Intesi Group Trust Service Provision Policy (TSPP)

Data: 24 November 2017

History

Protocol	Change	Rev.	Date	Author	Approved by
QTSPP	First release	1.0	04/04/2017	G. Damiano	F. Catullo
QTSPP	Clause 4.8 updated to include the maximum delay for certificate status publication	1.1	21/05/2017	G. Damiano	F. Catullo
TSPP	Updated to include CA services for QC and Advanced Electronic Signatures	1.2	19/07/2017	G. Damiano	F. Catullo
TSPP	Updated some inaccuracy	1.3	31/07/2017	G. Damiano	F. Catullo
TSPP	General revision of the document	1.4	24/11/2017	G. Damiano	F. Catullo

Summary

1 INTRODUCTION

1.1 TSPP Overview

This Trust Service Provision Policy (hereafter referenced also as TSPP) covers the technical, security and organizational requirements for Intesi Group S.p.A. (hereafter referenced also as “Intesi Group”) to provide Trust Services in compliance with the Regulation (UE) n. 910/2014 (eIDAS Regulation).

In general, the present TSPP states "what is to be adhered to", while the specific practices needed to implement the present TSPP, "how it is adhered to", are described in the Intesi Group Trust Service Provider Practice Statement (TSPPS), published on the Intesi Group web site, together with the present policy, at the following URI:

http://www.intesigroup.com/en/documents

Compliance with security and policy requirements specified in ETSI EN 319 401, ETSI EN 319 411 and ETSI EN 319 421 guarantees that Intesi Group adopts international state-of-the-art in trust service provisioning and fulfilment of the eIDAS Regulation requirements.

The present document describes the policy to which the Intesi Group Trust Services adheres, to confirm to Subjects, Subscribers and Relying Parties of the correct operation and management of the respective services.

1.1.1 Purpose

The present document specifies a Trust Service Provider Policy to meet general requirements for Intesi Group Trust Services.

This Certificate Policy applies to the following certificates and time stamp tokens issued by Intesi Group:

- Root CA (self-signed) certificates;
- Qualified certificates for electronic signatures and seals;
- Time Stamp Unit (TSU) certificates;
- Qualified Electronic Time Stamps (Qualified Time Stamp Tokens, QTST).

The qualified certificates issued by Intesi Group that specify one of the OIDs for qualified certificates defined in this TSPP in their Certificate Policies field, can be considered as fully compliant with the relevant requirements of the eIDAS Regulation for TSP issuing qualified certificates.

The qualified TSTs issued by Intesi Group that specify the OIDs for qualified Timestamps defined in this TSPP in the TSA Policy field, can be considered as fully compliant with the relevant requirements of the eIDAS Regulation for Qualified Electronic Time stamps provisioning.

The present document is publicly available. Its distribution is regulated as described in the "Intellectual Property Rights" section.

1.1.2 Level of specificity

The present Qualified Trust Service Provider Policy describes only general rules of issuing and managing qualified certificates (QC) and TST's. Detailed description of the infrastructure and related operational procedures are described in the Security Plan (Piano della Sicurezza) that is available only to authorised Intesi Group personnel, to the Conformity Assessment Body auditors and to the relevant Supervisory Body (AgID).

1.1.3 References

1. "eIDAS Regulation": Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
2. IETF RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol – August 2001.
3. ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
4. ETSI EN 319 422 Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp profiles.
5. Intesi Group Trust Service Provision Practice Statement latest version in force available on Intesi Group site.

6. IETF RFC 5280 – Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile.
7. ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
8. ETSI EN 319 411 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements and Part 2: Requirements for trust service providers issuing EU qualified certificates.
9. ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures, Part 2: Certificate profile for certificates issued to natural persons, Part 3: Certificate profile for certificates issued to legal persons, Part 4: Certificate profile for web site certificates and Part 5: QCStatements.

1.2 Document name and identification

Policy Name: Intesi Group Qualified Trust Service Provision Policy

All the TSP policies defined by Intesi Group in the present document have the Object Identifier (OID) prefix 1.3.6.1.4.1.48990.1 named TSPP

OID for TSU certificates supporting qualified timestamps:

- TSPP.1.5.1

OID for Best practice Time Stamp Policy (BTSP):

- 0.4.0.2023.1.1

Note: This is the Best Practices Policy for Time-stamp defined in EN 319 421 and is included in the time stamps to claim conformance to it.

OID for Qualified Certificates for Qualified Electronic Signatures:

- TSPP.1.1.1, and
- 0.4.0.194112.1.2 (QCP-n-qscd defined in ETSI EN 319 411-2)

OID for Qualified Certificates for Qualified Seal:

- TSPP.1.2.1, and
- 0.4.0.194112.1.3 (QCP-l-qscd defined in ETSI EN 319 411-2)

1.3 PKI participants

This Certificate Policy applies to:

- The Intesi Group Root Certification Authority CAs:
  - its logistic and technical infrastructure;
  - its personnel.
- Subjects to whom certificates, time stamps have been issued in compliance with this TSP Policy.
- Relying parties, relying on certificates, time stamps or any trust token issued by Intesi Group in compliance with this TSP Policy.

A detailed description of the PKI participants can be found in the paragraph 1.3 of the TSPPS.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

1.4.1.1 Qualified certificates appropriate uses

Qualified certificates issued by Intesi Group may be used only to create qualified electronic signatures (in case of qualified signature certificates) and qualified electronic seals (in case of qualified electronic seal certificates) in full compliance with the present policies and the applicable practice statements.

1.4.1.2 TSU certificates appropriate uses

TSU certificates issued by Intesi Group may be used only to sign Time Stamp Tokens with the authorized technical and physical infrastructure.

1.4.1.3 Time Stamp Tokens appropriate uses

TSTs issued by Intesi Group may be used:

- to testify that the datum represented by the time stamped digest existed before the time specified in the TST, with the accuracy provided for in section 7.3.3;
- to extend a signature validity beyond the signer's certificate expiration date;
- in all cases unless otherwise stated in the rules of law and the Terms and Conditions agreed upon by Intesi Group and the subscriber.

1.4.2 Prohibited certificate uses

1.4.2.1 Qualified certificates prohibited uses

Certificates issued to subjects under this policy must not be used by applications:

- other than set forth in clause 1.4.1.1 in case of qualified outside the limit of use specified in this policy, TSPPS and Terms and Conditions;
- inconsistent with the Terms and Conditions in force and accepted by the subscriber.

Certificates issued to subjects shall not be used for authentication, data or key encryption and decryption.

1.4.2.2 TSU certificates prohibited uses

TSU certificates issued by Intesi Group must not be used other than for validation of Time Stamp Tokens issued with the corresponding private key within the authorized technical and physical infrastructure.

1.4.2.3 CA certificates prohibited uses

CA certificates issued by Intesi Group must not be used other than for validation of certificates issued with the corresponding private key.

1.4.2.4 Time Stamp Tokens prohibited uses

TSTs may not be used for purposes other than the use defined in this document, in the TSPPS and as in the "Terms & Conditions" accepted by the user.

1.5 Policy administration

1.5.1 Organization administering the document

This Policy is issued under the responsibility of:

Intesi Group S.p.A.
via Torino, 48
20123 Milano (MI)
ITALY
Email: tsp@intesigroup.com

1.5.2 Contact person

The person in charge of this Policy is:

Giuseppe Damiano, Security and RA Officer

1.6 Definitions and acronyms

AES	Advanced Electronic Signature
ARL	Authority Revocation List
B2B	Business to Business
CA	Certification Authority
CRL	Certificate Revocation List
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organisation for Standardisation
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
NCP	Normalised Certificate Policy
NCP+	Normalised Certificate Policy +
OID	Object Identifier
PKCS	Public Key Certificates Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)

QES	Qualified Electronic Signature
RFC	Request for Comments
RSA	A specific Public Key algorithm
TSA	Time Stamping Authority
TSP	Trust Service Provider
TSPP	Certificate Policy
TSPPS	Certification Practice Statement
TSS	Time Stamping Service
TST	Time Stamp Token
TSU	Time Stamping Unit
UTC	Coordinated Universal Time

2 Publication and repository responsibilities

2.1 Repositories

2.2 Publication of certification information

The following documents are published at the URL http://www.intesigroup.com/en/documents:

- this TSPP,
- the TSPPS corresponding to this TSPP,
- PKI Disclosure Statement (PDS),
- Terms & Conditions,
- Various forms

Root certificates and CRLs are published through the website www.time4mind.com with the frequency described in the TSPPS.

2.3 Time or frequency of publication

Refers to TSPPS paragraph 2.3

2.4 Access controls on repositories

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

The Subject should be identified with an X.500 Distinguished Name inserted in the Subject field of the X.509 certificate.

3.2 Initial Identity Validation

The Initial Identity validation of natural and legal persons is carried out by RAOs through RA processes described into the TSPPS.

TSU certificates are issued only to Intesi Group allowed personnel according to internal procedures as described into the TSPPS.

3.3 Identification and Authentication for Re-key Requests

The re-key operation is not available for qualified and TSU certificates.

3.4 Identification and Authentication for Revocation Requests

Qualified certificates are revoked or suspended after identification according to the procedures specified in the TSPPS.

The TSU certificate is revoked according to internal Intesi Group procedures under the supervision of the Security and RA Officer and TSP Operation Officer.

4 Certificate life-cycle operational requirements

4.1 Certificate Application

Qualified certificate application can be executed by:

- The subject for certificates issued to natural persons.
- A subscriber allowed to represent the legal persons.

TSU certificates application can be done only by Intesi Group authorized operators.

The application procedure is described in the TSPPS.

4.2 Certificate Application Processing

The certificate application process for qualified certificates, TSU certificates and TimeStampToken is described in the paragraph 4.2 of the TSPPS.

4.3 Certificate Issuance

The certificate issuance can be found fully described in the paragraph 4.3 of the TSPPS.

4.4 Certificate Acceptance

The certificate is considered accepted after being delivered to the subject or to the TSP operator. Subjects and operators can verify the content of the certificate and, in case of errors, can request the revocation and issuance of a new certificate according to the procedures described in the TSPPS.4.5 Key Pair and Certificate Usage

4.5 Key Pair and Certificate Usage

Key pairs and certificate usage are fully described in the paragraph 4.6 of the TSPPS.

4.6 Certificate Renewal

The TSP provides procedures for renewal of signature, seal and TSU certificates as described in paragraph 4.6 of the TSPPS.

The keys of expired certificates are deleted by Intesi Group internal procedures.

4.7 Certificate Re-key

Certificate re-key is never allowed.

4.8 Certificate Modification

Modification for qualified certificates is supported only by revoking the certificate to be modified and issuing a new certificate.

In case the TSU certificate needs an update, a new certificate is issued on TSP Operation Officer request as part of a new TSU initiation key ceremony.

4.9 Certificate Revocation and suspension

Revocation determines the premature termination of the validity of a certificate, starting from a given moment in time (date/time). Revocation of a certificate is irreversible and not retroactive.
The suspension of the certificate determines a temporary suspension of the validity of a certificate, starting from a given moment in time. Once a certificate has been suspended, it can be reactivated or revoked at any time.
Implementation of the suspension or revocation consists in the generation and publication of a new CRL (Certificate Revocation List) which includes the serial number of the suspended or revoked certificate. The CRL is accessible to anyone needs to verify the certificate status (see to section 4.10). Re-activation consists in the generation and publication of a new CRL in which the serial number of the previously suspended certificate does not appear.

4.9.1 Circumstances for revocation

The conditions which could cause a revocation of a qualified certificate are as follows:

1. the subscriber requests to the CA the certificate revocation;
2. the private key of the subscriber is lost, stolen or potentially compromised;
3. there is a condition of non-compliance of the contract from the owner and the certification authority.
4. the subscriber no longer has “sole” control of the Private Key because the Private Key Activation Data (PIN code) has been compromised.
5. the user can no longer use the secure device signature.
6. there is a change of the user personal data for example, loss of qualifications, cessation of powers of representation, deletion from registers or cessation of organizations membership.
7. terminates the relationship between the owner and the certification authority.
8. the CA is made aware of a possible compromise of the private key of the root CA used for issuing the certificate;
9. the CA is made aware that the subscriber organization ceased its activity.

In case of a TSU certificate the conditions which may lead to a revocation are:

1. the certificate is not correct in terms of information contained.
2. the TSP ceases the time-stamping service.
3. the TSP loses its qualification, upon request by the Supervision Authority.
4. there is the evidence of a private key compromise.
5. the TSP is made aware of a possible compromise of the private key of the TSS CA or the root CA used for issuing the TSS CA certificate.

The revocation of TSU certificate must be authorized by the Intesi Group management and must be published within 24 hours after the revocation authorization.

The suspension is not available for TSU and CA certificates.

4.10 Certificate Status Service

The status of the qualified certificates is made available through the publication of CRLs, in conformance to RFC 5280, and through a status checking service based on OCSP (On-line Certificate Status Protocol) in compliance with the specification [RFC2560].

The status of the TSU certificates is made available through the publication of CRLs, in conformance to RFC 5280.

4.11 End of Subscription

The contract between the CA and the subscriber terminates when the certificate expires or is revoked, unless there are different conditions in the contracts.

4.12 Key Escrow and Recovery

The Key Escrow is not applicable except for the cases described in the paragraph 4.12 of the TSPPS.

5 FACILITIES, MANAGEMENT AND OPERATIONAL CONTROLS

The qualified trust service controls must comply with:

- EN 319 421 for timestamp issuing
- EN 319 411-1 NCP+ policy for non-qualified certificate issuing,
- EN 319 411-2 QCP-n-qscd policy for qualified signature certificate issuing, and
- EN 319 411-2 QCP-l-qscd policy for qualified seal certificate issuing.

The Intesi Group information security management system is guided by and compliant with ISO/IEC 27001.

5.1 Physical security

Intesi Group TSP systems and devices (both HW and SW) are managed in and from secure facilities, protected from unauthorized access.

Details about security measures are described into the paragraph 5.1 of the TSPPS.

5.2 Procedural controls

Refers to paragraph 5.2 of the TSPPS.

5.3 Personnel controls

Refers to paragraph 5.2 of the TSPPS.

5.4 Event logging

All TSP systems keep track of all relevant operations. Logged events range from normal operations (e.g.: SW installation and update, log-in and log-out by operators) up to abnormal operations (e.g.: operator errors, unauthorized attempts).
For each event, information about the type, date and time of occurrence is logged.
Log files are preserved for 20 years as per rules of law currently in force.
Log files are kept in a safe and tamper proof environment.

5.5 Record Archival

The log files generated by the TSP and the documentation produced by the execution of internal procedures are safely collected and stored for a period of 20 years. Details can be found in paragraph 5.5 of the TSPPS.

5.6 Renewal of CA Key

Root certificates are renewed at least 5 years before the expiration date. The renewal procedure is described within the TSPPS and follow the key ceremony procedure.

5.7 Compromise and disaster recovery

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.

A backup copy of data, applications, and any other file necessary for a complete recovery of the service is performed daily. All of these measures are described in the "business continuity plan" and in the ISO/IEC 27001 procedure.

5.8 CA termination

The TSP has a CA cessation plan that describes the communication plan for all service stakeholders and the management of stored information such as certificate status information, log files, contracts and everything that is kept according to the Italian and European regulation.

6 TECHNICAL SECURITY CONTROLS

ETSI EN 319 411-1, ETSI EN 319 411-2 and ETSI EN 319 421 controls shall be implemented to protect systems, cryptographic keys, repositories and their management.

6.1 Key pair generation and installation

6.1.1 Root CA

Intesi Group has a Key Ceremony procedure that must be followed by authorized TSP operators to generate CA key pairs and certificates. The execution of procedure is documented on a verbal that is kept for 20 years.

6.1.2 End User Certificate

The subject certificate generation process is performed only through the processes defined in the TSPPS.

6.1.3 TSU Certificate

Intesi Group has a Key Ceremony procedure that must be followed by authorized TSP operators to generate TSU key pairs and certificates. The execution of procedure is documented on a verbal that is kept for 20 years.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Root CA

The key pair used by the Root CA is generated and managed by a properly certified HSM, at least according to FIPS PUB 140-2 Level 3 or Common Criteria (ISO 15408) at EAL 4 or higher.

6.2.2 TSU Certificate

The key pair used by the TSU is generated and managed by a properly certified HSM, at least according to FIPS PUB 140-2 Level 3 or Common Criteria (ISO 15408) at EAL 4 or higher.

6.2.3 Qualified Certificates

The key pair used by qualified certificates is generated and managed by a QSCD certified device.

6.3 Other Aspects of Key Pair Management

All the certificates are archived by Intesi Group.

6.4 Activation data

Access to activation codes of CA and TSS cryptographic devices is reserved for authorized TSP operators. Activation codes are stored in a safe place.

Accesses to the activation devices are logged and stored according to regulation.

6.5 Computer Security Controls

Role separation is enforced, and all activities performed are traced by the systems and the applications logging features.

6.6 Life cycle technical controls

Intesi Group applies procedures conforming to ISO 9001 and 27001 standards.

6.7 Network security controls

Intesi Group's systems architecture includes network protection systems. The protection of the network is also guaranteed by the processes defined in the Intesi Group‘s ISO 27001 procedure.

6.8 Time-stamping

All servers have clocks aligned with a secure time source. The Intesi Group’s monitoring system verifies the alignment of the server’s clocks with the time source. In case of misalignment the

monitoring system raise the alarm and excludes from the CA and TSS service the servers with misaligned clocks.

7 CERTIFICATE AND CRL PROFILE

7.1 Certificate profile

The certificates conform to the ISO/IEC 9594-8:2005 [X.509] standard and to the [RFC 5280] public specification and are version 3.

Qualified certificates conform to EN 319 412-2 and EN 319 412-3 respectively for electronic signature and electronic seal certificates. Qualified certificates conform also to EN 319 412-5 and the Italian laws.

TSU certificates conform to EN 319 412-3 and EN 319 422.

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

7.2 CRL profile

The CRLs are compliant with the ISO/IEC 9594-8:2005 [X.509] International Standard and public specification [RFC 5280].
As for cryptographic algorithms, minimum length of keys, key parameters and hashing functions, the CRLs conform to ETSI TS 119 312.

8 COMPLIANCE AUDIT

Intesi Group provides for auditing of all procedures as described in this TSPP and in the related TSPPS, with the purpose of verifying:

- actual compliance by personnel
- procedures efficaciousness and effectiveness
- actual possibility to comply with the procedures.

The goal is to improve the overall Intesi Group security by adopting procedures that can be effectively complied with and that present no known security loopholes.

8.1 Frequency or circumstances of assessment

Inspections are held every month or yearly depending on the audited procedures.

Compliance audit are performed every 12 months engaging a Conformity Assessment Body accredited according to the eIDAS Regulation.

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

8.2 Identity and qualification of assessor

The Internal Auditing is performed by personnel of the Internal Intesi Group Auditor.

External Auditing is performed by a Conformity Assessment Body accredited for eIDAS audit according to ISO/IEC 17065 and EN 319 403.

8.3 Assessor's relationship to assessed entity

There are no hierarchical relationships between audited Intesi Group departments and Internal Auditor.

External Auditing is performed by an independent CAB.

8.4 Topics covered by assessment

The audit covers the procedures and obligations listed in this TSPP and in the related TSPPS.

8.5 Actions taken as result of deficiency

The actions to be taken to resolve non-conformities are defined by the Intesi Group staff with the goal of resolving them as soon as possible.

8.6 Communication of results

Significant deviations from the procedure or severe security breaches are reported to TSS Officers or senior level managers, depending on the violation severity.

When relevant and according to the eIDAS Regulation security incidents with loss of personal data integrity will be notified to the Supervision Body and relevant authorities.

9 OTHER BUSINESS AND LEGAL MATTERS

The general Terms & Conditions of the TSP services are made available to subscribers and subjects as a separate document, published on the CA web site.
The “Terms & Conditions” document takes precedence in case of discrepancies with this document.

9.1 Service fees

It applies the provisions described into the paragraph 9.1 of the TSPPS and what is published on the website www.intesigroup.com.

9.2 Financial responsibility

Intesi Group maintains proper capital and insurance in relation to its performance and obligations as TSP.

9.3 Confidentiality of Business information

No additional stipulation.

9.4 Privacy of personal information

All personal data collected in the operation of the TSP are kept confidential and handled according to Regulation (EU) 2016/679 and Intesi Group's privacy policy.

9.5 Intellectual property rights

This Policy (TSPP) is the property of Intesi Group who reserves all rights associated with the same.

9.6 Representation and warranties

9.6.1 Certification Authority

The CA shall operate in compliance with this TSPP and relevant stipulations in the related TSPPS.

9.6.2 Registration Authority

The LRA shall operate in compliance with this TSPP and relevant stipulations in the related TSPPS.

The RA service is not applicable for the Time-Stamp service.

9.6.3 Subscribers

Refers to "Terms and Conditions" document at chapter 5.

9.6.4 Relying parties

Refers to "Terms and Conditions" document at chapter 7.

9.7 Disclaimer of warranties

Refers to “TSPPS” document at chapter 9.7

9.8 Limitations of Liability

Refers to “Terms and Conditions” document at chapter 8

9.9 Indemnities

Refers to “Terms and Conditions” document at chapter 8.

9.10 Term and Termination

This TSPP is effective from the time it is published on the CA website (see Chapter 2) and will remain in force until it is replaced with a new version.

9.11 Amendments

Intesi Groups reserves the right to modify this TSPP at any time whatsoever without prior notification.

9.12 Dispute Resolution Provisions

Complaints received by Intesi Group will be treated by Intesi Group internal services according to TSPPS.

9.13 Governing Law

This TSPP is subject to Italian Law and as such shall be interpreted and carried out. For that not expressly prescribed in this Policy or the related TSPPS, the law shall apply.

9.14 Compliance with Applicable Law

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

9.15 Miscellaneous Provisions

Intesi Group CA incorporates into the certificates issued under this policy the OIDs defined in paragraph 1.2 of this document to indicate that this TSPP and TSPPS apply.