures for the resolution, Intesi Group will generate a new key pair and new CA certificate that will send to AgID which will insert it into the TSL. After the TSL publication Intesi Group will proceed with the reactivation of the qualified service.

5.7.4 Business continuity capabilities after disaster

Intesi Group S.p.A. establishes the necessary measures to ensure full and highly automated recovery of the time Certification Authority in case of a disaster, corrupted servers, software or data. Any such measures are compliant against the ISO/IEC 27001 standard. A Contingency Plan has been implemented to ensure business continuity following a natural or other disaster and is available as a separate internal document.

5.8 CA termination

In case of termination the TSP will take any measure necessary to minimize disruption to the certificate holders and relying parties; the TSP shall:

- at least 60 days before termination inform all customers and certificate holders;
- publish a notice on its website;
- terminate all contracts with any subcontractor;
- before the effective date of termination, transfer to another TSP the registration information, the certificate status information and all the relevant logs; If it is not possible to identify a TSP, all the data will be sent to AgID
- at the date of termination, destroy its private CA and TSU keys unless the service is taken over by another TSP; any issued certificates that have not expired will be revoked and a final long term CRL with a nextUpdate time past the validity period of all issued certificates shall be generated. This final CRL shall be available for all relying parties until the validity period of all issued certificates has passed. Once the latest CRL has been issued, the private signing key(s) of the CA will be destroyed.

6 TECHNICAL SECURITY CONTROLS

The security measures taken by Intesi Group S.p.A. with regards to its CAs to protect CAs cryptographic key and activation data, the constraints on repositories, subject CAs, and other PKI Participants, to protect their

Private Keys, activation data for their Private Keys, and critical security parameters, ensuring secure key management, and other technical security controls used by Intesi Group S.p.A. to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, auditing, archiving, and other technical security controls on PKI Participants are compliant with the following technical standards:

- ETSI EN 319 411-1
- ETSI EN 319 411-2
- ETSI EN 319 421

These controls are further described and ruled by the following sub-sections.

6.1 Key pair generation and installation

6.1.1 Key Pair Generation

6.1.1.1 Root CA

The CA generation procedure is executed by two Intesi Group operators following the Intesi Group's Key Ceremony procedure. Execution of the key generation procedure (or “key ceremony”) is recorded by Intesi Groups’ internal auditor and is kept for 20 years.

The key pair used by the Root CA is generated inside a high quality HSMs (Hardware Security Module) located into the Intesi Group data center in a controlled access area. The HSMs used are certified in accordance with FIPS PUB 140-3 Level 3 and Common Criteria (ISO 15408) at EAL 4 or higher.

6.1.1.2 Subject Certificate

The subject's key pair is generated:

- on a QSCD managed by Intesi Group data center or located in the Intesi Group's customers data center and is recorded by the internal auditing system.
- on a QSCD certified device (SmartCard or USB device) owned by the subject.
- On a QSCD managed by a customer listed in the applicable Trusted List as a qualified trust service provider for the management of remote qualified electronic signature creation devices and/or remote qualified electronic seal creation devices. This option is subject to prior documented verification of compliance with all applicable QSCD certification conditions.

6.1.1.3 TSU Certificate

Generation of the TSU key pair takes place in a physically secured environment, according to the Time-Stamp internal procedures.

Execution of the key generation procedure is recorded by Intesi Groups’ internal auditor.

The key pair used by the timestamp to sign the TimeStampToken is generated inside a high quality HSM (Hardware Security Module) located into the Intesi Group data center in a controlled access area. The HSMs used are certified in accordance with FIPS PUB 140-3 Level 3 and Common Criteria (ISO 15408) at EAL 4 or higher.

6.1.2 Private key delivery to holder

Private keys are securely generated and stored into a QSCD device located into the Intesi Groups' server room or in the Intesi Group's customers server room. Access to the private key takes place only by means of the interfaces provided by the QSCD device and only after having executed a successful authentication.

6.1.3 Public key delivery to certificate issuer

The public keys are sent to the certification service in form of a PKCS#10 request over an HTTP channel protected by a TLS v 1.2 protocol. Every RA must authenticate to the QTSP service by means of a client certificate.

6.1.4 CA public key delivery to Relying Parties

The Root CA public keys are distributed by means of the publication on the QTSP web portal (www.intesigroup.com) and distributed through the Trust-service Status List (TSL) issued and maintained by AgID.

6.1.5 Key sizes

The key pairs are generated in accordance with the **eIDAS Regulation**, the **ETSI TS 119 312** standard, and the **ENISA Agreed Cryptographic Mechanisms** guidelines.

In particular:

- Root CA keys are generated using the RSA algorithm with a key length of 4096 bits, or the NIST ECDSA P-521 algorithm.
- Keys for end-entity certificates and TSU certificates are generated using the RSA algorithm with a key length of 3072 bits, or the NIST ECDSA P-256 algorithm.
- As of 1 January 2026, certificates used for signing CRLs and OCSP responses, as well as for timestamping, are generated using the RSA algorithm with a key length of 3072 bits..

6.1.6 Public key parameters generation and quality checking

The algorithms and parameters used by Intesi Group for key pairs generation for qualified certificates and seals comply with eIDAS2 Regulation and Italian Regulations.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

6.1.7.1 Root CA

The root certificate includes KeyUsage extension with the appropriate values which indicate the purpose of the private key:

- keyCertSign (sign certificates)
- cRLSign (sign CRLs)

For further details see chapter 7.

6.1.7.2 Qualified and Seal certificates

The qualified certificate includes KeyUsage extension with the appropriate values which indicate the purpose of the private key:

- Non-repudiation

For further details see chapter 7.

6.1.7.3 TSU

The TSU certificate includes KeyUsage extension with the appropriate values which indicate the purpose of the private key:

- Digital Signature

The TSU certificate also contains the extended key usage extensions:

- Timestamping.

For further details see chapter 7.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Intesi Group ensures the secure management of the CA private keys used for issuing qualified certificates and the private keys used for signing revocation status information (CRL, OCSP) and prevents the private keys disclosure, copy, deletion, modification and unauthorized usage. The CA private keys are stored at a physically secure location, in a secure Hardware Security Modules (HSM).

The private keys used by the Root CA is kept inside a high-quality HSM (Hardware Security Module) with security certification in accordance with FIPS PUB 140-3 Level 3 and Common Criteria (ISO 15408) at EAL 4 or higher.

The private keys used by the qualified certificates, seals are generated and kept inside a QSCD (Qualified Electronic Signature Creation Device) certified device.

6.2.2 Private key (n out of m) multi-person control

Access to devices containing CA and TSU private keys is available with two operators authenticated simultaneously. No single person has all the activation data needed for accessing any of the private CA keys.

Access to the private keys related to certificates qualified for digital signature and for seal can be executed only by the holder using the authentication credential that he defined during the certificate issuance and only through the interfaces of the QSCD device.

6.2.3 Private key escrow

Key escrow is never allowed.

6.2.4 Private key backup

For guaranteeing continuity of service, the QTSP keeps an encrypted backup copy of CA and TSU keys on removable media. The backup copy is kept in a safe place in a different location of the operational copy (inside the HSM). Backup and restore procedures require the joint intervention of at least two people (“dual control”).

Subscriber’s key back-up and key recovery are not allowed except for the purpose of disaster recovery as stated by this TSPPS and the applicable TSPP.

6.2.5 Private key archival

Not applicable.

6.2.6 Private key transfer into or from a cryptographic module

Not applicable.

6.2.7 Private key storage on cryptographic module

The private keys are generated and stored in a hardened and tamper-resistant protected area of the cryptographic module managed by the Certification Authority.

6.2.8 Method of activating private key

CA's private keys and TSU's private keys are activated using the procedures established by the HSM supplier and are consistent with the security certification. Activation always occurs under the dual control of two TSP operators.

The private keys related to the signature certificate and the private keys relating to the seal certificate can only be activated by the holder using the authentication credentials defined during the certificate issuance (see section 4.2) and in accordance with the procedure provided by the provider of the QSCD device.

6.2.9 Method of deactivating private key

CA's private keys and TSU's private keys are deactivated using the procedures established by the HSM supplier and are consistent with the security certification. Deactivation always occur under the dual control of two TSP operators.

The private keys related to the signature certificate and the private keys relating to the seal certificate can only be deactivated by the holder closing the working session opened with the authentication, according with the procedures established by the QSCD.

6.2.10 Method of destroying private key

The CA and TSU keys are destroyed through secure deletion from the primary and backup media removing permanently any keys were stored on. The CA key destruction is performed following and internal procedure and is executed under dual control of two authorized operators.

Signature's private keys and seal's private keys, at the end of the validity period of the related certificate, are automatically deleted form the security modules through a process that ensures the impossibility of recovering them and re-using them again.

6.2.11 Cryptographic module rating

See section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

See section 5.5.

6.3.2 Certificate operational periods and key pair usage periods

KeyPair usage period corresponds with the validity period indicated into the corresponding certificate.

TSU Certificates has ten years validity and three months usage period.

6.4 Activation data

Intesi Group S.p.A. ensures that activation data associated to operation executed with Intesi Group. CAs and TSUs private keys are securely generated, managed, stored and archived as described in the sub-section of sections 6.1 and 6.2.

The private keys activation data relating to qualified certificates (signature and seal) are defined by the holder during the certificate issuance phase. Holders are responsible for managing and securely protecting private activation data. For details see section 4.1.2 of this document and the related TSPP.

The Intesi Group's registration and issuing process ensures the confidentiality of the certificate activation data by protecting all communications between the components of the infrastructure through a secure TSL/SSL channel and saving all the information in encrypted form.

The activation mechanism of the private keys managed by Intesi Group is handled by the SAM (Security Access Module) component, which is part of the PkBox architecture and is subject to QSCD certification.

6.5 Computer Security Controls

Intesi Group ensures that computer security controls are implemented in compliance with the technical standard ETSI EN 319 411-1, ETSI EN 319 411-2 and ETSI TS 119 431-1. Intesi Group internal procedures are ISO/IEC 27001 certified. System configurations are monitored by the internal monitoring system and by the SOC (Security Operations Center). Any unplanned change detected by the monitoring systems is assessed and, where necessary, handled as a security incident.

6.6 Life cycle technical controls

The software development supporting the trust services of Intesi Group is executed conforming with the quality management system in compliance with UNI EN ISO 9001:2015

Intesi Group internal procedures are ISO/IEC 27001 certified.

Detailed descriptions of implemented life cycle technical controls are available as internal document(s).

Intesi Group only uses applications and devices that:

- are commercial off-the-shelf hardware and software, designed and developed by a documented design methodology, or;
- custom hardware and software developed by a reliable party in a controlled environment using structured development methods, or;
- open-source software which comply with the security requirements and their adequacy is ensured by software verification and validation.

New components are first tested within the testing environment before being used in production environment. Production and development environments are totally uncoupled.

Hardware is procured and shipped in a manner to reduce the likelihood of tampering. The hardware is dedicated to QTSP and QTSP related operations.

6.7 Network security controls

Network security controls including but not limited to firewalls, network intrusion detection secure communication between PKI Participants ensuring confidentiality and mutual authentication, anti-virus protection, website security, databases and other resources protection from outside boundaries, etc. are implemented in compliance with the requirements contained into the standard ETSI EN 319 411-1 and with ETSI EN 319 411-2.

Intesi Group relies on a Security Operations Center (SOC) that monitors systems 24/7 and promptly reports any anomalies, tampering, or attempted intrusions to the CISO team

Detailed descriptions of implemented network security controls are available into the security policy document.

6.8 CA and Timestamping

All the computer systems used by the CA and Time-stamping service are synchronized with a Network Time Protocol (NTP) synchronized using “Stratum 1” time source. NTP service grants the time accuracy within few milliseconds of Coordinated Universal Time. Time stamps are issued with an accuracy of 1 second.

6.9 Asset inventory

Intesi Group every six months executes an internal audit aimed to verify the respect of the internal security policy and to check if significant changes to the assets occurred to ensure their continuing suitability, adequacy and effectiveness. The result of every audit is recorded in an internal audit report.

7 CERTIFICATE AND CRL PROFILE

The certificates conform to the ISO/IEC 9594-8:2005 [X.509] standard and to the [RFC 5280] public specification.

As for cryptographic algorithms, minimum length of keys, key parameters and hashing functions, the QTSP conforms to: ETSI TS 119 312.

7.1 Certificate profile

7.1.1 CA for Time-stamp certificate

Field	Value
Version Number	V3
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
IssuerDistinguishedName	CN=Intesi Group EU Qualified Time-Stamp CA G2, OU=Qualified Trust Service Provider, O = Intesi Group S.p.A., 2.5.4.97 = VATIT-02780480964, C = IT
Validity	<20 years>
SubjectDistinguishedName	CN=Intesi Group EU Qualified Time-Stamp CA G2, OU=Qualified Trust Service Provider, O = Intesi Group S.p.A., 2.5.4.97 = VATIT-02780480964, C = IT
SubjectPublicKeyInfo	<RSA public key of 4096 bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**
Basic Constraints	critical: CA=true
Authority Key Identifier (AKI)	<public key SHA1-digest>
Subject Key Identifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: keyCertSign, cRLSign

Field	Value
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
CRLDistributionPoints (CDP)	<not included>

7.1.2 CA for Qualified Electronic Signature

Field	Value
Version Number	V3
Signature	RSA with SHA-256 EC-DSA with SHA-256
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Signature CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OID.2.5.4.97=VATIT-02780480964, C=IT
Validity	<20 years>
SubjectDistinguishedName	CN=Intesi Group EU Qualified Electronic Signature CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OID.2.5.4.97=VATIT-02780480964, C=IT
SubjectPublicKeyInfo	<RSA public key of 4096 bits> <ECDSA public key of 521bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**
Basic Constraints	critical: CA=true
Authority Key Identifier (AKI)	<public key SHA1-digest>
Subject Key Identifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: keyCertSign, cRLSign
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
CRLDistributionPoints (CDP)	<not included>

7.1.3 CA for Qualified Electronic Seal

Field	Value
Version Number	V3
Signature	RSA with SHA-256 EC-DSA with SHA-256
IssuerDistinguishedName	CN = Intesi Group EU Qualified Electronic Seal CA G2, OU = Qualified Trust Service Provider, O = Intesi Group S.p.A., 2.5.4.97 = VATIT-02780480964, C = IT
Validity	<20 years>
SubjectDistinguishedName	CN = Intesi Group EU Qualified Electronic Seal CA G2, OU = Qualified Trust Service Provider, O = Intesi Group S.p.A., 2.5.4.97 = VATIT-02780480964, C = IT
SubjectPublicKeyInfo	<RSA public key of 3072 bits> <ECDSA public key of 256 bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**
Basic Constraints	critical: CA=true
Authority Key Identifier (AKI)	<public key SHA1-digest>
Subject Key Identifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: keyCertSign, cRLSign
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
CRLDistributionPoints (CDP)	<not included>

7.1.4 Certificate for TSU

Field	Value
Version Number	V3 (2)
Signature	RSA with SHA-256 EC-DSA with SHA-256
IssuerDistinguishedName	CN=Intesi Group Qualified Time-Stamp CA G2, OrganizationIdentifier=VATIT-02780480964, O=Intesi Group S.p.A., OU=Qualified Trust Service Provider, C=IT

Field	Value
Validity	<10 years>
SubjectDistinguishedName	CN=Time-Stamping Authority TSU<n>, OrganizationIdentifier=VATIT-02780480964, O=Intesi S.p.A., C=IT
SubjectPublicKeyInfo	<RSA public key of 3072 bits> <ECDSA public key of 256 bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
Subject Key Identifier (SKI)	<included>
KeyUsage	Critical: Digital Signature
Extended Key Usage (EKU)	Critical: Time Stamping
CertificatePolicies	PolicyOID = 1.3.6.1.4.1.48990.1.1.5.1 PolicyOID = 1.3.76.16.6 (agidCert) TSPPS-URI = http://www.intesigroup.com/en/documents
CRLDistributionPoints (CDP)	http://crl.time4mind.com/Intesi/qualifiedtimestampCA.crl
QCStatement	ETSI Qualified Certificate compliance esi4-qcStatement-1 (0.4.0.1862.1.1)
Basic Constraints	<not included>
Policy Mappings	<not included>
Name constraints	<not included>
Policy constraints	<not included>
Inhibit any-policy	<not included>
SubjectAlternativeName (SAN)	<not included>
IssuerAlternativeName	<not included>
Subject directory attributes	<not included>

7.1.5 End User Certificate for Qualified Electronic Signature

Field	Value
Version Number	V3 (2)
Signature	RSA with SHA-256 EC-DSA with SHA-256

Field	Value
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Signature CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OrganizationIdentifier=VATIT-02780480964, C=IT
Validity	<max 5 years>
SubjectDistinguishedName	serialNumber=<see id-etsi-qcs-SemanticsId-Natural>, G=<Subject name>, SN=<Subject surname>, dnQualifier=<CA Internal identifier> CN=<Name Surname>, O=<Optional: subject organization>, OrganizationIdentifier=<Optional: subject organization Identifier> C=<ISO 3166 Country code>
SubjectPublicKeyInfo	<RSA public key of 3072 bits> <ECDSA public key of 256 bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
Subject Key Identifier (SKI)	<included>
KeyUsage	Critical: non-repudiation
CertificatePolicies	Not Critical: • PolicyOID = 0.4.0.194112.1.2 (QCP-n-qscd) • PolicyOID = 1.3.76.16.6 (agidCert) • PolicyOID = 1.3.6.1.4.1.48990.1.1.1.1 • TSPPS-URI = http://www.intesigroup.com/en/documents
CRLDistributionPoints (CDP)	Not Critical: http://crl.time4mind.com/Intesi/qualifiedsignatureCA.crl
Authority Information Access (AIA)	Not Critical: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) http://ocsp.time4mind.com 1.3.6.1.5.5.7.48.2 (id-ad-caIssuers) http://caissuers.time4mind.com/Intesi/qualifiedsignatureCA.crt
QCStatement	PKIX QCSyntax-v2 qcStatement-2 (0.4.0.194121.1.1) id-etsi-qcs-semanticsId-Natural
	ETSI Qualified Certificate compliance esi4-qcStatement-1 (0.4.0.1862.1.1)
	ETSI retention period esi4-qcStatement-3 (0.4.0.1862.1.3) QcEuRetentionPeriod: 20
	ETSI QCS SSCD esi4-qcStatement-4 (0.4.0.1862.1.4)
	ETSI PDS

Field	Value
	esi4-qcStatement-5 (0.4.0.1862.1.5) url:http://www.intesigroup.com/en/documents language: en
	ETSI type esi4-qcStatement-6 (0.4.0.1862.1.6) QcType: id-etsi-qct-esign
Basic Constraints	<not included>
Policy Mappings	<not included>
Name constraints	<not included>
Policy constraints	<not included>
Inhibit any-policy	<not included>
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
IssuerAlternativeName	<not included>
Subject directory attributes	<not included>

7.1.6 Certificate for Qualified Electronic Seal

Field	Value
Version Number	V3 (2)
Signature	RSA with SHA-256 EC-DSA with SHA-256
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Seal CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OrganizationIdentifier=VATIT-02780480964, C=IT
Validity	<max 5 years>
SubjectDistinguishedName	dnQualifier=<CA Internal identifier> CN=<Commonly used organization name>, O=<subject organization>, OrganizationIdentifier=<subject organization Identifier> C=<ISO 3166 Country code>
SubjectPublicKeyInfo	<RSA public key of 3072 bits> <ECDSA public key of 256 bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**

Field	Value
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
Subject Key Identifier (SKI)	<included>
KeyUsage	Critical: non-repudiation
CertificatePolicies	Not Critical: • PolicyOID = 0.4.0.194112.1.3 (QCP-l-qscd) • PolicyOID = 1.3.76.16.6 (agidCert) • PolicyOID = 1.3.6.1.4.1.48990.1.1.2.1 • TSPPS-URI = http://www.intesigroup.com/en/documents
CRLDistributionPoints (CDP)	Not Critical: http://crl.time4mind.com/Intesi/qualifiedsealCA.crl
Authority Information Access (AIA)	Not Critical: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) http://ocsp.time4mind.com 1.3.6.1.5.5.7.48.2 (id-ad-caIssuers) http://caissuers.time4mind.com/Intesi/qualifiedsealCA .crt
QCStatement	PKIX QCSyntax-v2 qcStatement-2 (0.4.0.194121.1.2) id-etsi-qcs-semanticsId-Legal
	ETSI Qualified Certificate compliance esi4-qcStatement-1 (0.4.0.1862.1.1)
	ETSI retention period esi4-qcStatement-3 (0.4.0.1862.1.3) QcEuRetentionPeriod: 20
	ETSI QCS SSCD esi4-qcStatement-4 (0.4.0.1862.1.4)
	ETSI PDS esi4-qcStatement-5 (0.4.0.1862.1.5) url:http://www.intesigroup.com/en/documents language: en
	ETSI type esi4-qcStatement-6 (0.4.0.1862.1.6) QcType: id-etsi-qct-eseal
Basic Constraints	<not included>
Policy Mappings	<not included>
Name constraints	<not included>
Policy constraints	<not included>
Inhibit any-policy	<not included>
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>

Field	Value
IssuerAlternativeName	<not included>
Subject directory attributes	<not included>

7.1.7 OCSP Certificate for Qualified Electronic Signature

Field	Value
Version Number	V3 (2)
Signature	RSA with SHA-256 EC-DSA with SHA-256
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Signature CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OrganizationIdentifier=VATIT-02780480964, C=IT
Validity	<max 5 years>
SubjectDistinguishedName	CN=OCSP, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., C=IT
SubjectPublicKeyInfo	<RSA public key of 3072 bits> <ECDSA public key of 256 bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**
Authority Key Identifier (AKI)	<included>
Subject Key Identifier (SKI)	<included>
KeyUsage	Critical: Digital Signature
ExtendedKeyUsage	Not Critical: OCSP Signer
CertificatePolicies	<not included>
CRLDistributionPoints (CDP)	<not included>
Authority Information Access (AIA)	<not included>
QCStatement	<not included>
Basic Constraints	<not included>
Policy Mappings	<not included>
Name constraints	<not included>
Policy constraints	<not included>

Inhibit any-policy	<not included>
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
IssuerAlternativeName	<not included>
Subject directory attributes	<not included>

7.1.8 OCSP Certificate for Qualified Electronic Seal

Field	Value
Version Number	V3 (2)
Signature	RSA with SHA-256 EC-DSA with SHA-256
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Seal CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OrganizationIdentifier=VATIT-02780480964, C=IT
Validity	<max 5 years>
SubjectDistinguishedName	CN=OCSP, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., C=IT
SubjectPublicKeyInfo	<RSA public key of 3072 bits> <ECDSA public key of 256 bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**
Authority Key Identifier (AKI)	<included>
Subject Key Identifier (SKI)	<included>
KeyUsage	Critical: Digital Signature
ExtendedKeyUsage	Not Critical: OCSP Signer
CertificatePolicies	<not included>
CRLDistributionPoints (CDP)	<not included>
Authority Information Access (AIA)	<not included>
QCStatement	<not included>
Basic Constraints	<not included>

Policy Mappings	<not included>
Name constraints	<not included>
Policy constraints	<not included>
Inhibit any-policy	<not included>
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
IssuerAlternativeName	<not included>
Subject directory attributes	<not included>

7.2 CRL profile

The CRLs are compliant with the with the ISO/IEC 9594-8:2005 [X.509] International Standard and public specification [RFC 5280].

Besides the mandatory information, the CRLs also contain:

- *nextUpdate* (date for next issue of CRL)
- *CRLNumber* (sequential number of CRL)

Moreover, in correspondence with each item of the CRL there is a *reasonCode* extension to indicate the reasons for suspension or revocation.

The CRLs are signed using the hashing algorithm sha256WithRSAEncryption (1.2.840.113549.1.1.11).

7.2.1 CRL issuing parameter

Field	Value
CRL Issuance Period	6 hours
CRL Duration	24 hours
CRL Grace Period	600 seconds

7.2.2 CRL for the Qualified Timestamp certificate

Field	Value
Version Number	V2
CRL Number	<included>

Field	Value
IssuerDistinguishedName	CN=Intesi Group EU Qualified Time-Stamp CA G2, OU=Qualified Trust Service Provider, O = Intesi Group S.p.A., 2.5.4.97 = VATIT-02780480964, C = IT
Signature	RSA with SHA-256 EC-DSA with SHA-256
thisUpdate	<included>
nextUpdate	<included>
Extentsions	**Value**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
expireCertsOnCrl	<Same as the notBefore date of the CA certificate>
Revoked Certificate List Entries	
Certificate Serial Number	<included>
Revocation Date	<included>
Revocation Reason Code	<included when reason code different from unspecified>

7.2.3 CRL for the Qualified Electronic Qualified certificate

Field	Value
Version Number	V2
CRL Number	<included>
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Signature CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., 2.5.4.97=VATIT-02780480964, C=IT
Signature	RSA with SHA-256 EC-DSA with SHA-256
thisUpdate	<included>
nextUpdate	<included>
Extentsions	**Value**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
expireCertsOnCrl	<Same as the notBefore date of the CA certificate>

Field	Value
Revoked Certificate List Entries	
Certificate Serial Number	<included>
Revocation Date	<included>
Revocation Reason Code	<included when reason code different from unspecified>

7.2.4 CRL for the Qualified Electronic Seal certificate

Field	Value
Version Number	V2
CRL Number	<included>
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Seal CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., 2.5.4.97=VATIT-02780480964, C=IT
Signature	RSA with SHA-256 EC-DSA with SHA-256
thisUpdate	<included>
nextUpdate	<included>
Extensions	**Value**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
expireCertsOnCrl	<Same as the notBefore date of the CA certificate>
Revoked Certificate List Entries	
Certificate Serial Number	<included>
Revocation Date	<included>
Revocation Reason Code	<included when reason code different from unspecified>

7.3 Timestsamp Profile

Version		V1
Policy		0.4.0.2023.1.1
MessageImprint	hashAlgorithm	2.16.840.1.101.3.4.2.1 (sha-256) or upper

	hashedMessage	<included>
SerialNumber		<included>
accuracy		1 second
genTime		<included>
qcStatement		"esi4-qtstStatement1

8 COMPLIANCE AUDIT

The technological infrastructure, physical and logical security controls, the operating procedures, and the personnel employed in providing the TSP services described in this TSPPS conforms to the EU eIDAS2 Regulation, implementing acts and corresponding ETSI standards for trust services eIDAS2 Regulation, implementing acts and corresponding ETSI standards for trust services.

Intesi Group is subject to external audits. Audits are conducted every year with compliance review in between according to eIDAS2 Regulation. These include audits pursuant to EU eIDAS2 Regulation, ETSI EN 319 401 and other relevant ETSI standards for the services provided. All these audits require demonstration of a maximum level of security and conformity to documented policies and practices.

The auditor shall be an accredited Conformity Assessment Body (CAB), according to EU eIDAS2 Regulation and ETSI standards. The list of the accredited CABs is published and maintained updated by the European Commission.

In addition, Intesi Group performs internal self-audits. Topics covered by these audits include checks of proper implementation of Intesi Group's certificate policies and extensive checks on key management policies, security controls, operations policy and comprehensive checks on certificate profiles.

Intesi Group reserves the right to perform periodic inspections and audits of any LRA facilities to validate that the LRA is operating in accordance with the security practices and procedures laid out in the present CPS and in internal documents. Intesi Group is a Qualified Trust Service Provider (QTSP) according to European legislation; as such, Intesi Group is supervised by AgID.

8.1 Frequency or circumstances of assessment

Intesi Group commits to do what is necessary so that a compliance audit be done at least every 12 months engaging a Conformity Assessment Body accredited according to the eIDAS2 Regulation.

The internal audits are carried out in accordance with a schedule which provides different periods (from monthly to annual) for the various technical-operational aspects of the QTSP service.

8.2 Identity and qualification of assessor

The internal audits are carried out by Intesi Groups' internal auditor, who is suitably qualified for the task. External audits are performed by a Conformity Assessment Body accredited according to the eIDAS2 Regulation.

8.3 Assessor's relationship to assessed entity

No relationship shall exist between the QTSP and any external auditors that can influence the outcome of the audits in favor of Intesi Groups.

Intesi Group internal auditor does not belong to the organizational unit in charge of TSP operations.

8.4 Topics covered by assessment

Audits performed by external assessors (other than AgID) are aimed at verifying compliance of Intesi Group and the qualified services it provides according to the applicable requirements of the eIDAS2 Regulation.

The main objective of the internal audit is to verify the respect of Intesi Group internal operating procedures and their compliance with this TSPPS.

8.5 Actions taken as result of deficiency

In the case of non-compliances, AgID will require the QTSP to adopt the necessary corrective measures within a certain period, under penalty of fines and revocation of the accreditation.

Non-compliances found by CABs are brought to the attention of Intesi Group management who decides how to handle them on a case-by-case basis.

8.6 Communication of results

The results of internal audits are presented directly to Intesi Group top management, and shared with the other internal stakeholders, via an audit report.

When relevant and according to the eIDAS2 Regulation security incidents will be notified to the interested parties.

9 OTHER BUSINESS AND LEGAL MATTERS

The general Terms & Conditions of the QTSP service herein described are provided to customers as a separate document to be accepted at application time. The Terms & Conditions document is published on the QTSP web site.

In the case of a discrepancy between this TSPPS and the separate "Terms & Conditions" document, "Terms & Conditions" will take precedence.

9.1 Service fees

The fees are published on Intesi Group's website at www.intesigroup.com. Changes to fees applicable to existing Contracts shall be communicated and take effect in accordance with Section 10 of the General Terms and Conditions of the Certification Service Contract.

Different conditions may be negotiated case by case, according to the volumes requested.

9.2 Financial responsibility

Intesi Group maintains the following insurance related to its performance and obligations under this TSPPS:

- Commercial General Liability insurance
- Professional Liability/Errors and Omissions insurance.

Such insurance is with a company rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide.

9.3 Confidentiality of Business information

9.3.1 Confidential information

The following information are considered confidential:

- data provided by Certificate Applicants except for information that must be included in the certificates or that for other reasons are considered non-confidential (see paragraph 9.3.2 e 9.3);
- certificates issuance requests;
- certificates suspension or certificates revocation requests;
- communications exchanged between PKI participants (see section 1.3);
- reserved codes provided to the certificate holder (e.g. login credentials, private keys activation data etc.) if are generated by the QTSP or are managed by the QTSP systems;
- private keys;
- system logs;
- contracts with external RAs.

9.3.2 Non-confidential information

All information that must be public in compliance with the law or the certification services technical standards (e.g. RFC 5280) or for the explicit request of the certificate holder are not considered confidential.

The following information are not considered confidential:

- certificates and the information contained therein;
- lists of suspended or revoked certificates (CRL);
- information on the status of certificates issued on-line (e.g. via OCSP).

9.3.3 Responsibility for the protection of confidential information

The QTSP ensures that confidential information is physically and/or logically protected from unauthorized access (even if read only) and from the risk of loss due to disasters.

All confidential information is processed by the QTSP in compliance with applicable data protection and privacy laws.

9.4 Privacy of personal information

The Intesi Group privacy policy is published at the URL:

https://www.intesigroup.com/en/privacypolicy/

9.5 Intellectual Property Rights

Within the service regulated by this TSPPS, the QTSP does not collect and does not process sensitive data nor judicial data (with reference to article 4 of the aforesaid Decree [DLGS196]). This TSPPS is the property of Intesi Group who reserves all rights associated with the same. The subscriber of the service keeps all the rights on its own commercial marks (brand names) and its own domain names. With regards to the property rights of other data and information, the applicable law shall be applied.

9.6 Representation and warranties

9.6.1 Certification Authority

The QTSP shall:

- operate in compliance with this TSPPS;
- identify the subscriber as described in this TSPPS;
- issue and manage the certificates as described in this TSPPS;
- provide an efficient suspension and revocation service for the certificates;
- guarantee that the subscriber, at the time when the certificate is issued, did possess the corresponding private key;
- timely inform about any eventual compromise of its own private key;
- provide clear information about the procedures and requirements of the service;
- provide a copy of this TSPPS to anyone requesting it;
- guarantee processing of personal data in compliance with applicable law;
- provide an efficient and reliable information service about the status of the certificates.

Intesi Group guarantees an availability level of at least 99.8% for the services described in this TSPPS, measured separately for each service on a quarterly basis, with services expected to be available 24 hours a day, 7 days a week.

Availability is calculated as the percentage ratio between the actual service availability time and the total time of the relevant calendar quarter. Service unavailability is detected through the company's monitoring systems.

The same availability level applies to public information repositories and certificate status checking services.

9.6.2 Registration Authority

The RA activities are performed by RAO and LRA under a contractual obligation to comply scrupulously with the TSPPS, with the relevant section of the applicable TSPP, and with the RA relevant Intesi Group internal procedures.

The registration authority service is not applicable for Time Stamp service.

9.6.3 Subscribers

For the obligations of Subjects and Subscribers, see Section 5 of the Terms and Conditions.

9.6.4 Relying parties

For the obligations of Relying Parties, see Section 7 of the Terms and Conditions.

9.6.5 Timestamp Authority

For the obligations of users and third parties, refer to the document "Terms and Conditions" of the Timestamping Service published on Intesi Group's official website.

9.6.6 External suppliers

Intesi Group retains overall responsibility for the compliance of its trust services with applicable policies and security requirements, including activities performed by external suppliers.

Relationships with suppliers supporting qualified trust services are governed by written agreements defining the activities entrusted to them, responsibilities, applicable requirements and service levels, proportionate to the associated risks.

Where a supplier processes personal data on behalf of Intesi Group, the relationship is governed by an agreement compliant with Article 28 GDPR.

9.7 Disclaimer of warranties

Except where expressly stated elsewhere in the TSPPS and applicable regulations, Intesi Group S.p.A., as a TSP, disclaims any and all warranties and obligations of any kind, including any warranties of merchantability, fitness for a particular purpose, and accuracy of the information provided (other than the fact that it comes from an authorized source). Furthermore, Intesi Group disclaims any liability regarding negligence or lack of care by Subscribers and Relying Parties. Intesi Group S.p.A. provides no warranties for any software.

9.8 Limitations of Liability

Please refer to Chapter 8 of the “Terms and Conditions” document.

9.9 Indemnities

The indemnification obligations of Subscribers, Subjects and Relying Parties are set out in Sections 8.4 and 8.5 of the General Terms and Conditions of the Certification Service Contract.

9.10 Term and Termination

This TSPPS is published on the QTSP website (see Chapter 2) and on the AgID website and remains in force until replaced by a new version. The effective date of amendments affecting existing Contracts is subject to the notification and acceptance arrangements described in Section 9.11.

9.11 Amendments

Intesi Group reserves the right to amend this TSPPS.

Material amendments, namely those that may affect the conditions of use or acceptance of the service by Subjects, Subscribers or Relying Parties, shall be communicated before they take effect, in accordance with the notice periods and procedures specified in Section 10, “Notifications and Contract Amendments”, of the General Terms and Conditions of the Certification Service Contract. Examples include changes to identification methods, suspension and revocation services, certificate policies and applicable fees.

For services provided under agreements with customers who manage communications with their own users, Intesi Group shall send the notice to the customer’s designated contacts. The customer shall promptly inform the affected users, in accordance with the contractual arrangements and sufficiently in advance of the effective date of the amendments.

For users who have a direct contractual relationship with Intesi Group, notices shall be provided in accordance with Section 10 of those Terms and Conditions.

Purely editorial changes, corrections of typographical errors and updates to references that do not affect rights, obligations, security or conditions of use may be published without individual notification, subject to applicable contractual obligations.

Each new version of this TSPPS shall be published in Intesi Group’s document repository, identifying its version number, date and changes made. Users are required to consult the repository periodically for updates. This requirement does not replace the notification obligations applicable to material amendments.

9.12 Dispute Resolution Provisions

For the certification service, Subscribers and certificate applicants should refer to Section 11 of the General Terms and Conditions of the Certification Service Contract, published on Intesi Group’s official website. For

the timestamping service, refer to the dispute resolution provisions of the applicable Terms and Conditions of the Timestamping Service.

All customers and third parties may submit complaints or reports by email, preferably via certified email (PEC), to tsp@ig-trustmail.com.

The email must include the sender's identifying details (first name, last name, address, and tax code or VAT number) and a detailed description of the reasons for the complaint or report.

9.13 Governing Law

This TSPPS is subject to Italian and European Law and as such shall be interpreted and carried out. For that not expressly prescribed in this TSPPS, the applicable law shall prevail.

9.14 Compliance with Applicable Law

Mandatory applicable laws shall prevail on the provisions of this TSPPS.

9.15 Miscellaneous Provisions

Intesi Group incorporates by reference the following information in all Certificates it issues:

- Terms and conditions described in the applicable CP;
- Any other applicable Certificate Policy as may be stated in an issued Certificate;
- The mandatory elements and any non-mandatory but customized elements of applicable standards;
- Content of extensions and enhanced naming not addressed elsewhere;
- Any other information that is indicated to be so in a field of a Certificate.

To incorporate information by reference Intesi group through its CAs uses computer-based and text-based pointers that include URLs, OIDs, etc.