Certificate Policy

Version 1.0

30/3/2017

History

Protocol	Change	Rev.	Date	Author	Approved by
CP	First release	1.0	30/03/2017	G. Damiano	F. Catullo

Index

1 INTRODUCTION

1.1 CP Overview

This Certificate Policy (hereafter referenced also as CP) 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 CP states "what is to be adhered to", while the specific practices needed to implement the present CP, "how it is adhered to", are described in the Intesi Group Trust Service Provider Practice Statement (CPS), published on the Intesi Group web site, together with the present policy, at the following URL:

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 issued by Intesi Group:

- Root CA (self-signed) certificates;
- Subordinate CA to issue and end entity certificates;
- Certificates for advanced electronic signatures certificates and seals;

The present document is public available. Its distribution is regulated as described in the “Intellectual Property Rights” section.

1.1.2 Level of specificity

The present Certificate Policy describes only general rules of issuing and managing certificates advanced electronic signatures (ACS). 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.

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. 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. EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
8. 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 Certificate Policy

All the certificate 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 Certificates for Advanced Electronic Signatures #1:

- TSPP.2.1.1
- 0.4.0.2042.1.2 (NCP+ defined in ETSI EN 319 411-1)

OID for Certificates for Advanced Electronic Seal #1:

- TSPP.2.2.1
- 0.4.0.2042.1.2 (NCP+ defined in ETSI EN 319 411-1)

Certificates with policy OID with the:

- TSPP.1 prefix is for qualified certificates.
- TSPP.3 prefix is for testing purposes only without any kind of warranty.

A detailed list of all OID used can be found into the OID document published on the Intesi Group website.

1.3 PKI participants

This Certificate Policy applies to:

- The Intesi Group Root Certification Authority, non-qualified subordinate CAs, End Entity certificates and its logistic and technical infrastructure and its personnel.
- Subjects to whom certificates have been issued in compliance with this TSP Policy.

Relying parties, relying on certificates or any trust token issued by Intesi Group in compliance with this TSP Policy.

1.3.1 Intesi Group as Time Stamping and Certification Authority

Intesi Group is a company based in Milan (Italy).

Intesi Group as Certification Authority (CA) issues qualified and not qualified certificates to any subscriber (private or public user) according to the eIDAS Regulation.

Intesi Group as Time Stamping Authority (TSA) issues qualified time stamp tokens to any subscriber (private or public user) according to the eIDAS Regulation.

Intesi Group issues TSU certificates to each Time Stamp Unit under its own responsibility.

Intesi Group root CA issues certificates to any end entity CAs issuing non-qualified certificates or certificates for keys used to create trust tokens, for example time stamp tokens, according to this TSP Policy.

1.3.2 Registration Authority (RA) and Local Registration Authority (LRA)

A Registration Authority (RA) is responsible for the subject's registration and certificate management procedures. RA activities are performed using the RA platform made available by Intesi Group by Local Registration Authorities that can be:

- Intesi Group itself by mean of appointed Registration Authority Officers.
- external organizations that subscribed a specific agreement with Intesi Group and appointed Registration Authority Officers.

LRAs enable legal person subscribers to validate the registration and to ask for revocation, suspension and reactivation of the subjects belonging to the legal person organization.

1.3.3 Subjects

Subjects are the natural or legal persons to whom non-qualified certificates or non-qualified timestamps are issued.

1.3.4 Subscribers

Subscribers are:

- natural persons acting as individual subjects, or

- natural persons representing legal persons, or
- legal persons

bound by agreement with Intesi Group as TSP to any subscriber obligations.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

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

1.4.2 Prohibited certificate uses

1.4.2.1 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.

1.4.2.2 Non-qualified certificates prohibited uses

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

- other than set forth in clause 1.4.2.1;
- outside the limit of use specified in this policy, CPS 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.

1.5 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
CP	Certificate Policy
CPS	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 will be available at the URL http://www.intesigroup.com/en/documents:

- this CP,
- the CPS corresponding to this CP,
- Terms & Conditions,
- Various forms

2.3 Time or frequency of publication

Refers to CPS 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 is identified with an X.500 Distinguished Name inserted in the Subject field of the X.509 certificate.

3.2 Initial Identity Validation

RAOs do the Initial Identity validation of natural and legal persons following RA processes described into the CPS.

3.3 Identification and Authentication for Re-key Requests

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

3.4 Identification and Authentication for Revocation Requests

Non-qualified certificates are revoked or suspended after identification according to the procedures specified in the CPS.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Non-qualified certificate application can be executed by:

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

The application procedure is described in the CPS.

4.2 Certificate Application Processing

The certificate application process for non-qualified certificates is described in the paragraph 4.2 of the CPS.

4.3 Certificate Issuance

The certificate issuance procedure is fully described into the paragraph 4.3 of the CPS.

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 CPS paragraph 4.5.

4.5 Key Pair and Certificate Usage

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

4.6 Certificate Renewal

The TSP provides procedures for certificates renewal as described in paragraph 4.6 of the CPS.

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

4.7 Certificate Re-key

Certificate re-key is never allowed.

4.8 Certificate Modification

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

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). Certificates revocation is irreversible and not retroactive.

The certificate suspension 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.

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 or non-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 subordinate CA used for issuing the certificate;
9. the CA is made aware that the subscriber organization ceased its activity.

The revocation must be authorized by the management and must be published within 24 hours after the revocation authorization.

4.10 Certificate Status Service

The status of the non-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].

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 trust service controls must comply with:

- EN 319 411-1 NCP+ policy for non-qualified 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 CPS.

5.2 Procedural controls

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

5.3 Personnel controls

Refers to paragraph 6.2 of the CPS.

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

5.6.1 Root CA

Root Ca is renewed at least 5 years before the end of the validity. The renewal procedure is described within the CPS and follow the key ceremony procedure.

5.6.2 SubCA

Subordinate CA is renewed at least 5 years before the end of the validity. The renewal procedure is described within the CPS 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 certification services recovery in case of a disaster, corrupted servers, software or data.
A backup copy of data, applications and any other file necessary for a complete service recovery is performed daily. All 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 Subordinate CA

Clause 6.1.1 shall apply.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Root CA

The Root Ca key pairs are generated and managed into an HSM, certified according to FIPS PUB 140-2 Level 3 or Common Criteria (ISO 15408) at EAL 4.

6.2.2 Subordinate CA

The Subordinate Ca key pairs are generated and managed into an HSM, certified according to FIPS PUB 140-2 Level 3 or Common Criteria (ISO 15408) at EAL 4.

6.3 Other Aspects of Key Pair Management

All the certificates are archived by Intesi Group.

6.4 Activation data

Only authorized TSP operators can access to CA activation codes. The activation codes are stored in a safe place. Any 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 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.

Non-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.

As for cryptographic algorithms, minimum length of keys, key parameters and hashing functions, the CA 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 CP and in the related CPS, 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 CP and in the related CPS.

8.5 Actions taken as result of deficiency

Security violation will be prosecuted as per the rules of law currently in force.

Should the violation have possibly exposed at risk the CA and / or the TSS private key, relevant provisions apply.

8.6 Communication of results

Significant deviations from the procedure or severe security breaches are reported to TSP 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 (CP) 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 CP and relevant stipulations in the related CPS.

9.6.2 Registration Authority

The LRA shall operate in compliance with this CP and relevant stipulations in the related CPS.

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 “CPS” 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 CP 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 CP 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 CPS.

9.13 Governing Law

This CP 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 CPS, 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 CP and CPS apply.