INTESI GROUP

Certificate Practice Statement

Ver. 1.2

01/08/2023

History

ID	Changes	Rev.	Data	Author	Approval
CPS	First release	1.0	30/03/17	F.Barcellini	G.Damiano
CPS	Modification to paragraphs 9.3.3 and 9.4	1.1	20/07/18	F.Barcellini	G.Damiano
CPS	Modification to paragraphs 3.2.1, 3.3, 4.1.1, 4.2.2, 4.7, 5.2, 5.5.4	1.2	01/08/2023	D.Saccò	F.Barcellini

Index

1 INTRODUCTION

1.1 Overview

This Certificate Practice Statement (CPS) describes the technical, security and organizational requirements implemented by Intesi Group S.p.A. (hereafter referred to also as “Intesi Group”) applicable to the Advanced Electronic Signature certificates:

- root CA issuing subordinate CA certificates for Advanced CA services;
- subordinate CA issuing End User Advanced Electronic Signature certificates;
- End User certificates, CRL and OCSP services;

The trust services comply with the relevant requirements of the eIDAS regulation (Regulation (EU) N°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.

This CPS conforms to the public specification [RFC 3647] and refers to the Certificate Policy whose OIDs are specified in relating CP, hereafter referenced as “related CP”.

1.2 Document Name and Identification

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

This document is public and freely downloadable from the Intesi Group web site (http://www.intesigroup.com).

1.3 PKI participants

1.3.1 Intesi Group as Time Stamping and Certification Authority

Intesi Group as Advanced Electronic Signature certification authority 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

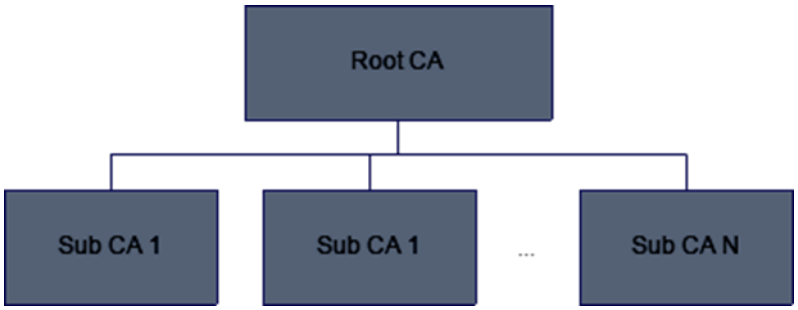
Telephone: +39 02 6760641

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 CA infrastructure is based on a two-level hierarchy, as shown in the following diagram:



The Root CA is used for issuing certificates to sub CAs and related CRLs whereas end-entity certificates are issued only by Sub Cas, each dedicated to a specific trust service.

The Root CA is described below:

SubjectDistinguishedName	SubjectKeyId	Not Before	Not After
CN=Intesi Group Cloud Root CA, O=Intesi Group, C=IT	EB:F2:B4:4A:02:21:EE :A8:FF:19:7A:FA:8F:A D:17:46:35:D7:36:45	Mar 10 15:49:43 2017 GMT	Mar 5 15:49:43 2037 GMT

The sub CAs maintained by Intesi Group is described as follow:

SubjectDistinguishedName	SubjectKeyId	Not Before	Not After
CN=Intesi Group Advanced Cloud Signature CA, O=Intesi Group, C=IT	17:44:95:BD:6C:31:08:77 :24:E8:01:C7:BD::CD:45: 3B:5D:17:28:74	Mar 10 15:53:34 2017 GMT	Mar 8 15:53:34 2027 GMT

1.3.2 Local Registration Authority

The Local Registration Authority (RA) is a third party delegated by Intesi Group to carry out:

- subjects identification and authentication (I&A);
- transmission to the CA of the identified subject information.
- registration of the applicant data and certificate issuance authorization.

- validation and management of any suspension, unsuspension and revocation request.

LRAs are periodically assessed by Intesi Group to verify the respect of the agreements taken.

1.3.3 Subscribers or applicants

In this CPS 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 advanced electronic signature certificates.
- legal persons holding advanced electronic seal certificates.

1.3.5 Holders

A holder is an advanced electronic signature certificate or an advanced electronic seal certificate user. For advanced electronic signature is the certificate subject, for advanced electronic seal is the certificate user.

1.3.6 RAO

RAOs are involved in the process of identifying, collecting and recording user's personal data and responsible for the transmission of the documentation to the CA.

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

At the end of the training course, operators will obtain the Intesi Groups RAO application's access privileges. The access privileges assignment is under the control of the CA.

1.3.7 Relying parties or users

The "Relying Parties" are the subjects relying on the information contained in the certificates issued according to this CPS.

1.4 Certificate Usage

See the corresponding CP stipulations.

The certificates **policy** issued under this CPS are identified by the **OIDs** specified in clause 1.2 of the relating CP.

1.5 Policy Administration

This CPS is developed, reviewed and updated by Intesi Group and is published after being approved by the Intesi Group management.

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

1.6 Definition and Acronyms

Acronym	Definition
CA	Certification Authority
CAO	Certificate Authority Officer
CP	Certificate Policy
CPS	Certificate Practice Statement

Acronym	Definition
CRL	Certificate Revocation List
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
PKI	Public Key Infrastructure
RAO	Registration Authority Officer
RFC	Request For Comments
TIN	Tax Identification Number
TSA	Time-Stamping Authority
TSU	Time-Stamping Unit
TLS	Transport Layer Security
TSP	Trust Service Provider

2 PUBLICATION AND REPOSITORY

2.1 Repository management

The Intesi Group repositories are:

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

The repositories are available 24 hours a day, 7 days a week and are designed to guarantee 99.9% 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:

- the Certificate Policy (CP)
- the Certificate Practice Statement (CPS).
- service Terms & Conditions.
- CRL – Certificate revocation lists.
- Various forms.

2.3 Time and frequency of publications

The documentation updating, and publication frequency is established by Intesi Group's internal processes. The version valid is the latest version available on the certification service website (www.intesigroup.com). For the CRL issuance frequency refer to section 4.

2.4 Access control

Documentation and CRLs are freely accessible and does not require authentication.

3 IDENTIFICATION AND AUTHENTICATION

Intesi Group I&A procedures comply with ETSI EN 319411-1 requirement.

3.1 Naming

3.1.1 Types of names

All the advanced electronic signature certificates issued under this CPS are identified by an X.500 Distinguished Name (DN).

3.1.2 Need for names to be meaningful

The names used under this CPS and the applicable CP shall be meaningful as identifying certificate Subjects.

3.1.3 Rules for interpreting names

Names respect X.500 standard.

3.1.4 Uniqueness of names

The subjectDistinghishedName uniqueness is granted by a unique code inserted into the dnQualifier field (OID 2.5.4.46).

3.1.5 Recognition, authentication, and role of trademarks

The Subject 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.

3.2 Initial Identity Validation

Initial Identity validation is part of the certificate application process described in chapter 4.1. Initial identity validation procedures for subject, subscribers and organizations comply with provisions of the CPS and are fully detailed in Intesi Group internal documents.

3.2.1 Proving possession of private key

The private key is generated within Intesi Group's infrastructure, so proof-of-possession is not required.

3.2.2 Authentication of organization identity

A Subject must demonstrate the organization's powers of attorney by providing the CA (or the RAO) with appropriate documentation issued by an authoritative body such as, for example, an official certification issued by a chamber of commerce.

3.2.3 Identification and authentication requirements for an individual

The RAOs (see 1.3.6) operate according to the identification procedures applied by Intesi Group:

- Face-to-face identification.
- Identify mobile app identification.
- Federated Identity.

3.2.4 Face-to-face identification and registration

A RAO must physically meet a subject and must verify the subject's identification documents. The documents are:

- Identity card number.
- Passport.
- Documents that are legally recognized as identification documents.

If the subject requests the insertion of professional qualifications, role and organization must present documentation to demonstrate the authorization to use the qualifications required.

RAO checks document validity. If the verification is successfully executed, the Identification officer completes the procedure doing:

- Subscriber's personal data registration using the Intesi Group RAO portal. A detailed list of the information inserted is shown in section 0..
- make a digital copy of subject identification document.
- Printing a copy of the contract and terms and conditions.

If the user provides complete and valid information, the RAO will approve the signature or seal certificate issuance.

If the user provides incomplete information, invalid or missing identification documents or does not sign the contract, the RAO will not approve the signature or seal certificate issuance.

3.2.5 Identify mobile App identification

The user uses IDentify mobile app to execute a self-service identification process:

- collect subject personal data;
- make a digital copy of subject identification document (passport, identity card and tax identification number).
- confirm subject personal data in a self-service video to complete identification materials and aimed to avoid identification fraud.

The collected data are sent, by the IDentify App, to a remote server where are securely stored. A Registration Authority Officers, using the Registration Authority Officer portal, evaluates the identification data and accept or reject the collected data. In case of rejection, the user is notified through the IDentify App and advised on what data needs correction. In case of acceptance, the operator completes the registration and authorize the certificate enrolment.

The IDentify user identification process is used only for long-term certificates.

3.2.6 Identification and registration through IDentify Web

This identification takes place through a videocall between a RAO and a Subscriber using the Intesi Group videoconference application (Identify Web). Before the video meeting, Intesi Group informs the Subscriber with all necessary instructions to access it and to successfully complete the identification.

The subscriber shall own a device (PC, Smartphone or Tablet) equipped with a webcam and a audio system. On the agreed date the Subscriber and the RAO connect to IDentify Web and start the Identification. The RAO asks a list of questions aimed to verify the actual presence of the subject and the authenticity of the identification documents presented. The RAO can consider not admissible a document presented by the Subscriber if the document is not valid (expired or issued by an invalid public body) or suspect it is not authentic. Furthermore, the RAO may not start or interrupt the identification process if the audio and video quality is poor or not adequate. 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.

3.2.7 Federated Identity

The Time4Mind portal can delegate the authentication to an external Trusted Identity Provider.

When the Trusted Identity Providers use an authentication granting at least a Level of Assurance (LoA) 3 of the ISO-IEC 29115, implemented for example by the Italian SPID layer 2, and use a Trusted Identity Protocol like, for example, SAML or bankID, the CA can avoid the subject identification considering the data provided by the Identity Provider federated and trusted.

In this case the subject identification data stored by the CA are the responses received from the Trusted Identity Provider containing the subject data. Other subject identification data like copy of personal document must be stored by the Trusted Identity Provider.

The information taken from the answers received from external identity providers are immediately stored into the registration database. The certificate issuance is automatically authorized.

Intesi Group accepts authentication transmitted by means of trusted and secure authentication protocol like:

- SAML Identity Provider that can be managed by a private company or can be part of a national authentication system like, for example, the Italian SPID (Sistema Pubblico di Identità Digitale).
- BankID Protocol the public citizen authentication system adopted by the Swedish government.

3.2.7.1 SAML Identity Provider

The user login is managed by the OAuth2 Time4Mind login pages, which contains the policy rules to recognize the username and redirect him / her to the corresponding SAML Identity Provider. The user is redirected to the SAML Single Sign On page to authenticate himself / herself. The Single Sign On platform redirect the user to Time4Mind platform returning a signed SAML assertion containing the user's personal data:

- First name.
- Last name.
- Email address.
- Employer identifier.
- Country code.

The user personal data are required to register and generate a new digital certificate. Time4Mind verifies the SAML assertion signature and checks if the user already owns a valid signature certificate. The user is automatically registered, a new digital certificate is generated under the Advanced Cloud Signature root certificate.

3.2.7.2 BankID Identity Provider

The user login is managed by the OAuth2 Time4Mind login pages, which contains the policy rules to recognize the username and redirect him / her to the corresponding BankID Identity Provider. The

user is redirected to BankID login page to authenticate himself / herself. BankID platform send back to Time4Mind platform an XML assertion containing the user's personal data:

- First name.
- Last name.
- Email address.
- Country code.

The user personal data are required to register and generate a new digital certificate. Time4Mind verifies BankID response and checks if the user already owns a valid signature certificate. The user is automatically registered, a new digital certificate is generated under the Advanced Cloud Signature root certificate.

BankID authentication certificates must be supplied to used Intesi Group to authorize Time4Mind platform to connect to BankID services.

3.3 Identification and Authentication for Re-Key Requests

Re-key requests are not available. Issuance of new certificate for the same key, is not allowed by Intesi Group Advanced Cloud CA.

3.4 Identification and Authentication for Revocation Requests

Suspension or revocation requests must be submitted through the CA portal and require the username and password supplied after the registration;

If the user does not remember or has lost the authentication information, he can submit revocation requests by sending an email to Intesi Group support as described in paragraph 4.9.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Advanced certificate application can be submitted by:

- the subject, for certificates issued to natural persons.
- a subscriber, allowed to represent the legal persons.

The subject can submit certificate application directly to Intesi Group RAOs or to a RAO of an authorized LRA.

4.1.2 Enrolment process and responsibilities

The registration process must be carried out after the identification process (see par. 0) and includes the following steps:

- registration of personal data;
- acquisition of the signed contract with terms and conditions;
- sending the collected information to the Intesi Group;

The registration process requires the following different actors:

- the Subscriber must:
  1. read and accept the privacy policy;
  2. provide the required data for registration and present the require documentation for the identification;
  3. sign a copy of the contract with Terms and Conditions;
  4. read and accept this CPS;

- the RAO must:
  1. identify the subject;
  2. acquire the privacy policy acceptance;
  3. register user data;
  4. send to the CA an Identification documents copy;
  5. approve certificate issuance;
- the CA:
  1. issues advanced electronic signature certificates;
  2. stores the identification data;
  3. disseminates certificates and seals status information;

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

4.2 Application processing

The application processing takes place through the following steps:

- The RAO performs the identification process described in 3.2;
- The subscriber must:
  1. read and accept the Intesi Group's privacy policy;
  2. read and accept the contract and relating Terms and Conditions;
  3. read this CPS;
- The RAO, through Intesi Group’s RAO portal, register user personal data and send to the CA copies of the documentation collected during the Identification. The RAO must approve or deny the certificate request.
- The CA, having received and validated the documentation, communicates to the user (e.g. through and e-mail) the request approval and the certificate issuance procedure.

- The subscriber, using the credentials provided with the procedure described in par. 4.2.2.1, must authenticate to the Intesi Group Web portal or Mobile App and execute the issuing procedure following the steps proposed (described in section 4.3). The holder, through the features provided by the portal will perform:
    1. The credential access PIN definition and (where present) the OTP token customization.
    2. The keys generation on the QSCD device and the certificate issuance on the PKI Intesi Group. The communication between QSCD and PKI takes place within the Intesi Group infrastructure and is secured using the TLS protocol and SSL authentication.

4.2.1 Subject information required

The advanced electronic signature certificate request requires the following mandatory information:

- Name and surname;
- Birth date, birth city, birth state and birth country;
- Country, state, city and address of residence;
- mobile phone number;
- email address;
- Identification document data (document number, release date);

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;
- Attestation or evidence demonstrating the authorization to act on behalf of the legal person.

4.2.2 Registration and authentication

User data registration is executed at the end of the identification process described in paragraph 3.2.

Intesi Group provides a web application called pkra (reachable at the url https://pkra.time4mind.com) allowing RAO to execute the registration process through the following steps:

1. After successful authentication, the RAO must select the certificate profile to be authorized for issuance.
2. Then the RAO must fill a form with the applicant data.
3. At the completion, the application requires the acquisition of a digital copy of the identification documents. For this purpose, the operator must use a mobile App developed by Intesi Group (called Identify) installed on a smart device (mobile phone or tablet).
4. The RAO digitally sign and send to the CA's servers the collected data. The signature is applied by means of a remote signature credential provided upon the RAO mandate reception.
5. The CA server automatically checks the data received and, if they result complete and correct, saves them on the internal repository where they will be stored in accordance with the current legislation requirements.
6. The RAO can now complete the registration defining, where applicable, the type of OTP token to be associated with the applicant credential. Finally, the RAO can approve the certificate issuance.

The registration completion is confirmed to the applicant with an email containing:

- A unique code called "security code" that will be required to start the procedure for issuing the advanced electronic signature certificates for signature or seal.
- A link that automatically starts the certificate issuance.

After the email reception, the user can execute the certificate issue procedure.

4.2.2.1 Subject authentication credentials

The holder must authenticate to the Intesi Group's user portal (reachable at the URL https://user.time4mind.com) using basic credentials provided by the RAO during the identification or self-generated filling out the "Registration" tab of the authentication form of the time4mind portal.

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

The basic credentials only 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 portal and must be provided with remote signing credentials to execute the registration procedure.

The RAOs authentication credentials are generated by Intesi Group operators following internal procedures.

4.2.2.3 LRA authentication credentials

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.
- a remote signature credential to sign the documentation sent.

Authentication and signature certificates are generated and distributed by Intesi Group operator following internal procedures.

4.2.3 Registration from Federated Identity

The registration is automatically done using data coming from a trusted federated identity in an electronically sealed form (for example a SAML assertion).

Every registration is done only after having informed the subject and having obtained its approval to proceed.

4.3 Certificate Issuance

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 OTP provided by the RAO upon registration.
- Users using Mobile Valid App OTP tokens, before starting the certificate issuance procedure must be ensure that the App is installed on their mobile device. 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 Valid 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" and complete the authentication inserting the "security code" received after the registration.

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 in addition to the PIN is required to enter an OTP generated by the token that will be coupled with the signing credential.

Upon receipt of the information, the Time4Mind server starts the key pair generation process on the QSCD device and the certificate issuance with the internal PKI. At the end of this process the signing credential is created.

The certificate issuance process completes sending to the holder a confirmation email containing a revocation code that can use to send to Intesi Group customer care a request for revocation or suspension.

4.4 Certificate Acceptance

4.4.1 Certificate acceptance

The certificate is considered accepted after being delivered to the subject.

4.4.2 Publication of the certificate by the CA

Every certificate is stored into the CA database and not made public.

4.4.3 Notification of Certificate issuance by the CA to other entities

An e-mail containing a confirmation message is sent to the holder.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

The holder must:

- be the sole private key user.
- maintain the exclusive 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 certificate revocation if there is reason to believe that the authentication data (e.g. PIN code) have been compromised;
- ask for the certificate revocation if the data contained in are changed or incorrect.

4.5.2 Relying Party public key and Certificate usage

Who rely on certificates information (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 certificate CRLDistributionPoints and AuthorityInformationAccess extensions.

The verification must consider the certificate status at 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.

4.5.3 User notice

The Subscriber can request the inclusion of custom user. The CA is not responsible for any damage caused by the misuse of the certificate.

4.6 Certificate Renewal

The subscriber can execute a certificate renew if the certificate is not yet expired and only within the ninety days before the certificate expiration. The certificate renewal always includes a new key pair generation.

4.6.1 Procedure to process renewal request

The Holder can start the procedure from its Valid 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. defined a new pin.

Obtained this information, CA generates new key pair and new certificate using the same procedure used for the first generation (see 4.3).

4.6.2 Notification to the subscriber

The notifications sent to the holder are:

- Ninety 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.

- After the certificate renewal process is completed, a confirmation message containing a revocation code that will be required to revoke or suspend the certificate. When present a copy of the message is sent to the third party.
- If the user left expires its certificates, it will receive an email informing about the certificate expiration and the instruction on how to apply for a new certificate.

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 CA to other entities

Refer to section 4.4.3.

4.7 Certificate Re-key

Certificate re-key is not allowed. Issuance of new certificate for the same key is not allowed by Intesi Group Advanced Cloud CA.

4.8 Certificate Modification

The certificate modification is not allowed by Intesi Group Advanced Cloud CA. To modify a certificate a user must revoke the certificate and issue a new one according with the procedure described in section 4.9 and 4.3.

4.9 Certificate Revocation and suspension

4.9.1 Circumstances for revocation

No additional stipulations.

4.9.2 Who can request revocation

The certificate may be revoked on request of:

1. The certificate holder.
2. The “certification authority”.

4.9.3 Procedure for revocation request

A subject can suspend, un-suspend or revocation a certificate:

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

Revocation request are processed using the process described below.

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 the certificate to be revoked;
3. invoke the “revocation” function and confirm the request.

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

4.9.3.2 Revocation by means of Intesi Group RAO

Any RAO operator can revoke a certificate using the PkRA RAO requested from:

- Certificate holder;
- CA;

The holders who wish to revoke a certificate must present the revocation form, downloadable from the Time4Mind portal, filled in all its parts and a personal document copy.

A RAO using the provided information can:

1. search the user;
2. Check the data provided.;
3. request the certificate revocation or the certificate suspension.

If the information provided for a revocation are wrong or incomplete, the RAO will only suspend the certificate.

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 holder.

4.9.3.3 Customer care revocation

Only in case of time4mind revocation service is unavailable, users and RAOs can submit a revocation request to the Intesi Group's customer care sending an email containing the revocation form to the address:

certificate@intesigroup.com

When the sender is a RAO, the email must be sent within eight hours of revocation request reception.

Any email must contain a filled revocation form including the revocation code and a digital copy of the identification document. In case of missing information the certificate will be only suspended

and then the user has ten days to proceed with the certificate revocation or un-suspension. At the end of this period, if nothing has done, the certificate will be automatically un-suspended.

Note, for security reason the sender email address must be the same of the email address registered into the Time4Mind portal. Any email received from an unknown sender will be rejected.

A confirmation email of the certificate revocation or suspension is sent to the certificate subject.

4.9.4 Revocation request grace period

CA performs revocation to ensure that the time needed to process the revocation request and to publish the revocation status (updated CRL) is be as reduced as possible.

4.9.5 Time within which CA must process the revocation request

The revocation request is immediately executed. If the operation completes successfully, the revoked certificate is inserted in the CRL within 6 hours and not later than 24 hours after the operation. If the revocation fails, the certificate status is not changed and the holder is informed by an email.

4.9.6 Revocation checking requirement for Relying Parties

Refer to section 0.

4.9.7 CRL issuance frequency / OCSP response validity period

4.9.7.1 *CRLs*

The CRL is always re-generated and re-published every 6 hours. The CA can force a new CRL issuance before 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 CPS).

4.9.8 Maximum latency for CRLs

The time between the revocation or suspension request and new CRL issuance is at maximum six hours.

4.9.9 On-line revocation status checking availability

The CA 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. the CA receive a revocation request without necessary information to authenticate the requester.
2. the owner, the subscriber or the certification authority acquire elements of doubt about the certificate validity;
3. there are doubts about the key storage device or authentication system safety;
4. is required an interruption of the certificate validity.

4.9.13 Who can request suspension

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

4.9.14 Procedure for suspension and un-suspension requests

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

4.9.15 Limits on suspension period

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

4.10 Certificate Status Service

The advanced electronic signature certificates status is disseminated through the CRLs, in conformance to RFC 5280, via HTTP protocol [RFC7230] on the server **crl.time4mind.com**.

The certificate status is also available through the OCSP (On-line Certificate Status Protocol) in compliance with the specification [RFC6960].

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 available 24 x 7.

4.11 End of Subscription

The subscription ends when the certificate expires or is revoked, unless there are different conditions that may be stipulated in contracts.

4.12 Key Escrow and Recovery

The key recovery is available for CA keys in the case of unintentional cancellation or HSM fault. For this purpose, the CA keeps a backup of CA key pair and recovery is performed according to the HSM certification requirements and under dual control.

5 FACILITIES, MANAGEMENT, AND OPERATIONAL CONTROLS

The management, operational, procedural, personnel and physical (non-technical security) controls used by Intesi Group comply with the technical standards EN 319 411 and with 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 available only to Intesi Group personnel, to auditors and to the Italian Supervisory Body.

5.1 Physical security

All computer systems used for the qualified trust services provision 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;
- a video surveillance
- 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 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 Intesi Group 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.

5.3 Personnel security controls

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

The roles assigned to personnel are defined in accordance with the ETSI EN 319 401.

5.4 Audit logging procedures

5.4.1 Type of events recorded

The events logged and stored 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 equipped with event logging systems.
- Data center physical access.
- QTSP server area physical access.
- TSP systems logical access.
- Certificate life cycle events.

- Clock synchronization events.
- Software update and release.

For each event, information about the type, date and time of occurrence is also logged. The time source used is the system clock kept aligned with the NTP service.

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.

5.4.4 Protection of audit log

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

The log file access is allowed only to 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 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 and is 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 CA service;
- Identifications data, digital copy of identification document and contract approval.

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

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

5.5.2 Retention period for audit log

Archived records are kept for 20 years.

5.5.3 Protection of archive

The archive system continuously checks the information consistency and immutability. In case of inconsistencies fires an alarm to the monitoring system.

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

5.5.4 Archive backup procedures

The archives are kept at Intesi Group.

Archives are protected with encryption and have access limited to allowed Intesi Group personnel.

Archives are backuped daily.

5.5.5 Requirements for time-stamping of records

The time-stamp date is obtained through the system date. The System date is synchronized with NTP Service that 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 Subject or Subscriber, may access to related records and other information related to the Subject by contacting Intesi Group.

5.6 Renewal of CA Key

5.6.1 Root CA

The Key ceremony procedure shall be applied.

5.6.2 Sub CA

The Key ceremony procedure 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 are available as internal document.

These procedures comply with ISO/IEC 27001 standard. All incident and/or compromise events are documented and any associated record is archived as described in section 5.5 of this CPS.

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

Intesi Group establishes the necessary measures to ensure full and highly automated certification services recovery in case of a disaster, corrupted servers, software or data. Any measure complies with the ISO/IEC 27001 standard.

Disaster recovery site and production site are far away to avoid that a disaster would corrupt resources at both sites. Secure and fast communications are established between the two sites to ensure data integrity.

Disaster recovery infrastructure and procedures are tested every year with witnessing of at least one CSP Board member.

5.7.3 Entity private key compromise procedures

CA private key(s) compromising implies immediate CA certificate revocation. In this case Intesi Group will additionally take the following measures:

- stop the compromised services.
- revoke all certificates became unreliable;
- 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 CA private key corruption and revoked the CA certificate, Intesi Group will generate a new key pair and new CA certificate and re-issue all end user certificates that were revoked.

5.7.4 Business continuity capabilities after disaster

Intesi Group 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 measures comply with the ISO/IEC 27001 standard. A Contingency Plan has been implemented to ensure business continuity and is available as internal document.

5.8 CA termination

In case of CA termination, the TSP will take the following measures:

- at least 30 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;
- at the date of termination, destroy its private CA keys unless the service is taken over by another TSP in compliance with the applicable legislation.

6 TECHNICAL SECURITY CONTROLS

The security measures taken by Intesi Group to protect the whole infrastructure comply 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

Root CA certificate is generated by two Intesi Group operators following the Intesi Group's Key Ceremony procedure. Execution of the procedure (or “key ceremony”) is recorded and kept for 20 years.

The key pair used is generated inside an 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 140-2 Level 3 and Common Criteria (ISO 15408) at EAL 4 or higher.

6.1.1.2 Sub CA

Sub CA certificate is generated by two Intesi Group operators following the Intesi Group's Key Ceremony procedure. Execution of the procedure (or “key ceremony”) is recorded kept for 20 years.

The key pair used is generated inside an 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 140-2 Level 3 and Common Criteria (ISO 15408) at EAL 4 or higher.

6.1.1.3 Advanced Electronic Signature Certificate

The subject's key pair is generated on a QSCD certified device located into the Intesi Group data center and is recorded by the internal auditing system.

6.1.2 Private key delivery to subscriber

Private keys are securely generated and stored into a QSCD device located into the Intesi Groups' server room. Access to the private can be done by means of the QSCD interfaces 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

6.1.4 CA public key delivery to Relying Parties

The Root CA public keys are published on the CA web portal (www.intesigroup.com).

6.1.5 Key sizes

The Root CA and Sub CA keys are generated with RSA algorithm and are 4096 bits length.

The Subject are generated with RSA algorithm and are 2048 bits length.

6.1.6 Public key parameters generation and quality checking

Public key parameters generation and checking during CA key pair generation are implemented according to the applicable CPS.

Public Key generation procedure is regularly reviewed to grant maximum available security level.

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 Sub CA

The Sub CA 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.

6.1.7.3 Advanced Electronic Signature certificates

The Advanced Electronic Signature Certificate includes KeyUsage extension with the appropriate values which indicate the purpose of the private key:

- Non-repudiation

For further details see chapter 7.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The private keys used by the Root CA is kept inside an HSM (Hardware Security Module) with security certification in accordance with FIPS PUB 140-2 Level 3 and Common Criteria (ISO 15408) at EAL 4.

The certificate private keys 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

The CA private keys can be accessed by two operators simultaneously authenticated.

The Advanced Electronic Signature private keys access can be done by the holder using the authentication credential only using the QSCD device interfaces.

6.2.3 Private key escrow

Key escrow is never allowed.

6.2.4 Private key backup

The CA keeps an encrypted backup copy of CA 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 at least two operators ("dual control").

Subscriber's key back-up and key recovery are not allowed except for the purpose of disaster recovery as stated by this CPS and the applicable CP.

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.

6.2.8 Method of activating private key

CA's private keys are activated using the HSM procedures and always occur under the dual control of two operators.

The subject can activate its signature private keys using the authentication credentials defined during the certificate issuance (see section 0) 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 are deactivated using the HSM procedures and always occur under the dual control of two TSP operators.

The subject can deactivate its signature private keys 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 keys are destroyed through secure deletion from the HSM and any backup media. The CA key destruction follows an internal procedure and is executed under dual control of two authorized operators.

User’s private key are automatically deleted at the end of the related certificate validity period.

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.

6.4 Activation data

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

End User private keys activation data are defined by the Subject during the enrolment phase. End users are responsible for the secure management and protection of private activation data. See section 4.1.2 of the CPS and the applicable CP for further details.

Intesi Group enrolment process ensures the subscriber's certificate activation data using TLS/SSL secure channel and saving all the information in encrypted form.

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 and with ETSI EN 319 411-2.

Intesi Group internal procedures are ISO/IEC 27001 certified.

Detailed descriptions of implemented computer security controls are available as internal document(s).

6.6 Life cycle technical controls

The software development supporting the Intesi Group trust services is executed conforming with the quality management system 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).

6.7 Network security controls

Network security controls are implemented in compliance with the requirements contained into the standard ETSI EN 319 411-1 and with ETSI EN 319 411-2 and includes firewalls, network intrusion detection, secure communication between PKI Participants, anti-virus protection, website security, databases and other resources protection from outside boundaries, etc. Detailed descriptions of implemented network security controls are available as internal document(s).

6.8 CA and Time-stamping

All the computer systems used 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.

7 CERTIFICATE AND CRL PROFILE

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

Minimum length of keys, key parameters and hashing functions, the CA conforms to: ETSI TS 119 312.

7.1 Certificate profile

7.1.1 Intesi Group Cloud Root CA

Field	Value
Version Number	V3
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
IssuerDistinguishedName	CN = Intesi Group Cloud Root CA, O = Intesi Group, C = IT
Validity	<20 years>
SubjectDistinguishedName	CN = Intesi Group Cloud Root CA, O = Intesi Group, 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)	<included, KeyID>
Subject Key Identifier (SKI)	<included>
KeyUsage	critical: keyCertSign, cRLSign

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

7.1.2 CA for Advanced Electronic Signature

Field	Value
Version Number	V3
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
IssuerDistinguishedName	CN = Intesi Group Cloud Root CA, O = Intesi Group, C = IT
Validity	<10 years>
SubjectDistinguishedName	CN = Intesi Group Advanced Cloud Signature CA, O = Intesi Group, 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)	<Same value as the Root CA SKI extension>
Subject Key Identifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: keyCertSign, cRLSign
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>

Field	Value
CRLDistributionPoints (CDP)	http://crl.time4mind.com/Intesi/CloudRootCA.crl

7.1.3 Certificate for Advanced Electronic Signature

Field	Value
Version Number	V3 (2)
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
IssuerDistinguishedName	CN = Intesi Group Advanced Cloud Signature CA, O = Intesi Group, C = IT
Validity	<Max 5 years>
SubjectDistinguishedName	E=<Subject Reference Email>, dnQualifier=<Intesi Group Internal Code>, CN=<Name Surname>, G=<Subject name>, SN=<Subject surname>, O=<Subject reference organization>, C=<Subject country address>
SubjectPublicKeyInfo	<RSA public key of 2048 bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**
Basic Constraints	<not included>
Authority Key Identifier (AKI)	<Same value as the Sub CA SKI extension>
Subject Key Identifier (SKI)	<included>
KeyUsage	Critical: non-repudiation
Extended Key Usage (EKU)	<not included>
CertificatePolicies	PolicyOID = 1.3.6.1.4.1.48990.1.2.1.1 CPS-URI = http://www.intesigroup.com/en/documents
SubjectAlternativeName (SAN)	<not included>
CRLDistributionPoints (CDP)	http://crl.time4mind.com/Intesi/CloudfeaCA.crl

Field	Value
Authority Information Access (AIA)	http://ocsp.time4mind.com
QcStatement	

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)

The CRL is signed using the hashing algorithm sha256WithRSAEncryption (1.2.840.113549.1.1.11). Moreover, in correspondence with each item of the CRL there is a *reasonCode* extension to indicate the reasons for suspension or revocation.

8 COMPLIANCE AUDIT

The technological infrastructure, physical and logical security controls, the operating procedures, and the personnel employed in providing Certification services described in this CPS conforms to the EU directive on electronic signatures.

Intesi Group is a Qualified Trust Service Provider (QTSP) according to European legislation; as such, Intesi Group is under supervision by AgID (the Italian supervision body) and is required to perform periodic internal audits and periodic conformity assessment by a Conformity Assessment Body accredited according to the eIDAS Regulation.

8.1 Frequency or circumstances of assessment

A Conformity Assessment Body enabled to assess the conformity to eIDAS Regulation does an assessment at least every 12 months.

The internal audits are carried out in accordance with a schedule.

8.2 Identity and qualification of assessor

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

8.3 Assessor's relationship to assessed entity

No relationship shall exist between the CA 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 CA operations.

8.4 Topics covered by assessment

Audits performed by external assessors verify the compliance of Intesi Group and the certification services to the applicable requirements of the eIDAS Regulation.

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

8.5 Actions taken as result of deficiency

In the case of non-compliances, the CA will adopt all the necessary corrective measures within the defined period to avoid fines or accreditation revocation.

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

8.6 Communication of results

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

Relevant incidents will be notified to the interested parties according to the internal incident procedure.

9 OTHER BUSINESS AND LEGAL MATTERS

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

In the case of a discrepancy between this CPS and the separate “Terms & Conditions” document, “Terms & Conditions” will take precedence.

9.1 Service fees

The fees are published on the TSP web site www.intesigroup.com and are subject to change without notification. 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 CPS:

- 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

Provisions relating to the treatment of confidential information that PKI Participants may communicate to each other, and relating to the scope of what is considered as information within or not within the scope of confidential information, to the responsibility to protect confidential information, and to disclosure conditions are provided within the CPS.

All confidential information is processed by the CA 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/privacy-policy/

9.5 Intellectual property rights

Within the service regulated by this CPS, the CA does not collect and does not process sensitive data nor judicial data (with reference to article 4 of the aforesaid Decree [DLGS196]). This CPS 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 CA shall:

- operate in compliance with this CPS;
- identify the subscriber as described in this CPS;
- issue and manage the certificates as described in this CPS;
- 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 CPS 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.

9.6.2 Registration Authority

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

Not applicable for 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

Except as expressly provided elsewhere in the CPS, the applicable CP and in the applicable legislation, Intesi Group acting as TSP disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except that it came from an authorized source), and further disclaims any and all liability for negligence and lack of reasonable care on the part of Subscribers and Relying Parties. Intesi Group does not warrant “non repudiation” of any Certificate or message. Intesi Group does not warrant any software.

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 CPS 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 CPS at any time whatsoever without prior notification.

9.12 Dispute Resolution Provisions

The Subscribers can submit their claim or complaint on the following email:

tsp@intesigroup.com.

Complaints received by Intesi Group will be treated by Intesi Group internal services to resolve any dispute promptly and efficiently.

Any controversy that cannot be solved by Intesi Group internal services shall be submitted to the exclusive jurisdiction of the Milan Court, except for the conditions that apply in case the Subscriber can be qualified as Consumer according to Italian Legislative Decree 206/2005.

9.13 Governing Law

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

Other contracts in which this CPS is incorporated by means of reference, may contain distinct and separate clauses with respect to applicable law

9.14 Compliance with Applicable Law

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

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.