INTESI GROUP

Trust Service Practice Statement

Ver. 1.9

20/07/2018

History

ID	Cambiamenti	Rev.	Data	Autore	Approvazione
TSPPS	Prima versione in italiano.	1.4	15/09/17	F.Barcellini	G.Damiano
TSPPS	Revisione generale del documento	1.5	22/11/17	F.Barcellini	G.Damiano
TSPPS	Corretta la formattazione. Modifiche ai paragrafi 1.3.1; 1.3.4; 3.1.4; 3.2.4; 3.2.5; 4.2; 4.5.3; 6.2.2; 6.2.8; 6.2.9; 6.2.10; 7; 8.6.	1.6	20/12/17	F.Barcellini	G.Damiano
TSPPS	Modifiche al paragrafo 3.1.4.	1.7	17/01/18	F.Barcellini	G.Damiano
TSPPS	Modifica al paragrafo 3.1.3, 3.2.3, 3.2.6 e 3.2.7	1.8	13/03/18	F.Barcellini	G.Damiano
TSPPS	Modifica paragrafi 3.2.3, 3.2.7, 3.4, 9.3.3 e 9.4	1.9	20/07/2018	F.Barcellini	G.Damiano

Indice

1. INTRODUZIONE

1.1 Quadro generale

Il presente Manuale Operativo (TSPPS) descrive i requisiti tecnici, di sicurezza e di organizzazione adottati da Intesi Group S.p.A. (di seguito denominata anche “Intesi Group”) applicabili a tutti i seguenti Servizi Fiduciari:

- emissione a persone fisiche di certificati di firma qualificata;
- emissione a persone giuridiche di certificati per sigilli qualificati;
- emissione certificati di marcatura temporale qualificata;
- generazione certificati e CRL emessi dalle CA sopra elencate e i relativi servizi di emissione OCSP;
- generazione marche temporali;

I servizi fiduciari qualificati soddisfano i requisiti eIDAS (Regolamento (EU) N°910/2014) e sono conformi ai seguenti standard:

- 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.

La struttura del presente TSPPS è conforme alla specifica pubblica [RFC 3647] e fa riferimento alle Policy di Certificato definite nel documento "Intesi Group Trust Service Provision Policy" TSPP ed ai seguenti certificati emessi da Intesi Group:

- Il certificato di root CA dedicato all'emissione di certificati di firma qualificata;
- Il certificato di root CA dedicato all'emissione di certificati per sigilli elettronici;
- Il certificato di root CA dedicato all'emissione di certificati di marcatura temporale;
- i certificati di firma qualificata di Intesi Group emessi a persone fisiche;
- i certificati per sigilli qualificati di Intesi Group emessi a persone giuridiche;
- i certificati di marcatura temporale;
- alle marche temporali.

1.2 Nome e identificativo del documento

Nome e versione sono indicati sul frontespizio del presente documento.

Questo documento è reso pubblico attraverso il sito web istituzionale di Intesi Group (http://www.intesigroup.com) e pubblicato in copia sul sito web di AgID (http://www.agid.gov.it/).

1.3 Partecipanti alla PKI

1.3.1 Intesi Group come Autorità di Certificazione e Marcatura Temporale

TSP Intesi Group funge da autorità di certificazione e validazione temporale e si identifica nel seguente modo:

Nome della società: Intesi Group S.p.A.

Sede Legale: Via Torino, 48 – 20123 Milano (MI) – ITALIA

Rappresentante Legale: Paolo Sironi (Consiglio di Amministrazione)

Partita IVA e Codice Tributario: IT02780480964

Telefono: +39 02 6760641

Identificatore di Oggetto ISO (OID): 1.3.6.1.4.1.48990

Sito web della società: http://www.intesigroup.com

Indirizzo e-mail della società: intesi@intesigroup.com

La PKI realizzata da Intesi Group prevede un solo livello di chiavi di certificazione. Le chiavi di CA attualmente in uso da parte di Intesi Group e coperte dal presente CPS sono indicate con i seguenti subjectDistinguishedName:

SubjectDistinguishedName
CN=Intesi Group EU Qualified Electronic Signature CA G2, OrganizationIdentifier=VATIT-02780480964, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., C=IT
CN=Intesi Group EU Qualified Electronic Seal CA G2, OrganizationIdentifier=VATIT-02780480964, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., C=IT
CN=Intesi Group Qualified Time-Stamp CA G2, OrganizationIdentifier=VATIT-02780480964, O=Intesi Group S.p.A., OU=Qualified Trust Service Provider, C=IT

1.3.2 Local Registration Authority

La Local Registration Authority (LRA) è una terza parte delegata, a seguito di accordi stipulati con Intesi Group, a svolgere attività di:

- identificazione e autenticazione (I&A) dei soggetti che richiedono i certificati di firma e sigillo elettronico;
- trasmissione, con procedure sicure, delle informazioni dei soggetti riconosciuti alla CA.
- registrazione dei dati del richiedente e della autorizzazione all'emissione di certificati attraverso appositi strumenti messi a disposizione da Intesi Group.
- validazione e gestione di eventuali richieste di sospensione, revoca e riattivazione;

Le RA sono soggette a verifiche da parte di Intesi Group finalizzate a verificare il rispetto degli accordi sottoscritti con la CA Intesi Group.

1.3.3 Sottoscrittori o richiedenti

Nell'ambito di questo CPS per sottoscrittore o richiedente si intende:

1. Una persona fisica titolare del certificato.
2. Una persona fisica autorizzata a rappresentare una persona giuridica.
3. Una persona giuridica.

1.3.4 Soggetti

Per soggetti si intendono:

- persone fisiche titolari di certificati qualificati di firma elettronica.
- persone giuridiche titolari di sigilli qualificati.

1.3.5 Titolari

Per titolare si intende la persona che ha in uso le chiavi private relative ad un certificato di firma o un certificato per sigillo elettronico. Nel caso di certificati di firma coincide con il soggetto, nel caso di certificati per sigillo è la persona registrata dal RAO in fase di riconoscimento e che ha in uso le credenziali.

1.3.6 RAO

I RAO sono gli addetti alle attività di Identificazione, raccolta e trasmissione documentazione e alla registrazione di utenti.

I RAO possono essere selezionati tra il personale della CA oppure tra il personale di una LRA e vengono abilitati ad operare in seguito alla stipula di un mandato con la CA e solamente dopo avere seguito un corso di formazione.

Al termine di questo processo, agli operatori viene dato accesso agli strumenti telematici sicuri messi a disposizione dalla CA e necessari per consentire lo svolgimento delle attività RAO.

La gestione dei privilegi di accesso di questi strumenti è sotto il controllo della CA.

1.3.7 Relying parties o utilizzatori

Le “Relying Parties” sono tutti i soggetti che fanno affidamento sulle informazioni contenute nei certificati. In particolare, per quanto riguarda il servizio di CA qui descritto, sono tutti i soggetti che verificano firme elettroniche e sigilli elettronici attraverso i certificati emessi secondo questo TSPPS.

1.3.8 Altri partecipanti

Le attività svolte dalla CA qualificata Intesi Group è soggetta alla supervisione di Agid (Agenzia per l’Italia Digitale).

1.4 Uso dei certificati e dei sigilli

Le policy dei certificati per l'apposizione di firme e l'apposizione di sigilli contenute in questo TSPPS sono identificate dagli OID specificati nella clausola 1.2 del TSPP.

1.5 Amministrazione del CPS

Il presente TSPPS viene redatto, revisionato, e aggiornato da personale appositamente incaricato di Intesi Group S.p.A. e viene pubblicato solamente dopo essere stato approvato dalla Direzione di Intesi Group. Richieste di informazioni o chiarimenti riguardo al presente TSPPS possono essere inviate scrivendo una email all'indirizzo **tsp@intesigroup.com.**

1.6 Definizione e acronimi

Acronimi	Definizione
CA	Certification Authority
CAO	Certificate Authority Officer
TSPP	TSP Policy
TSPPS	TSP Practice Statement
CRL	Certificate Revocation List
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
QTSA	Qualified Time-Stamping Authority
PKI	Public Key Infrastructure – componente per l'emissione dei certificati.
RAO	Registration Authority Officer
RFC	Request For Comments
TIN	Tax Identification Number
TSA	Time-Stamping Authority

Acronimi	Definizione
TSU	Time-Stamping Unit
TLS	Transport Layer Security
TSP	Trust Service Provider

2 PUBBLICAZIONE E ARCHIVIAZIONE

2.1 Repository

I repository pubblici di Intesi Group sono costituiti dai seguenti siti web:

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

che sono gestiti e mantenuti da personale di Intesi Group addetto alle operazioni di CA.

I repository sono disponibili 24 ore al giorno, 7 giorni a settimana e sono progettati per garantire livelli di servizio (SLA) del 99.9%. In caso di guasti del sistema o di altri eventi accidentali che ne possano interrompere l'erogazione, Intesi Group metterà in atto tutte le procedure sistemistiche interne atte ad assicurare che il servizio venga ripristinato nel più breve tempo possibile.

2.2 Informazioni pubblicate

Intesi Group pubblica attraverso il proprio sito Web la seguente documentazione:

- Policy TSP (TSPP), per tutti i servizi fiduciari offerti.
- Manuale Operativo (TSPPS).
- PKI Disclosure Statement (PDS)
- Termini & Condizioni di contratto dei servizi.
- CRL – Liste di revoca dei certificati per tutte le CA.

- Modulistica varia.

2.3 Data e frequenza delle pubblicazioni

La frequenza di pubblicazione e aggiornamento della documentazione è stabilita da processi interni di Intesi Group. La versione da ritenersi valida è l'ultima versione disponibile presente sul sito web del servizio di certificazione (www.intesigroup.com) oppure, dove applicabile, quella pubblicata sul sito web di AgID (www.agid.gov.it).

In caso di incoerenza tra le due versioni, sarà da ritenersi valida la versione pubblicata sul sito web di AgID.

Per la frequenza di aggiornamento e pubblicazione delle CRL, fare riferimento al paragrafo 4.

2.4 Controllo all'accesso

L'accesso alla documentazione e alle CRL è libero e non richiede autenticazione.

3 IDENTIFICAZIONE E AUTENTICAZIONE

Le procedure di Identificazione e Autenticazione seguite da Intesi Group sono conformi al requisito ETSI EN 319 411-1.

3.1 Nomi

3.1.1 Tipi di nomi

Tutti i certificati qualificati emessi da Intesi Group sono conformi alla normativa italiana e al profilo specificato nelle parti applicabili dello standard ETSI EN 319 412, vale a dire alla parte 2 per i

certificati emessi per persone fisiche, alla parte 3 per persone giuridiche e alla parte 5 per certificati qualificati.

Tutti i certificati TSU emessi da "Intesi Group Qualified Time-Stamp CA" sono conformi al profilo specificato in ETSI EN 319 412-3 e ai requisiti specificati in ETSI EN 319 422.

3.1.2 Necessità di dare nomi significativi

Salvo l'uso di pseudonimi, i nomi usati nel presente TSPPS e nel TSPP dovranno essere significativi per identificare i soggetti dei certificati (persone fisiche o giuridiche) e dei certificati per Time Stamp Unit.

3.1.3 Anonimato e pseudonimia dei titolari

Durante il processo di un'identificazione (cfr 3.2.4, 3.2.5 e 3.2.6), il sottoscrittore può richiedere l'inserimento di uno pseudonimo da inserire nel campo pseudonym del subjectDistinguishedName del certificato di firma al posto dei propri dati personali. L'uso dello pseudonimo è accettato esclusivamente se:

- È unico e non è assegnato ad altri soggetti identificati da Intesi Group.
- I certificati sono emessi per una persona fisica.

Intesi Group conserva le informazioni personali del soggetto associate allo pseudonimo per venti (20) anni dal momento dell'emissione del certificato e le mantiene in modo che restino riservate e non possano essere divulgate a terzi salvo per i casi previsti dalla legge.

L'utilizzo di pseudonimi non è applicabile ai sigilli digitali ed ai certificati TSU.

3.1.4 Abilitazioni professionali, ruolo e organizzazione

Il Titolare del certificato di firma può ottenere, in autonomia o con il consenso dell'eventuale "Terzo Interessato", l'inserimento nel certificato di informazioni sulle proprie qualifiche, quali

l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, oppure i poteri di rappresentanza.

Queste informazioni sono inserite nell'attributo "title" del campo Subject del certificato. In questo caso il Richiedente oltre alla documentazione e alle necessarie informazioni identificative, dovrà produrre anche documentazione idonea a dimostrare l'effettiva sussistenza dello specifico ruolo o abilitazione professionale, eventualmente anche utilizzando apposita autocertificazione ai sensi dell'art. 46 del DPR n. 445/2000.

Ai sensi della Deliberazione CNIPA n. 45/2009, nel caso in cui il ruolo sia autocertificato da parte del Richiedente, nel certificato non saranno inserite informazioni sull'organizzazione a cui potrebbe essere associato il Richiedente; In questo caso la CA non assume alcuna responsabilità per l'inserimento del ruolo nel certificato, salvo nei casi di dolo o negligenza.

Informazioni sull'organizzazione saranno invece inserite nel certificato solamente se tale organizzazione ha espressamente richiesto o autorizzato il rilascio del certificato, anche senza l'esplicita indicazione di un ruolo. In tal caso, la CA effettua un controllo sulla regolarità formale della documentazione presentata dal Richiedente.

3.1.5 Regole di interpretazione dei nomi

I nomi rispettano lo standard X.500.

3.1.6 Univocità dei nomi

La combinazione degli attributi del Soggetto (SubjectDistinguishedName) garantisce l'univocità dei nomi. In particolare, per i certificati emessi per persone fisiche, le informazioni che garantiscono l'unicità sono:

- il Givenname (OID 2.5.4.44) contenente il nome del soggetto.
- il Surname (OID 2.5.4.44) contenente il cognome del soggetto.

- il SerialNumber (OID 2.5.4.44) contenente il codice fiscale del soggetto o, in alternativa, un codice tratto dal documento di identità utilizzato per il processo di identificazione.

Quando il soggetto usa uno pseudonimo, l'unicità dei nomi è garantita dall'unicità dello pseudonimo.

Per i certificati emessi per una persona giuridica, l'unicità è garantita dalla combinazione dei campi:

- OrganizationName (OID 2.5.4.10) contente il nome completo del soggetto (persona giuridica).
- OrganizationIdentifier (OID 2.5.4.97) contenente un codice di identificazione dell'organizzazione del soggetto diversa dal nome dell'organizzazione. Questo campo è definito in base a ETSI EN 319 412-1 [i.4].

Per i certificati TSU, l'unicità è garantita delle procedure interne di Intesi Group.

3.1.7 Riconoscimento, autenticazione e ruolo dei marchi commerciali

I richiedenti del certificato devono garantire di operare in piena conformità alle leggi sulla proprietà intellettuale nazionali e internazionali.

Intesi Group non effettua controlli sull'uso dei marchi commerciali e può rifiutare di emettere o imporre la revoca di certificati coinvolti in una controversia giuridica.

3.2 Verifica dell'identità

La verifica dell'identità fa parte del processo di emissione del certificato descritto nel capitolo 4.1. Le procedure utilizzate per la verifica dell'Identità di soggetti fisici e giuridici sono descritte in dettaglio nei documenti interni di Intesi Group S.p.A.

3.2.1 Prova del possesso di una chiave privata

La prova di possesso della chiave privata corrispondente al certificato richiesto si basa sulla verifica crittografica del CSR (Certificate Signing Request) inviato alla CA. Il richiedente deve inviare la propria chiave pubblica alla CA sotto forma di CSR nel formato PKCS#10 [RFC2314] e la CA dovrà verificare che la firma digitale del CSR sia valida.

3.2.2 Validazione dell'identità di una organizzazione

La domanda per un certificato qualificato emesso per una persona giuridica (sigillo elettronico) viene fatta da una persona fisica che rappresenta la persona giuridica e che è identificata secondo le stesse procedure usate per le persone fisiche (vedere par. 3.2.3).

I poteri di rappresentanza della persona giuridica devono essere dimostrati fornendo alla CA o al RAO adeguata documentazione emessa da un organismo di autorità come, per esempio, una certificazione emessa dalla camera del commercio.

3.2.3 Validazione delle identità individuali

Il processo di Identificazione viene condotto dai RAO (cfr. 1.3.6) che devono operare secondo le seguenti procedure di identificazione applicate da Intesi Group:

- Identificazione de-visu che avviene con un incontro tra un RAO ed il richiedente.
- Identificazione e registrazione tramite processo IDentify Web.
- Identificazione attraverso procedure di identificazione di un cliente con mandato LRA.
- Identificazione attraverso verifica firma elettronica qualificata.

3.2.4 Identificazione e registrazione de-visu

Questa modalità di identificazione viene condotta da un operatore qualificato come RAO e richiede la presenza fisica del titolare, il quale deve farsi riconoscere presentando adeguati documenti di identità.

I documenti che un RAO può accettare sono:

- Carta di identità nazionale.
- Passaporto.
- Documenti che siano legalmente riconosciuti come documenti di identificazione al momento del riconoscimento.

Nel caso in cui il soggetto stia richiedendo:

- un certificato per sigillo elettronico.
- un certificato previa autorizzazione del terzo interessato.
- l'inserimento di proprie qualifiche o abilitazioni professionali.

deve presentare documentazione sufficiente a dimostrare al RAO l'autorizzazione a richiedere il certificato o ad utilizzare le qualifiche ed abilitazioni personali richieste.

Il RAO deve verificare la documentazione presentata e nel caso in cui la ritenga sufficiente e valida, procedere con:

- La registrazione dei dati anagrafici del richiedente attraverso il portale RAO di Intesi Group. Un elenco dettagliato delle informazioni inserite è riportato nel paragrafo 4.2.1.
- La digitalizzazione di una copia dei documenti di identificazione presentati.
- La stampa di una copia del contratto d'uso.

La copia del contratto viene presentata al richiedente che è tenuto a leggerla, firmarla e riconsegnarla al RAO. Il RAO dovrà trattenere con sé la copia cartacea firmata che dovrà poi consegnare in un secondo tempo ad Intesi Group mentre le copie digitali sono inviate ad Intesi Group tramite il portale RAO.

Intesi Group avrà cura di conservare sia le copie digitali che quella cartacea secondo quanto previsto dalla normativa vigente.

Nel caso in cui l'utente fornisca informazioni incomplete, documenti identificativi non validi o mancanti o non firmi una copia del contratto, il RAO non potrà approvare l'emissione del certificato di firma o del sigillo.

3.2.5 Identificazione tramite processi LRA

Intesi Group si può riservare di accettare modalità di identificazione differenti da quelle previste dai propri processi ed adottate da aziende proprie clienti autorizzate a svolgere attività di RA dopo avere attentamente verificato che la procedura adottata sia adeguata ed aderente con le modalità previste dalla normativa, da Agid e dal presente TSPPS.

In ogni caso prima di approvare l'identificazione attraverso processi di terze parti, Intesi Group dovrà ottenere autorizzazione da Agid.

3.2.6 Identificazione e registrazione IDentify Web.

Questa modalità di identificazione viene condotta da un operatore RAO attraverso una videoconferenza con il richiedente del certificato. Il sistema di video conferenza utilizzato è messo a disposizione da Intesi Group che si occuperà di fornire al richiedente tutte le istruzioni necessarie per potervi accedere. Il richiedente, da parte sua, deve essere dotato di un dispositivo (PC, Smartphone o Tablet) dotato di una webcam e di un sistema audio funzionante.

Alla data concordata il richiedente viene contattato dal RAO tramite la piattaforma IDentify Web. Il RAO eseguirà una serie di procedure, mantenute riservate per ragioni di sicurezza, volte a verificare la reale presenza del richiedente e l'autenticità dei documenti presentati.

Il RAO che effettua l'identificazione si accerta dell'identità del Titolare tramite la verifica di uno o più documenti di riconoscimento in corso di validità. I documenti accettati sono elencati nel par. 3.2.4.

Il RAO che effettua l'identificazione si può riservare di non considerare ammissibile un documento presentato del Titolare se ritiene che non rispetti le caratteristiche di validità e autenticità.

Il RAO può inoltre non avviare o interrompere il processo di identificazione nel caso in cui la qualità audio/video sia di scarsa qualità o ritenuta non adeguata a soddisfare i requisiti dell'art 32 comma 3, lettera a) del Codice dell'Amministrazione Digitale.

All'avvio della video conferenza all'utente verrà sempre richiesto di:

1. confermare il consenso al trattamento dei dati personali.
2. confermare di accettare i termini e condizioni del servizio.

Entrambi i documenti sono inviati all'utente tramite email prima della sessione di video conferenza ed in ogni caso sono liberamente scaricabili dal sito istituzionale di Intesi Group.

In mancanza del consenso la video conferenza ed il processo di riconoscimento sono interrotti dal RAO.

Se al termine della videoconferenza il RAO ritiene il processo di riconoscimento avvenuto con successo approverà l'emissione del certificato, in caso contrario rigetterà la richiesta informandone l'utente.

I dati di registrazione, costituiti dal file audio-video e metadati strutturati in formato elettronico, vengono conservati in maniera sicura secondo quanto indicato nell'art. 32, comma 3, lettera j del Codice dell'Amministrazione Digitale.

3.2.7 Identificazione attraverso verifica firma elettronica qualificata.

L'identificazione di un utente può avvenire attraverso la verifica di una firma digitale qualificata (emessa da un prestatore di servizi fiduciari qualificati) apposta sul modulo di richiesta di certificato.

Per questo tipo di identificazione l'utente deve:

1. Compilare con i propri dati personali e firmarlo digitalmente con il certificato qualificato.
2. Inviarlo attraverso uno dei canali messi a disposizione da intesi Group e preventivamente concordati con l'utente.

Alla ricezione del documento firmato, Intesi Group verificherà la validità della firma e la corrispondenza dei dati dell'intestatario del certificato qualificato con i dati inseriti all'interno del modulo di richiesta.

Se la verifica avrà successo verrà approvata l'emissione del certificato, in caso contrario la richiesta verrà rigettata informandone l'utente.

La copia del contratto firmato verrà conservata secondo quanto previsto dalla normativa vigente.

3.2.8 Informazioni non verificate

Alcune informazioni necessarie per l'attivazione e la gestione dell'account, come per esempio l'indirizzo di posta elettronica o il numero di telefono cellulare, non vengono verificate dalla CA, che non si assume responsabilità nel caso in cui tali informazioni siano fornite in modo errato.

3.3 Identificazione e autorizzazione per riutilizzo chiave (re-key)

Intesi Group non mette a disposizione funzionalità che consentano il riutilizzo della chiave.

3.4 Identificazione e autenticazione per richieste di revoca

I metodi per l'identificazione e l'autenticazione delle richieste di sospensione e di revoca attraverso il portale CA, è necessario che l'utente effettui la login utilizzando lo username e la password forniti dopo la prima registrazione;

Nel caso l'utente non ricordi o abbia smarrito le informazioni di autenticazione può presentare richieste di revoca ad un RAO abilitato o inviando una richiesta al supporto di Intesi Group secondo le modalità descritte nel paragrafo 4.9.

La revoca di un certificato TSU deve essere autorizzata dal Security Officer, in base alla procedura descritta in 4.9.

4 REQUISITI GESTIONE DEL CICLO DI VITA DEL CERTIFICATO

4.1 Richiesta di certificato

4.1.1 Chi può richiedere il certificato

La richiesta per un certificato qualificato emesso a persona fisica può essere presentata dal soggetto (cfr. 1.3.4) facendone domanda alla CA o ad una LRA autorizzata e può prevedere anche un "terzo interessato", ovvero un soggetto che acconsente all'inserimento di un ruolo nel certificato o una organizzazione che richiede o autorizza il rilascio del certificato del titolare (cfr. Del. CNIPA n. 45/2009).

La richiesta per un certificato qualificato emesso a persona giuridica può essere richiesta da una persona fisica che è autorizzata a rappresentare la persona giuridica presentando la domanda alla CA o ad una LRA autorizzata.

Infine, il certificato per marche temporali (TSU) può essere solamente richiesto da personale interno di Intesi Group nell'ambito dell'attività per la key ceremony delle chiavi.

4.1.2 Processo di registrazione e responsabilità

Il processo di registrazione deve essere svolto a valle del processo di identificazione (cfr. par 3), e prevede i seguenti passi:

- la registrazione dei dati anagrafici;
- L'acquisizione dell'accettazione da parte del richiedente del contratto e dei termini e condizioni di servizio;
- l'invio delle informazioni raccolte alla CA Intesi Group;

Il processo di registrazione necessita dei seguenti diversi attori:

- del Sottoscrittore che deve:
    1. Leggere ed accettare l'informativa sul trattamento dei dati personali.
    2. Fornire i dati necessari alla registrazione e presentare la documentazione necessaria al riconoscimento.
    3. Accettare i Termini e condizioni del contratto di CA.
    4. Dichiarare di avere preso visione del presente TSPPS e di averlo compreso e accettato.
- Il RAO che deve effettuare:
    1. il riconoscimento dell'utente:
    2. acquisire il consenso al trattamento dei dati personali e l'accettazione del contatto.
    3. opzionalmente la registrazione dei dati dell'utente.
    4. inviare copia dei documenti acquisiti alla CA.
    5. approvare l'emissione del certificato o del sigillo.
- LA CA che emette il certificato, conserva i dati di identificazione dell'utente e mantiene e diffonde informazioni sullo stato di certificati e sigilli.

Come indicato nei paragrafi precedenti le funzioni di registrazione possono essere svolte anche da terze parti (LRA) sulla base di accordi e procedure concordate con la CA.

4.2 Processo di emissione

La procedura di emissione di certificati a persone fisiche e persone giuridiche si svolge attraverso i seguenti passi:

- Il RAO esegue il processo di identificazione descritto in 3.2;
- Il titolare deve:
    1. fornire il consenso al trattamento dei dati personali;
    2. leggere ed accettare il contratto ed i Termini e Condizioni del servizio di CA;
    3. dichiarare di avere preso visione del presente TSPPS;
- Il RAO effettua la registrazione e l'invio di copia della documentazione raccolta alla CA utilizzando gli strumenti che quest'ultima mette a disposizione. Il RAO approva la richiesta di emissione del certificato.
- La CA, acquisita e validata la documentazione, comunica all'utente (ad. esempio attraverso e-mail) l'approvazione della richiesta e le informazioni necessarie per emettere il certificato.
- Il titolare, utilizzando le credenziali fornite con la procedura descritta nel par. 4.2.2.1, deve autenticarsi al servizio di emissione tramite portale Web o App Mobile di Intesi Group ed eseguire la procedura di emissione seguendo i passi che vengono proposti (cfr. par. 4.3). Il titolare, attraverso le funzionalità fornite dal portale effettuerà:
    1. La personalizzazione delle quantità di accesso alla propria credenziale, definendo un PIN di accesso e personalizzando il token OTP (dove presente).
    2. la generazione delle chiavi sul dispositivo QSCD e la relativa emissione del certificato sulla PKI Intesi Group. La comunicazione tra QSCD e PKI avviene completamente all'interno dell'infrastruttura Intesi Group ed è resa sicura attraverso l'uso dal protocollo TLS e dalla mutua autenticazione dei componenti attraverso l'uso di certificati.

La procedura di emissione dei certificati qualificati può essere eseguita solamente dall'utente titolare del certificato. La procedura di emissione di certificati TSU è descritta nelle procedure interne di Intesi Group.

4.2.1 Informazioni del soggetto richieste

Per richiedere un certificato per persona fisica o persona giuridica, il richiedente deve fornire le seguenti informazioni obbligatorie:

- Nome e cognome;
- Data di nascita, città di nascita, provincia di nascita e stato di nascita;
- Stato, provincia, città e indirizzo di residenza;
- Numero di telefono mobile;
- Indirizzo email;
- Codice fiscale o codice equivalente;

Per richiedere un certificato per persona giuridica deve fornire anche:

- Nome della società;
- Codice tributario della società;
- Indirizzo della società (stato, provincia, città ed indirizzo);
- Email e numero di telefono della società;

4.2.2 Registrazione e autenticazione

La registrazione dei dati dell'utente è compita dei RAO ed è eseguita al termine del processo di identificazione descritta al paragrafo 3.2.

Per poter effettuare la registrazione, la CA mette a disposizione una applicazione Web denominata pkra (raggiungibile all'url https://pkra.time4mind.com) che consente al RAO di eseguire il processo di registrazione attraverso i seguenti passi:

1. Dopo essersi autenticato con successo il RAO deve selezionare il profilo di certificato da autorizzare per l'emissione.
2. A fronte della selezione l'applicazione presenterà un form di inserimento che il RAO dovrà compilare in tutte le sue parti inserendo i dati forniti dal richiedente.
3. Completato l'inserimento, l'applicazione richiede l'acquisizione delle immagini digitalizzate dei documenti di riconoscimento presentati. A tale scopo l'operatore deve utilizzare una App appositamente sviluppata da Intesi Group (Identify) e che deve essere installata su uno smart device (smartphone o tablet) che deve essere in possesso del RAO.
4. I dati così raccolti devono essere digitalmente firmati dal RAO e quindi inviati ai server della CA. La firma deve essere apposta con una credenziale di firma remota che viene fornita al RAO a seguito della ricezione del mandato RAO e della stipula degli accordi contrattuali.
5. Il server della CA verifica in modo automatico i dati ricevuti e, se risultano completi e corretti, li salva sul repository interno dove verranno conservati conformemente ai requisiti previsti dalla normativa vigente.
6. Il RAO può ora completare la registrazione definendo, dove applicabile, il tipo di token OTP da associare alla credenziale del richiedente ed infine può approvare l'emissione del certificato.

Per le LRA che hanno processi di identificazione propri e approvati dalla CA, i passi descritti sopra possono essere eseguiti in modo automatico utilizzando appositi WebServices esposti dal portale Time4mind di Intesi Group.

Il completamento della registrazione è confermato al richiedente con l'invio di una email contenente:

- Un codice univoco definito "security code" che sarà necessario per avviare la procedura di emissione del certificato o del sigillo.
- Un link che avvia automaticamente il processo di emissione del certificato.

A seguito del ricevimento dell'email l'utente può eseguire la procedura di emissione del certificato.

4.2.2.1 Credenziali autenticazione soggetto

Per emettere il certificato il titolare deve autenticarsi con credenziali semplici al portale utente della CA raggiungibile all'url https://user.time4mind.com oppure deve autenticarsi, sempre utilizzando le medesime credenziali, all'App Mobile Valid.

La coppia di credenziali di autenticazione può essere fornita direttamente dal RAO durante il riconoscimento oppure può essere generata direttamente dal richiedente in modalità self-service compilando la sezione "Registration" della form di autenticazione del portale time4mind.

La richiesta di registrazione al portale Time4Mind viene notificata all'utente attraverso una email contenente un link di conferma che l'utente è tenuto a cliccare per finalizzare la registrazione.

Le credenziali semplici servono per accedere al portale ma non sono sufficienti per avviare il processo di emissione di un certificato perché per questo è necessario che l'utente inserisca anche il codice di sicurezza che ha ricevuto al termine della registrazione.

4.2.2.2 Credenziali autenticazione RAO

I RAO per poter accedere ai servizi di Registration Authority offerti dal portale devono essere dotati di credenziali semplici abilitate ad accedere al portale PkRA e devono essere dotati di credenziali di firma necessarie per eseguire la procedura di registrazione.

La generazione delle credenziali è effettuata da personale di Intesi Group appositamente incaricato ed avviene seguendo le procedure di incarico dei RAO definite da Intesi Group.

4.2.2.3 Credenziali autenticazione LRA

I clienti abilitati ad operare come LRA possono invocare i servizi di Registration Authority attraverso webservices esposti dal portale Time4Mind.

La comunicazione tra client e server è protetta da un canale sicuro TLS e richiede:

- una certificate authentication per ottenere l'accesso ai servizi.

- una credenziale di firma remota o di firma automatica per firmare la documentazione inviata.

I certificati di autenticazione e di firma sono generati e distribuiti da personale interno Intesi Group a seguito delle procedure di incarico delle LRA definite dalla CA Intesi Group.

4.3 Emissione del certificato

4.3.1 Emissione del certificato

Gli utenti che richiedono la firma remota devono verificare di essere in possesso degli strumenti necessari per la generazione dei token OTP.

In particolare:

- gli utenti che fanno uso di token SMS devono accertarsi di avere il dispositivo mobile associato al numero di telefono fornito in fase di registrazione.
- gli utenti che usano token OTP fisico devono accertarsi di avere l'OTP fornito dal RAO a seguito della registrazione.
- gli utenti che fanno uso di token OTP generati tramite App Mobile Valid, prima di avviare la procedura di emissione certificato devono assicurarsi di avere installato l'App sul proprio dispositivo mobile. L'App è disponibile per il download gratuito sul Play Store di Google per dispositivi Android e sull'App Store di Apple per dispositivi iOS.

La procedura di emissione del certificato può essere eseguita dal portale Time4Mind di Intesi Group oppure, nei casi in cui si applica, direttamente dall'App mobile Valid.

Per avviare la procedura di emissione del certificato attraverso il portale user di Time4Mind l'utente deve loggarsi al portale utilizzando le proprie credenziali semplici e selezionare la voce di menu "Enroll Certificate".

Come primo passo, all'utente verrà richiesto di selezionare la credenziale da emettere e di inserire il "security code" ricevuto via e-mail per autenticare la richiesta di emissione. In alternativa l'utente può saltare questi passi cliccando sul link ricevuto con l'email di conferma registrazione.

In entrambi i casi, se le verifiche si concludono con successo, si viene rimandati direttamente all'avvio della procedura di generazione della credenziale di firma.

A questo punto, a seconda della tipologia di certificato da emettere e del tipo di token da associare la procedura proseguirà con modalità differenti.

In particolare, per certificati di firma automatica richiede di definire un PIN che, abbinato all'alias generato automaticamente e visualizzato all'utente, costituirà la quantità di autenticazione alla credenziale.

Per certificati di firma remota che fanno uso di OTP SMS, oltre al PIN viene richiesto di inserire l'OTP che la procedura avrà automaticamente inviato al numero di telefono fornito in fase di riconoscimento. In questo caso l'abbinamento alias, PIN e OTP SMS costituiranno le credenziali di sblocco della credenziale di firma.

Per certificati di firma remota che fanno uso di OTP fisico, oltre al PIN viene richiesto di inserire l'OTP generato dal dispositivo fornito dal RAO. In questo caso l'abbinamento alias, PIN e OTP costituiranno le credenziali di sblocco della credenziale di firma.

L'ultimo caso riguarda certificati di firma remota abbinati a token OTP generati da App Valid per cui la procedura, una volta avviata, proseguirà dall'interno dell'App a cui nel frattempo sarà stata inviata una notifica "Out Of Band" per avvisarla della procedura di enroll in corso. L'App richiederà all'utente di definire un PIN e quindi autonomamente ed in completa sicurezza avvierà la procedura di emissione certificato comunicando col portale Time4Mind.

Alla ricezione delle informazioni, il server Time4Mind avvia la procedura di generazione di una coppia di chiavi sul dispositivo QSCD e ottenendo in risposta una richiesta di certificato in formato

PKCS#10. Questa viene poi inviata al sistema interno di generazione dei certificati (PKI) che si occuperà di convalidare la richiesta ed emettere un certificato in formato X.509.

Il certificato così generato verrà restituito al chiamante che si occuperà di salvarlo sul dispositivo QSCD in associazione con la chiave privata completando così la credenziale di firma.

Il certificato così ottenuto verrà salvato sul dispositivo QSCD in associazione con la chiave privata completando così il processo di generazione della credenziale di firma.

Il processo di emissione del certificato si completa con l'invio di un messaggio di conferma al titolare contenente un codice di revoca che potrà utilizzare per inviare una richiesta di revoca o sospensione al customer care di Intesi Group.

Copia dell'email di conferma potrà essere inviata al terzo interessato qualora fosse presente.

4.3.2 Emissione del certificato TSA

La richiesta di certificato viene eseguita manualmente da due operatori TSP nel modo seguente:

- Il primo operatore TSP utilizzando le funzionalità del software di emissione marche in uso ad Intesi Group, genera la coppia di chiavi sulla partizione dell'HSM dedicata ad ospitare le chiavi di marcatura temporale e genera la richiesta di certificato in formato PKCS#10 che salva su un dispositivo fisico (ad. es. una Pen Drive) e che passa ad un secondo operatore TSP preposto ad emettere il certificato.
- Quest'ultimo, ricevuto il supporto fisico, procede con il recupero della richiesta e l'emissione del certificato operando sul pannello di amministrazione della PKI Intesi Group. Il certificato ottenuto lo salva sullo stesso supporto fisico con cui ha ricevuto la richiesta e lo restituisce al primo operatore TSP.
- Il primo operatore TSP, operando sul software di emissione marche, procederà con l'installazione del certificato sull'HSM e alla attivazione sul servizio di marcatura temporale.

L'intero processo viene eseguito sotto la supervisione del TSA Officer.

4.4 Accettazione del certificato

4.4.1 Accettazione del Certificato

4.4.1.1 Accettazione del certificato

Il certificato viene considerato accettato dopo essere stato consegnato al titolare.

4.4.1.2 Accettazione del certificato TSA

In caso di certificati errati, l'operatore TSA richiederà al Security Officer l'autorizzazione a revocare il certificato in conformità con la procedura descritta in 4.8.

4.4.2 Pubblicazione del Certificato da parte della CA

Una volta che il certificato è stato emesso, viene conservato sul database della CA e non viene reso pubblico.

4.4.3 Notifica dell'emissione del Certificato da parte della CA ad altre entità

Una email contenente un messaggio di conferma emissione viene inviata al titolare e, qualora fosse presente, al terzo interessato. Non vengono inviate notifiche per i certificati TSA.

4.5 Coppia di Chiavi e Utilizzo del Certificato

4.5.1 Utilizzo della chiave privata e del Certificato

4.5.1.1 Chiavi e certificati di firma digitale e sigillo

Il titolare deve:

- essere il solo utilizzatore della chiave privata.

- mantenere in modo esclusivo la conoscenza dei dati per lo sblocco della firma (PIN, PUK e/o OTP) conservandoli con la massima diligenza.
- conservare con la massima diligenza il dispositivo OTP eventualmente fornito.
- utilizzare le proprie credenziali rispettando eventuali limitazioni d'uso contenute nei certificati.
- astenersi dall'utilizzare in modo improprio o fraudolento le chiavi ed i certificati in suo possesso.
- informare Intesi Group di ogni eventuale modifica ai dati non inclusi nel certificato ma comunicati e registrati durante il processo di registrazione.
- chiedere la revoca di certificato se ha fondate ragioni di credere che i dati di sblocco della chiave privata (ad es. codice PIN) siano stati compromessi.
- chiedere la revoca del certificato se i dati in esso contenuti sono cambiati o errati.

4.5.1.2 Chiavi e certificati di marcatura temporale

Le chiavi ed i certificati di TSU sono generati ed emessi internamente alla CA da personale autorizzato e secondo procedure interne e sono utilizzate solamente con lo scopo di generare marche temporali (cfr. rfc3161).

Ogni chiave privata viene usata per un massimo di 3 mesi dopodiché viene distrutta in presenza di un TSA officer.

4.5.2 Utilizzo della chiave pubblica e del certificato

Coloro che fanno affidamento sulle informazioni contenute nei certificati (cfr. utilizzatori 1.3.7) hanno l'obbligo di verificare che il certificato non sia scaduto, sospeso o revocato utilizzando le CRL o il servizio OCSP esposto dalla CA attraverso i propri repository ed i cui riferimenti sono contenuti nel certificato in particolare nelle estensioni CRLDistributionPoint e AuthorityInformationAccess.

La verifica deve considerare lo stato del certificato alla data e ora rilevante in base al contesto. In particolare la data e l'ora corrente se non c'è modo di sapere quando è stata apposta la firma oppure

la data e l'ora di apposizione della firma se è dimostrabile dalla presenza di una marca temporale nel documento firmato.

Gli utilizzatori possono esimersi dallo svolgere le verifiche sopra citate solo nel caso di certificato per "firma verificata", ai sensi della Determinazione AgID n.63/2014; l'esame dell'estensione CertificatePolicies del certificato consente agli utilizzatori di determinare se si tratta di un tale tipo di certificato. Per ulteriori dettagli sugli obblighi degli utilizzatori, si rimanda al par. 9.

4.5.3 User notice

I certificati qualificati per firma massiva contengono la limitazione d'uso stabilita dall'agenzia per l'Italia digitale – Agid – come Policy di Certificato aggiuntiva:

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

In conformità con la legislazione italiana, il Sottoscrittore può inoltre richiedere alla Certification Authority che nel certificato venga incluso una delle seguenti limitazioni d'uso:

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

Inoltre, il Sottoscrittore può anche richiedere l'inclusione di limitazioni d'uso personalizzate che devono essere preventivamente valutate dalla CA.

Il sottoscrittore può fare richiesta di un limite di valore delle operazioni per le quali si può usare un certificato ed è responsabile della verifica della conformità con i limiti di uso già presenti nel certificato.

La CA non è responsabile dei danni derivanti dall'uso di un certificato che non rispetti i limiti d'uso indicati nel certificato stesso.

4.6 Rinnovo del certificato

Il rinnovo di un certificato può essere effettuato solamente dal titolare solo se il certificato non è ancora scaduto e solo novanta giorni prima della scadenza del certificato e prevede sempre la generazione di una nuova coppia di chiavi.

La procedura di rinnovo di un certificato TSU viene eseguita ogni tre mesi da un Operatore TSP seguendo le procedure interne di Intesi Group.

4.6.1 Procedura per elaborare la richiesta di rinnovo

La procedura di rinnovo per certificati di firma o per sigillo può essere eseguita dal titolare attraverso la propria App mobile Valid (dove applicabile) o dal portale di Intesi Group.

I passi che deve seguire sono:

1. Autenticarsi con successo utilizzando le proprie credenziali semplici.
2. Firmare, con il certificato in scadenza, il contratto con i termini e condizioni del servizio di CA.
3. Definire un PIN di accesso alla nuova credenziale.

Fatto questo, la CA procede con la generazione delle chiavi e del certificato seguendo lo stesso flusso definito per la prima emissione del certificato (cfr. par. 4.3).

La procedura di rinnovo di un certificato di TSU è eseguita da una coppia di operatori TSP che agendo sul software di amministrazione del sistema di marcatura temporale possono generare una nuova chiave e possono emettere un nuovo certificato. Il rinnovo chiavi TSU viene effettuato seguendo una apposita procedura interna e viene verbalizzato su un documento di KeyCeremony che deve essere approvato dal TSP Officer e che viene conservato per un periodo di 20 anni.

4.6.2 Notifica al titolare

Le notifiche inviate al titolare sono:

- Novanta giorni prima della scadenza, il server invia al soggetto una email contenente un promemoria sulla scadenza del certificato e le istruzioni su come procedere con il rinnovo del certificato.
- Quando il processo di rinnovo del certificato è stato completato, viene inviato un messaggio di conferma contenente un codice di revoca che verrà richiesto per revocare o sospendere il certificato. Nei casi in cui sia presente, una copia del messaggio viene inviata anche al terzo interessato.
- Se l'utente lascia scadere il certificato senza effettuare la procedura di rinnovo, gli verrà inviata una email contenente nota informativa e istruzioni su come far domanda per un nuovo certificato.

4.6.3 Accettazione del certificato

Vale quanto riportato nella sezione 4.4.1.

4.6.4 Pubblicazione del Certificato

Vale quanto riportato nella sezione 4.4.2.

4.6.5 Notifica dell'emissione del Certificato da parte della CA ad altre entità

Vale quanto riportato nella sezione 4.4.3.

4.7 Re-key del Certificato

L'operazione di riutilizzo della chiave non è consentita dalla CA Intesi Group.

4.8 Modifica del Certificato

La modifica dei dati di un certificato non può essere eseguita. Per effettuare una modifica dei dati contenuti nel certificato occorre procedere con la revoca e la ri-emissione del certificato, seguendo le procedure descritte nelle sezioni 4.2 e 4.3.

4.9 Revoca e sospensione del certificato

4.9.1 Circostanze per la revoca

Le circostanze per richiedere la revoca sono quelle previste dalla normativa e dal TSPP.

4.9.2 Chi può richiedere la revoca

Il certificato può essere revocato su richiesta del:

1. titolare del certificato
2. terzo interessato quando presente.
3. la CA stessa, se ne ravvisa la necessità.

Per i certificati TSU la revoca può essere eseguita solamente dai TSP Operator dopo avere informato ed ottenuto l'approvazione da parte del TSP Security Officer.

4.9.3 Procedura per la richiesta di revoca

Il modulo e/o la procedura da utilizzare per fare domanda per la sospensione, riattivazione o revoca del certificato può essere eseguita dal titolare attraverso:

- il portale Time4Mind;
- inoltrando una richiesta ad un RAO;
- Inoltrando una richiesta all'assistenza clienti di Intesi Group;

Le domande per una revoca vengono elaborate al momento della ricezione e sono autenticate e confermate attraverso i seguenti processi:

4.9.3.1 Revoca tramite Time4Mind

Per revocare i propri certificati attraverso il portale Time4Mind (https://user.time4mind.com) il titolare deve:

1. accedere al portale Time4Mind effettuando una autenticazione con successo;
2. cercare il certificato da revocare tra quelli in suo possesso elencati dall'applicazione utilizzando il menu "Credential";
3. Invocare la funzione "Revoke" e confermare la richiesta.

La richiesta viene immediatamente presa in carico ed eseguita nel più breve tempo possibile. L'esito dell'operazione è mostrato a video all'utente e confermato con una email inviata al titolare e, quando applicabile, al terzo interessato.

4.9.3.2 Revoca tramite RAO di Intesi Group

La Revoca di un certificato può essere effettuata da qualsiasi operatore RAO usando il Portale PkRA a fronte di una richiesta del:

- titolare del certificato
- terzo interessato, quando applicabile.
- la CA.

I titolari ed i terzi interessati che desiderano chiedere la revoca di un certificato ad un RAO devono presentare il modulo di revoca, scaricabile dal portale Time4Mind compilato in tutte le sue parti ed una copia del documento di riconoscimento.

Il RAO, utilizzando le informazioni fornite e operando attraverso il portale web PkRA può:

1. Cercare l'utente;
2. Confrontare i dati forniti con quelli registrati al fine di autenticare il richiedente. Nel caso in cui il RAO ritenga che le informazioni non siano complete o comunque non

sufficienti procederà con la semplice sospensione del certificato in attesa che il richiedente fornisca chiarimenti o informazioni supplementari.

3. Richiedere la revoca o la sospensione del certificato.

La richiesta viene immediatamente presa in carico ed eseguita nel più breve tempo possibile. L'esito dell'operazione è mostrato a video all'operatore RAO e confermato con una email inviata al titolare e, nel caso in cui sia applicabile, al terzo interessato.

4.9.3.3 Revoca attraverso assistenza clienti

Solo in caso di indisponibilità dei servizi di revoca di Intesi Group, gli utenti ed i RAO possono richiedere una revoca all'assistenza clienti di Intesi Group, inviando un'email all'indirizzo:

certificate@intesigroup.com

Quando il mittente è un RAO, l'email deve essere inviata entro otto ore dal momento del ricevimento della richiesta di revoca da parte del soggetto.

Ogni email deve contenere una copia compilata del modulo di revoca che deve includere anche il codice di revoca oppure una copia digitale del documento identificativo. Se l'utente non è in grado di fornire uno di questi due documenti, il certificato verrà solo sospeso. L'utente, in seguito, ha dieci giorni per procedere con la revoca o con la riattivazione del certificato al termine del quale, se l'utente non ha effettuato alcuna operazione, il certificato verrà automaticamente riattivato.

Alla ricezione dell'email, un operatore di Intesi Group prenderà in carico l'attività verificando la correttezza delle informazioni fornite e verificando che l'indirizzo email del mittente sia lo stesso fornito durante la registrazione. Se tutte le verifiche danno riscontro positivo il RAO procederà con la revoca oppure con la sospensione del certificato.

L'esito dell'operazione è confermato con una email inviata al titolare e, nel caso in cui sia applicabile, al terzo interessato.

4.9.3.4 Revoca del certificato TSA

Secondo la clausola 4.8 della policy QTSP, la revoca del certificato viene eseguita dal TSP Operator con l'approvazione del Security Officer seguendo la Procedura Interna TSP.

A revoca eseguita, il TSP Operator procederà con l'eliminazione delle relative chiavi private dall'HSM.

4.9.4 Periodo di grazia della richiesta di revoca

La CA esegue la revoca con la massima diligenza possibile, allo scopo di assicurare che il tempo necessario per elaborare la richiesta di revoca e pubblicare il nuovo stato del certificato (aggiornamento CRL) sia ridotto il più possibile.

4.9.5 Termine entro il quale la CA deve elaborare la richiesta di revoca

Quando la CA riceve una richiesta di revoca prova ad eseguire l'operazione immediatamente. Se l'operazione va a buon fine, il certificato revocato viene inserito nella CRL entro 6 ore dalla revoca e comunque non oltre le 24 ore successive all'operazione. Se la revoca fallisce lo stato del certificato non viene cambiato ed il titolare, ed il terzo interessato dove applicabile, vengono informati tramite un messaggio email.

4.9.6 Esigenza di controllo per la revoca per gli Utilizzatori

Vedere paragrafo 4.5.2

4.9.7 Frequenza di emissione CRL / periodo di validazione della risposta OCSP

4.9.7.1 CRL

La CRL viene rigenerata e ripubblicata ogni 6 ore anche in assenza di nuove revoche. In alcune circostanze, la CA può imporre l'emissione di una nuova CRL prima delle 6 ore previste.

4.9.7.2 OCSP

Il servizio OCSP è disponibile per la validazione dello stato del certificato. I campi “this update” e “next update” rispecchiano il periodo di validità della risposta OCSP (vedere la sezione 7 del TSPPS).

4.9.8 Latenza massima della CRL

Il periodo tra la richiesta di revoca o sospensione e l’emissione di una nuova CRL è al massimo di sei ore.

4.9.9 Controllo della disponibilità dello stato di revoca on-line

Intesi Group mette a disposizione servizi di controllo dello stato del Certificato attraverso CRL e OCSP. Per dettagli vedere la sezione 4.10 del presente documento.

4.9.10 Altre forme disponibili di pubblicazione della revoca

Non disponibile.

4.9.11 Esigenze speciali per quanto riguarda la compromissione della chiave

Non disponibile.

4.9.12 Circostanze per la sospensione

La sospensione del certificato può essere eseguita nelle seguenti circostanze:

1. La CA riceve una richiesta di revoca che non contiene le informazioni necessarie per autenticare il richiedente.
2. Il proprietario, il sottoscrittore, o l’autorità di certificazione acquisiscono elementi che mettono in dubbio la validità del certificato;
3. Sono presenti dubbi riguardanti la salvaguardia del dispositivo di conservazione delle chiavi e delle quantità di autenticazione;
4. È necessaria un’interruzione della validità del certificato.

La sospensione per i certificati TSU non è disponibile.

4.9.13 Chi può richiedere la sospensione

Le persone o entità che possono richiedere la sospensione sono le stesse contenute nell'elenco presente nel paragrafo 4.9.2 del presente TSPPS.

4.9.14 Procedura di sospensione e richieste di riattivazione

Gli strumenti e le procedure disponibili sono gli stessi usati per invocare la revoca dei certificati come indicato nel paragrafo 4.9.3.

4.9.15 Limiti al periodo di sospensione

La sospensione è mantenuta per un periodo di dieci giorni, dopo i quali il certificato può essere automaticamente revocato o riattivato a seconda della configurazione richiesta dal cliente.

4.10 Servizi informativi sullo stato del certificato

Lo stato dei certificati qualificati è messo a disposizione sul server **crl.time4mind.com** attraverso la pubblicazione di CRL secondo il protocollo HTTP [RFC7230] ed in conformità con la specifica [RFC 5280].

Lo stato dei certificati è inoltre reso disponibile online attraverso un servizio basato sul protocollo OCSP (On-line Certificate Status Protocol) in conformità con la specifica [RFC2560].

Gli indirizzi per l'accesso ai servizi di revoca sono inseriti all'interno dei certificati utente, in particolare l'indirizzo delle CRL è inserito nell'estensione CRLDistributionPoints mentre l'indirizzo del server OCSP viene inserito nell'estensione AuthorityInformationAccess.

I Servizi sono ad accesso pubblico.

4.10.1 Disponibilità del Servizio

L'accesso ai servizi CRL e OCSP è sempre disponibile (24 x 7).

4.11 Cessazione del contratto

Il contratto tra la CA ed il titolare si intende cessato quando il certificato scade o viene revocato, salvo il caso in cui vi siano condizioni diverse che possono essere previste nei contratti stipulati con i clienti.

4.12 Key Escrow e Ripristino

Il recupero della chiave è disponibile solamente per chiavi di CA e TSU in caso di cancellazione accidentale o guasto degli HSM. Allo scopo, la CA mantiene una coppia di chiavi CA e TSU in backup che possono venire ripristinate seguendo le procedure previste dall'HSM in uso e sotto doppio controllo degli operatori.

5 CONTROLLI DELLE STRUTTURE DI GESTIONE E OPERATIVI

I controlli di gestione, operativi, procedurali, del personale e fisici (sicurezza non tecnica) utilizzati da Intesi Group S.p.A. per quanto riguarda il servizio qualificato sono in conformità con le norme tecniche EN 319 411-1 per l'emissione di certificati non qualificati, EN 319 411-2 per l'emissione di certificati qualificati, EN 319 421 per emissione di marche temporali, e Intesi Group ISO/IEC 27001 Sistema di Gestione della Sicurezza delle Informazioni certificato.

La policy di sicurezza delle informazioni di Intesi Group, così come la documentazione sui controlli di sicurezza e le procedure operative, sono disponibili sul Piano di Sicurezza e su altri documenti riservati, a disposizione solo del personale autorizzato di Intesi Group, degli auditor e dell'Autorità di Vigilanza italiana.

5.1 Sicurezza fisica

Tutti i sistemi informatici utilizzati per la prestazione di servizi fiduciari qualificati descritti nel presente documento sono ospitati nelle banche dati di Intesi Group, le quali garantiscono:

- un sistema di **controllo all'accesso fisico**, in modo tale che l'accesso all'edificio sia permesso esclusivamente a personale autorizzato;
- che l'accesso ai servizi TSP sia permesso esclusivamente a personale autorizzato in possesso di un pass personale e del PIN corrispondente;
- sorveglianza video
- un **sistema di protezione antincendio** che include **antifumo** (VEWASD) e impianto di estinzione apposito;
- un **sistema di alimentazione** completamente ridondante a tutti i livelli (trasformatori, centri di energia, generatori, UPS, pannelli di distribuzione, etc.)
- un sistema di **aria condizionata** (HVAC) che garantisce condizioni di lavoro ottimali;
- **connettività Internet** ridondante, con una capacità di almeno doppia rispetto al necessario.

5.2 Controlli procedurali

Intesi Group S.p.A. conduce una valutazione dei rischi per esaminare i rischi commerciali e determinare i requisiti di sicurezza necessari e le procedure operative. L'analisi di rischio viene eseguita con pieno supporto e collaborazione di tutti i fornitori di servizi componenti ed è regolarmente revisionata e corretta dove necessario. L'analisi di rischio fa parte della documentazione riservata. I servizi, le infrastrutture e le misure per la gestione della sicurezza delle informazioni vengono costantemente monitorate e periodicamente riviste. Qualsiasi cambiamento che vada a impattare sul livello di sicurezza fornito deve essere approvato del Security e RA Officer.

Le procedure operative sono documentate nel Sistema di Gestione della Qualità aziendale, certificato in conformità con lo standard ISO 9001.

5.3 Controlli di sicurezza del personale

Tutti i membri del personale coinvolto nella fornitura di servizi fiduciari sono dipendenti di Intesi Group S.p.A. o personale autorizzato e qualificato. Tutti i membri sono soggetti alle procedure di gestione del personale seguite da Intesi Group allo scopo di offrire ragionevole certezza sull'affidabilità e competenza dei membri del personale nei campi di tecnologie relative alla firma digitale e tecnologie relative alla validazione temporale.

Il personale coinvolto nello sviluppo e gestione del servizio di validazione temporale viene adeguatamente formato sulle procedure e gli strumenti da utilizzare durante le varie fasi operative.

I ruoli assegnati al personale vengono definiti in conformità con ETSI EN 319 401 e sono:

1. **Security e RA Officer**: ha la responsabilità della sicurezza delle informazioni e del rispetto della policy aziendale della sicurezza
2. **TSP Operation Officer:** ha la responsabilità del servizio di certificazione e validazione temporale.
3. **System Administrator:** ha la responsabilità della conduzione tecnica dei sistemi.
4. **System Operation Officer:** ha la responsabilità dei servizi tecnici e logistici.
5. **System Operator:** ha la responsabilità del funzionamento dei servizi e riporta al System Operation Officer.
6. **System Auditor:** ha la responsabilità delle verifiche e delle ispezioni (auditing).

Tutto il personale che operano sui servizi fiduciari ha ricevuto mandato attraverso apposita lettera di incarico.

5.4 Procedure di registrazione degli audit

5.4.1 Tipo di eventi registrati

I principali eventi pertinenti alle operazioni del servizio di certificazione sono registrati in forma elettronica. Gli eventi registrati sono:

- Tutti gli eventi relativi al ciclo di vita delle chiavi di CA.
- Tutti gli eventi relativi all'operazione di identificazione.
- Eventi relativi a operazioni sul ciclo di vita del certificato, quali:
    - Generazione della chiave del soggetto;
    - Emissione del certificato;
    - Revoca del certificato;
    - Sospensione del certificato;
    - Pubblicazione di una CRL.
- Tutti gli altri servizi di certificazione dispongono di sistemi di registrazione di eventi relativi ad ogni operazione svolta.
- Accesso fisico alla banca dati.
- Accesso fisico all'area server TSP.
- Accesso logistico a tutti i sistemi TSP.
- Eventi relativi al ciclo di vita del certificato.
- Eventi relativi alla sincronizzazione dell'orologio.
- Eventi relativi al rilascio e all'aggiornamento di software.

Per ogni evento vengono inoltre registrate informazioni riguardo al tipo, la data e l'ora dell'evento. La fonte per l'orario è l'orologio di sistema che viene mantenuto allineato da un servizio NTP.

5.4.2 Frequenza di elaborazione del registro

Gli audit log vengono elaborati continuamente e/o in seguito ad un allarme o una anomalia. Gli audit log vengono archiviati quotidianamente.

5.4.3 Periodo di detenzione per un registro audit

I file di log vengono conservati per 20 anni.

5.4.4 Protezione di un registro audit

Il sistema di archiviazione dei log è dotato di un processo che controlla costantemente la consistenza e l'immutabilità dei file di log archiviati. In caso di incongruenze, lancia un allarme al sistema di monitoraggio.

L'accesso al registro può essere effettuato dal personale di Intesi Group che ha il ruolo di "System Administrator" o di "System Auditor".

5.4.5 Procedure di backup del registro audit

I file di log vengono salvati sul sistema di backup secondo procedure interne.

5.4.6 Sistema di raccolta di audit (interno vs. esterno)

I sistemi di audit sono parte integrante della CA.

5.4.7 Notifica al soggetto di evento scatenante

Se necessario, Intesi Group notifica al soggetto un evento scatenato dall'audit.

5.4.8 Vulnerability assessment

Il vulnerability assessement relativo ai sistemi di audit log fa parte dell'analisi del rischio condotta da Intesi Group S.p.A. ed è disponibile come documento interno e riservato.

5.5 Archiviazione delle registrazioni

5.5.1 Tipi di informazioni archiviate

La CA conserva le seguenti informazioni relative all'emissione e gestione dei certificati:

- Registrazione di eventi rilevanti (emissione, revoca, sospensione ecc.);

- Tutti i file di log dei sistemi coinvolti nel servizio CA;
- Dati identificativi, copia digitale dei documenti di identificazione e azioni di approvazione del contratto.

Il sistema di archiviazione dei log è controllato da un processo che mantiene sotto controllo la consistenza e l'immutabilità dei file di registro archiviati. Nel caso in cui siano rilevate incongruenze, viene avviato un allarme sul sistema di monitoraggio.

L'accesso ai log è consentito solamente al personale di Intesi Group che ricopre il ruolo di "System Administrators" e di "System Auditor".

5.5.2 Periodo di conservazione di un registro audit

I file di registro vengono mantenuti per 20 anni.

5.5.3 Protezione dell'archivio

Il sistema di archiviazione dei log è controllato da un processo che mantiene sotto controllo la consistenza e l'immutabilità dei file di log archiviati. Nel caso in cui rilevi incongruenze, lancia un allarme al sistema di monitoraggio in modo che un "System Administrator" possa immediatamente intervenire e trattare il problema seguendo procedure interne di Intesi Group.

L'accesso ai log è consentito solamente al personale di Intesi Group che ricopre il ruolo di "System Administrators" e di "System Auditor".

5.5.4 Procedure di backup degli archivi

Rif. Paragrafo 5.5.3.

5.5.5 Marcatura temporale degli archivi

Intesi Group garantisce che venga registrato il momento preciso di archiviazione di tutti gli eventi, informazioni e documenti elencati nelle sezioni 5.4 e 5.5; il tempo viene acquisito attraverso il

servizio NTP attraverso cui sono allineati tutti gli orologi dei sistemi. Il servizio NTP è configurato in modo da garantire una precisione di orario di pochi millisecondi rispetto al Tempo Universale Coordinato.

5.5.6 Procedura di recupero e verifica delle informazioni archiviate

I file di log vengono conservati solamente in formato elettronico e sono accessibili solamente da personale autorizzato di Intesi Group, come descritto nelle procedure interne.

I titolari o le terze parti possono avere accesso alle informazioni relative al certificato contattando Intesi Group all'indirizzo email indicato nel paragrafo 1.5.

5.6 Rinnovo della Chiave CA

Per la generazione del certificato di CA viene applicata la procedura di key ceremony valida al momento della creazione.

5.7 Compromissione e disaster recovery

5.7.1 Procedure di gestione degli incidenti e delle compromissioni

Le procedure di segnalazione e gestione degli incidenti e/o compromissioni, le procedure di ripristino in caso di disastro ed il Business Continuity Plan sono stati definiti e sono disponibili come documentazione interna.

Tutte queste procedure sono conformi allo standard ISO/IEC 27001. Tutti gli eventi riguardanti incidenti e/o compromissioni vengono documentati e archiviati insieme ai log pertinenti come descritto nella sezione 5.5 del TSPPS.

5.7.2 Corruzione di risorse informatiche, software e/o dati

Intesi Group S.p.A. ha stabilito tutte le misure necessarie atte a garantire, con un elevato grado di automazione, un ripristino completo dei servizi di certificazione in caso di disastro, corruzione dei server, del software o dei dati. Tutte queste misure sono conformi alla procedura ISO/IEC 27001.

Il sito di Disaster Recovery e tutte le risorse necessarie al ripristino sono mantenute ad una distanza ragionevole dalle risorse di produzione, in modo da evitare che un disastro possa corrompere entrambi i siti. Comunicazioni sufficientemente rapide vengono stabilite tra il sito originale e il sito remoto, in modo da assicurare il costante allineamento e l'integrità dei dati. Infrastrutture di comunicazione sicura vengono istituite da entrambi i siti per le RA, lo stato di revoca del certificato ed i servizi di conservazione.

Le procedure di disaster recovery vengono testate in modo integrale almeno una volta all'anno, alla presenza di almeno un membro di Intesi Group.

5.7.3 Procedure in caso di compromissione della chiave privata

La compromissione della(e) chiave(i) privata(e) CA comporta la revoca immediata del certificato relativo alle chiavi compromesse. Le misure prese in seguito alla revoca sono:

- Fermare i servizi qualificati coinvolti.
- Revocare tutti i certificati utente diventati inaffidabili a causa dell'evento;
- Pubblicare immediatamente la CRL con le informazioni di revoca;
- Informare i clienti e gli utenti finali dell'avvenuta compromissione della chiave;
- Informare Agid.

Solo dopo aver esaminato la causa del problema ed avere messo in atto tutte le misure necessarie alla risoluzione, Intesi Group procederà alla generazione di una nuova coppia di chiavi e di un nuovo certificato di CA che invierà ad Agid per renderlo pubblico attraverso la propria TSL. In seguito alla pubblicazione Intesi Group procederà alla riattivazione del servizio qualificato.

5.7.4 Continuità operative a fronte di un disastro

Intesi Group S.p.A. stabilisce le misure necessarie allo scopo di garantire un ripristino completo della Certification Authority in caso di disastro, corruzione di server, software o dati. Tutte queste misure sono conformi allo standard ISO/IEC 27001. Intesi Group dispone di un proprio "Contingency Plan" che descrive tutti i processi da mettere in atto per garantire la continuità operativa a seguito di un disastro naturale.

5.8 Terminazione della CA

In caso di terminazione, il TSP prenderà ogni misura necessaria per ridurre al minimo i disagi per i possessori del certificato e gli utilizzatori; in particolare il TSP dovrà:

- Almeno 60 giorni prima della terminazione, informare tutti i clienti ed i detentori di certificati;
- Pubblicare una nota sul sito web;
- Chiudere tutti i contratti con qualsiasi fornitore coinvolto;
- Prima della data effettiva di terminazione, trasferire da un altro TSP le informazioni di registrazione, le informazioni sullo stato dei certificati e tutti i log rilevanti; Nel caso in cui non riesca ad individuare un TSP invierà i dati ad AgID.
- Al momento della terminazione, distruggere le proprie chiavi private di CA e TSU, se non vengono prese in carico da un altro TSP in conformità con la normativa vigente.

6 MISURE DI SICUREZZA TECNICA

Le misure di sicurezza prese da Intesi Group S.p.A. per:

- la protezione delle proprie chiavi crittografiche di CA, dei dati di attivazione, dei repository, dei soggetti e delle loro Chiavi Private, dei dati di accesso alle Chiavi Private e ai parametri di sicurezza critici,

- la gestione sicura delle chiavi,
- i controlli di sicurezza tecnica utilizzati da Intesi Group S.p.A. durante la generazione delle chiavi, autenticazione dell'utente, emissione di certificato, revoca di certificato, auditing, archiviazione

sono conformi con ai seguenti standard:

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

Tutti controlli sono descritti ulteriormente di seguito.

6.1 Generazione e installazione di una coppia di chiavi

6.1.1 Generazione di una coppia di chiavi

6.1.1.1 Root CA

La procedura di generazione della CA viene eseguita da due operatori di Intesi Group seguendo la procedura di Key Ceremony descritta come procedura interna di Intesi Group. L'esecuzione della procedura di generazione della chiave viene registrata su un apposito verbale di generazione che viene conservato per 20 anni.

La coppia di chiavi viene generata all'interno di un apposito HSM (Hardware Security Module) installato nella sala macchine di Intesi Group in un'area ad accesso controllato. L'HSM utilizzato è certificato in conformità allo standard di sicurezza FIPS PUB 140-2 Level 3 e Common Criteria (ISO 15408) EAL 4.

6.1.1.2 Certificato utente

La generazione della coppia di chiavi del titolare avviene su un dispositivo certificato QSCD presente nell'infrastruttura Intesi Group e viene registrata dal sistema di auditing interno.

6.1.1.3 Certificato TSU

La generazione della coppia di chiavi TSU avviene in un ambiente fisicamente protetto, in conformità con le procedure interne riguardanti i sistemi di marcatura temporale e viene registrata dall'auditor interno di Intesi Group.

La coppia di chiavi usata dal servizio di marcatura temporale viene generata all'interno di un HSM (Hardware Security Module) certificato in conformità allo standard di sicurezza FIPS PUB 140-2 Level 3 e Common Criteria (ISO 15408) EAL 4.

6.1.2 Consegna della chiave privata al titolare

Le chiavi private sono generate e conservate su un dispositivo QSCD sito nella sala macchine di Intesi Group. L'accesso alla chiave privata avviene attraverso le interfacce messe a disposizione dal dispositivo e solamente dopo avere eseguito una autenticazione con successo.

6.1.3 Consegna della chiave pubblica all'emittente del certificato

Le chiavi pubbliche vengono inviate dalle RA, attraverso i software messi a disposizione da Intesi Group, al servizio di certificazione sotto forma di una richiesta PKCS#10 utilizzando un canale HTTP protetto da un protocollo TLS v 1.2. Ogni RA deve avere un certificato di autenticazione da utilizzare per inviare le richieste alla CA.

6.1.4 Distribuzione della chiave pubblica della CA

Le chiavi pubbliche dei certificati di CA vengono distribuite attraverso la pubblicazione sulla sezione CA del portale web di Intesi Group (www.intesigroup.com) e attraverso la Trust-service List (TSL) distribuita da Agid.

6.1.5 Dimensioni delle chiavi

Le chiavi Root CA vengono generate con l'algoritmo RSA ed hanno lunghezza 4096 bits.

Le chiavi per i certificati dei titolari e per certificati di TSU vengono generate con l'algoritmo RSA ed hanno lunghezza 2048 bits.

6.1.6 Generazione dei parametri e qualità della chiave pubblica

La generazione della chiave pubblica ed il controllo durante la generazione della coppia di chiavi CA vengono realizzati in conformità con il presente TSPP.

La procedura di generazione della chiave pubblica viene regolarmente riesaminata per garantire i massimi criteri di sicurezza disponibili.

6.1.7 Key Usage (estensione X.509 v3)

6.1.7.1 Root CA

Il certificato di root include l'estensione KeyUsage valorizzata a:

- keyCertSign (firma certificati)
- cRLSign (firma CRL)

Per ulteriori dettagli, vedere il capitolo 7.

6.1.7.2 Firma e sigillo

Il certificato qualificato include l'estensione KeyUsage valorizzata a:

- Non-repudiation

Per ulteriori dettagli, vedere il capitolo 7.

6.1.7.3 TSU

Il certificato TSU include l'estensione KeyUsage valorizzata a:

- Digital Signature

Il certificato TSU contiene inoltre l'extended key usage valorizzato a:

- Timestamping.

Per ulteriori dettagli, vedere il capitolo 7.

6.2 Protezione della Chiave Privata e Sicurezza del Modulo Crittografico

6.2.1 Norme e controlli del modulo crittografico

La chiave privata usata dalle root CA è mantenuta all'interno di un HSM (Hardware Security Module) che ha conseguito una certificazione di sicurezza FIPS PUB 140-2 Level 3 e Common Criteria (ISO 15408) EAL 4.

Le chiavi private usate per i certificati utente (firma e sigillo) sono generate e mantenute all'interno di un dispositivo certificato QSCD (Qualified Electronic Signature Creation Device).

6.2.2 Controllo multi-utente della chiave privata (n di m)

L'accesso ai dispositivi contenenti le chiavi private CA e TSU è disponibile attraverso la simultanea autenticazione di due operatori.

L'accesso alle chiavi private relative a certificati qualificati per firma digitale e sigillo può essere eseguito solamente dal titolare attraverso l'uso delle quantità di autenticazione che ha definito durante l'emissione del certificato e utilizzando le interfacce messe a disposizione del dispositivo QSCD.

6.2.3 Ripristino della chiave privata

Il Ripristino della chiave privata non è consentito.

6.2.4 Backup della chiave privata

Allo scopo di garantire continuità del servizio, Intesi Group mantiene una copia cifrata delle chiavi della CA e delle TSU su un supporto rimovibile. La copia di backup è custodita in un luogo sicuro, diverso da quello in cui si trova la copia operativa. Le procedure di backup e ripristino delle chiavi sono definite e richiedono sempre l'intervento combinato di almeno due persone ("dual control").

Il backup ed il ripristino della chiave degli utenti non sono applicate ad eccezione del ripristino in caso di disastro come descritto all'interno del presente TSPPS e del relativo TSPP.

6.2.5 Archivio della chiave privata

Non applicabile.

6.2.6 Trasferimento della chiave privata tra moduli crittografici

Non applicabile.

6.2.7 Conservazione della chiave privata su un modulo crittografico

Le chiavi private sono generate e conservate in una zona protetta e a prova di manomissione dei dispositivi crittografici gestiti da Intesi Group

6.2.8 Metodo di attivazione della chiave privata

Le chiavi private delle CA e delle TSU sono attivate utilizzando le procedure previste dal fornitore dell'HSM e coerenti con la relativa certificazione di sicurezza e sempre sotto il doppio controllo di due operatori autorizzati.

Le chiavi private relative a certificati di firma e sigillo possono essere attivate solamente dal titolare utilizzando le credenziali di autenticazione definite durante la fase di emissione del certificato (vedi par. 4.2) e coerentemente con le procedure previste dalla certificazione QSCD.

6.2.9 Metodo di disattivazione della chiave privata

Le chiavi private delle CA e delle TSU possono essere disattivate utilizzando le procedure previste dal fornitore dell'HSM e sempre sotto doppio controllo di due operatori.

Le chiavi private relative a certificati di firma e sigilli possono essere disattivate solamente dall'utente titolare chiudendo la sessione di lavoro aperta attraverso l'autenticazione, coerentemente con le procedure previste dal QSCD.

6.2.10 Metodo di distruzione della chiave privata

Le chiavi delle CA e delle TSU sono distrutte attraverso la distruzione sicura del supporto primario e del relativo supporto di backup seguendo una apposita procedura interna. La distruzione delle chiavi di CA è eseguita sotto doppio controllo di due operatori.

Le chiavi private dei soggetti titolari, al termine del periodo di validità del certificato corrispondente, sono eliminate automaticamente dai moduli di sicurezza attraverso un apposito processo che assicura l'impossibilità di recuperarle e di riutilizzarle di nuovo.

6.2.11 Valutazione del modulo crittografico

Vedi par 6.2.1

6.3 Altri Aspetti sulla gestione delle coppie di chiavi

6.3.1 Archivio delle chiavi pubbliche

Vedere la sezione 5.5.

6.3.2 Periodi operativi del certificato e di utilizzo della coppia di chiavi

Il periodo di utilizzo della coppia di chiavi corrisponde al periodo di validità indicato nel relativo certificato.

I Certificati TSU hanno una validità di dieci anni ed un periodo di utilizzo di tre mesi.

6.4 Dati di attivazione

Intesi Group S.p.A. garantisce che i dati di attivazione associati alle chiavi private di CA e delle TSU siano generati, conservati e archiviati in sicurezza, come descritto nelle sottosezioni 6.1 e 6.2.

I dati di attivazione delle chiavi private relative a certificati digitali (firma e sigillo) sono definiti dal titolare durante la fase di emissione in modo tale che sia l'unico a conoscerle. I titolari sono responsabili della gestione e della protezione in sicurezza dei dati di attivazione privati. Per dettagli vedere la sezione 4.1.2 del presente documento ed il relativo TSPP. Il processo di registrazione ed emissione di Intesi Group assicura la segretezza dei dati di attivazione dei certificati proteggendo tutte le comunicazioni tra i componenti dell'infrastruttura attraverso un canale sicuro TLS/SSL e salvando tutte le informazioni in forma cifrata.

6.5 Controlli di sicurezza informatica

Intesi Group garantisce che le procedure ed i controlli di sicurezza informatica sono conformi ai requisiti contenuti negli standard tecnici ETSI EN 319 411-1 e ETSI EN 319 411-2. Le procedure interne di Intesi Group sono certificate ISO/IEC 27001.

Le procedure applicate sono descritte in documenti interni.

6.6 Controlli tecnici sul ciclo di vita

I controlli sul ciclo di vita dello sviluppo sono realizzati in conformità con i requisiti di sicurezza contenuti negli standard ETSI EN 319 411-1 e con ETSI EN 319 411-2 e sono definite nella procedura di qualità ISO 9001 e nelle policy di sicurezza ISO 27001.

6.7 Controlli di sicurezza di rete

I controlli di sicurezza della rete sono effettuati attraverso l'uso di: firewall, comunicazioni protette da autenticazione, sistemi di intrusion detection, protezione anti-virus, sicurezza dei siti web, sicurezza delle banche dati e altre risorse di protezione e sono realizzati in conformità i requisiti contenuti negli standard ETSI EN 319 411-1 e con ETSI EN 319 411-2.

Descrizioni dettagliate dei controlli di sicurezza di rete eseguiti sono disponibili come documenti interni.

6.8 CA e marcatura temporale

Tutti i sistemi informatici usati dalle CA e dal servizio di marcatura temporale sono sincronizzati con il protocollo NTP (Network Time Protocol) che si allinea usando fonti orarie "Stratum 1" per garantire una precisione di orario di pochi millisecondi rispetto al Tempo Universale Coordinato.

7 PROFILI DEI CERTIFICATI E DELLE CRL

I certificati sono conformi allo standard ISO/IEC 9594-8:2005 [X.509] e alla specifica pubblica [RFC 5280].

Per quanto riguarda gli algoritmi crittografici, la lunghezza minima delle chiavi, i parametri delle chiavi e le funzioni di hashing, la CA è conforme allo standard ETSI TS 119 312.

7.1 Profilo del certificato

7.1.1 CA per il certificato di Marcatura Temporale

Campo	Valore
Version Number	V3
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
IssuerDistinguishedName	CN=Intesi Group EU Qualified Time-Stamp CA G2, OU=Qualified Trust Service Provider, O = Intesi Group S.p.A., 2.5.4.97 = VATIT-02780480964, C = IT
Validity	<20 years>
SubjectDistinguishedName	CN=Intesi Group EU Qualified Time-Stamp CA G2, OU=Qualified Trust Service Provider, O = Intesi Group S.p.A., 2.5.4.97 = VATIT-02780480964, C = IT
SubjectPublicKeyInfo	<RSA public key of 4096 bits>
Signature Value	<Root CA signature>
Estensione del certificato	**Valore**
Basic Constraints	critical: CA=true
Authority Key Identifier (AKI)	<public key SHA1-digest>
Subject Key Identifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: keyCertSign, cRLSign
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
CRLDistributionPoints (CDP)	<not included>

7.1.2 CA per il certificato di Firma Elettronica Qualificata

Field	Value
Version Number	V3
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Signature CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OID.2.5.4.97=VATIT-02780480964, C=IT
Validity	<20 years>
SubjectDistinguishedName	CN=Intesi Group EU Qualified Electronic Signature CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OID.2.5.4.97=VATIT-02780480964, C=IT
SubjectPublicKeyInfo	<RSA public key of 4096 bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**
Basic Constraints	critical: CA=true
Authority Key Identifier (AKI)	<public key SHA1-digest>
Subject Key Identifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: keyCertSign, cRLSign
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
CRLDistributionPoints (CDP)	<not included>

7.1.3 CA per il Sigillo Elettronico Qualificato

Campo	Valore
Version Number	V3
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)

Campo	Valore
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Seal CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OrganizationIdentifier=VATIT-02780480964, C=IT
Validity	<20 years>
SubjectDistinguishedName	CN=Intesi Group EU Qualified Electronic Seal CA, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OrganizationIdentifier=VATIT-02780480964, C=IT
SubjectPublicKeyInfo	<RSA public key of 4096 bits>
Signature Value	<Root CA signature>
Estensione del certificato	**Valore**
Basic Constraints	critical: CA=true
Authority Key Identifier (AKI)	<public key SHA1-digest>
Subject Key Identifier (SKI)	<public key SHA1-digest>
KeyUsage	critical: keyCertSign, cRLSign
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
CRLDistributionPoints (CDP)	<not included>

7.1.4 Certificato per TSU

Campo	Valore
Version Number	V3 (2)
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
IssuerDistinguishedName	CN=Intesi Group Qualified Time-Stamp CA G2, O=Intesi Group S.p.A., OU=Qualified Trust Service Provider, OrganizationIdentifier=VATIT-02780480964, C=IT

Campo	Valore
Validity	<10 years>
SubjectDistinguishedName	CN=Time-Stamping Authority TSU1, O=Intesi S.p.A., OrganizationIdentifier=VATIT-02780480964, C=IT
SubjectPublicKeyInfo	<RSA public key of 2048 bits>
Signature Value	<Root CA signature>
Estensione del certificato	**Valore**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
Subject Key Identifier (SKI)	<included>
KeyUsage	Critical: Digital Signature
Extended Key Usage (EKU)	Critical: Time Stamping
CertificatePolicies	PolicyOID = 1.3.6.1.4.1.48990.1.1.5.1 TSPPS-URI = http://www.intesigroup.com/en/documents
CRLDistributionPoints (CDP)	http://crl.time4mind.com/Intesi/CloudRootCA.crl
QCStatement	ETSI Qualified Certificate compliance esi4-qcStatement-1 (0.4.0.1862.1.1)
Basic Constraints	<not included>
Policy Mappings	<not included>
Name constraints	<not included>
Policy constraints	<not included>
Inhibit any-policy	<not included>
SubjectAlternativeName (SAN)	<not included>
IssuerAlternativeName	<not included>
Subject directory attributes	<not included>

7.1.5 Certificato per Firma Elettronica Qualificata

Field	Value
Version Number	V3 (2)

Field	Value
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Signature CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OrganizationIdentifier=VATIT-02780480964, C=IT
Validity	<max 5 years>
SubjectDistinguishedName	serialNumber=<see id-etsi-qcs-SemanticsId-Natural>, G=<Subject name>, SN=<Subject surname>, dnQualifier=<CA Internal identifier> CN=<Name Surname>, O=<Optional: subject organization>, OrganizationIdentifier=<Optional: subject organization Identifier> C=<ISO 3166 Country code>
SubjectPublicKeyInfo	<RSA public key of 2048 bits>
Signature Value	<Root CA signature>
Certificate extension	**Value**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
Subject Key Identifier (SKI)	<included>
KeyUsage	Critical: non-repudiation
CertificatePolicies	Not Critical: • PolicyOID = 0.4.0.194112.1.2 (QCP-n-qscd) • PolicyOID = 1.3.6.1.4.1.48990.1.1.1.1 • TSPPS-URI = http://www.intesigroup.com/en/documents
CRLDistributionPoints (CDP)	Not Critical: http://crl.time4mind.com/Intesi/qualifiedsignatureCA.crl
Authority Information Access (AIA)	Not Critical: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) http://ocsp.time4mind.com 1.3.6.1.5.5.7.48.2 (id-ad-caIssuers) http://caissuers.time4mind.com/Intesi/qualifiedsignatureCA.crt
QCStatement	PKIX QCSyntax-v2

Field	Value
	qcStatement-2 (0.4.0.194121.1.1) id-etsi-qcs-semanticsId-Natural
	ETSI Qualified Certificate compliance esi4-qcStatement-1 (0.4.0.1862.1.1)
	ETSI retention period esi4-qcStatement-3 (0.4.0.1862.1.3) QcEuRetentionPeriod: 20
	ETSI QCS SSCD esi4-qcStatement-4 (0.4.0.1862.1.4)
	ETSI PDS esi4-qcStatement-5 (0.4.0.1862.1.5) url:http://www.intesigroup.com/en/documents language: en
	ETSI type esi4-qcStatement-6 (0.4.0.1862.1.6) QcType: id-etsi-qct-esign
Basic Constraints	<not included>
Policy Mappings	<not included>
Name constraints	<not included>
Policy constraints	<not included>
Inhibit any-policy	<not included>
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
IssuerAlternativeName	<not included>
Subject directory attributes	<not included>

7.1.6 Certificato per il Sigillo Elettronico Qualificato

Campo	Valore
Version Number	V3 (2)
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)

Campo	Valore
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Seal CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., OrganizationIdentifier=VATIT-02780480964, C=IT
Validity	<max 5 years>
SubjectDistinguishedName	dnQualifier=<CA Internal identifier> CN=<Commonly used organization name>, O=<subject organization>, OrganizationIdentifier=<subject organization Identifier> C=<ISO 3166 Country code>
SubjectPublicKeyInfo	<RSA public key of 2048 bits>
Signature Value	<Root CA signature>
Estensione del certificato	**Valore**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
Subject Key Identifier (SKI)	<included>
KeyUsage	Critical: non-repudiation
CertificatePolicies	Not Critical: • PolicyOID = 0.4.0.194112.1.3 (QCP-l-qscd) • PolicyOID = 1.3.6.1.4.1.48990.1.1.2.1 • TSPPS-URI = http://www.intesigroup.com/en/documents
CRLDistributionPoints (CDP)	Not Critical: http://crl.time4mind.com/Intesi/qualifiedsealCA.crl
Authority Information Access (AIA)	Not Critical: 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) http://ocsp.time4mind.com 1.3.6.1.5.5.7.48.2 (id-ad-caIssuers) http://caissuers.time4mind.com/Intesi/qualifiedsealCA .crt
QCStatement	PKIX QCSyntax-v2 qcStatement-2 (0.4.0.194121.1.2) id-etsi-qcs-semanticsId-Legal
	ETSI Qualified Certificate compliance esi4-qcStatement-1 (0.4.0.1862.1.1)

Campo	Valore
	ETSI retention period esi4-qcStatement-3 (0.4.0.1862.1.3) QcEuRetentionPeriod: 20
	ETSI QCS SSCD esi4-qcStatement-4 (0.4.0.1862.1.4)
	ETSI PDS esi4-qcStatement-5 (0.4.0.1862.1.5) url: http://www.intesigroup.com/en/documents language: en
	ETSI type esi4-qcStatement-6 (0.4.0.1862.1.6) QcType: id-etsi-qct-eseal
Basic Constraints	<not included>
Policy Mappings	<not included>
Name constraints	<not included>
Policy constraints	<not included>
Inhibit any-policy	<not included>
Extended Key Usage (EKU)	<not included>
SubjectAlternativeName (SAN)	<not included>
IssuerAlternativeName	<not included>
Subject directory attributes	<not included>

7.2 Profilo CRL

Le CRL sono conformi allo Standard Internazionale ISO/IEC 9594-8:2005 [X.509] e alla specifica pubblica [RFC 5280].

Oltre alle informazioni obbligatorie, le CRL contengono anche i seguenti campi:

- *nextUpdate* (data della prossima emissione della CRL)
- *CRLNumber* (numero sequenziale della CRL)

ed In corrispondenza con ogni elemento del CRL, è presente l'estensione *reasonCode* allo scopo di indicare il motivo della revoca.

Le CRL sono firmate utilizzando l'algoritmo di hashing sha256WithRSAEncryption (1.2.840.113549.1.1.11).

8 VERIFICHE DI CONFORMITÀ

I controlli sulla infrastruttura tecnica, la sicurezza fisica e logica, le diverse procedure operative, ed il personale assunto allo scopo di fornire il servizio di TSP descritti nel presente TSPPS sono uguali a quelli definiti nelle direttive europee relative all'emissione di certificati qualificati.

Intesi Group è un Qualified Trust Service Provider (QTSP); pertanto, Intesi Group opera sotto la supervisione di AgID. Intesi Group esegue audit interni e periodiche valutazioni di conformità da parte di un Organismo di Valutazione di Conformità accreditato in base alla Regolamentazione eIDAS.

8.1 Frequenza o circostanze di valutazione

Intesi Group si impegna a fare il necessario in modo che, almeno ogni 12 mesi, venga eseguito un audit di conformità, coinvolgendo un Conformity Assessment Body (CAB) accreditato in base alla Regolamentazione eIDAS.

Gli audit interni vengono eseguiti in base a una pianificazione che offre diversi periodi (da mensile ad annuale) per i vari aspetti tecnico-operativi del servizio CA.

8.2 Identità e qualificazione degli auditor

Gli audit interni sono eseguiti dall'auditor interno di Intesi Group, il quale è adeguatamente qualificato per questo compito. Gli audit esterni vengono eseguiti da un Conformity Assessment Body accreditato in base alla Regolamentazione eIDAS.

8.3 Relazioni tra la CA e gli ispettori

Tra la CA e qualsiasi auditor esterno non può esistere alcun tipo di relazione che influenzi i risultati degli audit in favore di Intesi Group.

L'auditor interno di Intesi Group non fa parte dell'unità organizzativa a capo delle operazioni TSP.

8.4 Argomenti coperti dalle verifiche

Gli audit eseguiti da auditor esterni (ovvero non AgID) sono volti a verificare la conformità di Intesi Group e dei servizi qualificati che eroga alla Regolamentazione eIDAS.

L'obiettivo principale dell'audit interno è accertarsi che Intesi Group rispetti le procedure operative interne e la loro conformità con il presente TSPPS.

8.5 Misure adottate in seguito a non conformità

In caso di non conformità, AgID richiederà alla CA di adottare misure correttive entro un certo periodo di tempo, sotto pena di sanzioni e revoca dell'accreditamento.

Le non conformità trovate dai CAB sono portate all'attenzione della dirigenza di Intesi Group che deve decidere come trattarle esaminando i singoli casi.

8.6 Comunicazione dei risultati

I risultati degli audit interni vengono presentati direttamente al management di Intesi Group, e condivisi con le altre parti interessate interne, attraverso un rapporto di audit.

Se rilevanti, e in base alla Regolamentazione eIDAS, gli incidenti di sicurezza verranno notificati alle parti interessate.

9 CONDIZIONI GENERALI DI SERVIZIO

I Termini & Condizioni generali del servizio CA descritti nel presente documento vengono fornite ai clienti in un documento separato, che deve essere accettato al momento della domanda, e che deve essere pubblicato sul sito web CA.

In caso di divergenza tra il presente TSPPS ed il documento separato “Termini & Condizioni”, quest’ultimo avrà la precedenza.

9.1 Tariffe del servizio

Le tariffe del servizio sono pubblicate sul sito web www.intesigroup.com e sono soggette a cambiamenti senza previa notifica. Condizioni diverse possono essere negoziate caso per caso.

9.2 Responsabilità finanziaria

Intesi Group ha stipulato la seguente assicurazione relativa alla propria prestazione ed ai propri obblighi previsti dal presente TSPPS:

- Assicurazione sulla Responsabilità Generale Commerciale,
- Assicurazione sulla Responsabilità Professionale/Errori e Omissioni.

Per tale assicurazione viene scelta una società con un rating non inferiore ad A- rispetto al Policy Holder's Rating nell'edizione corrente della Best's Insurance Guide.

9.3 Riservatezza delle informazioni commerciali

9.3.1 Ambito di applicazione delle informazioni confidenziali

Le seguenti informazioni sono trattate come confidenziali:

- tutti i dati forniti dai Richiedenti (futuri Titolari dei certificati) ad eccezione delle informazioni che devono essere inserite nei certificati o che per altre ragioni sono considerate non confidenziali (si veda il paragrafo 9.3.2);
- le richieste di emissione certificati;
- le richieste di sospensione o revoca dei certificati;
- le comunicazioni scambiate tra i partecipanti alla PKI (v. par. 1.3);
- i codici riservati forniti ai titolari (es. credenziali di accesso a siti, dati di attivazione delle chiavi private, ecc.) qualora siano generati dalla CA o transitino attraverso i sistemi della CA;
- le chiavi private dei titolari;
- i log dei sistemi di elaborazione della CA;
- i contratti con le RA esterne;

9.3.2 Informazioni considerate non confidenziali

Non sono considerate confidenziali tutte le informazioni che devono essere pubbliche per rispetto delle norme di legge o degli standard tecnici di riferimento dei servizi di certificazione (es. RFC 5280) o per esplicita richiesta del Titolare.

In particolare, le seguenti informazioni non sono considerate confidenziali:

- i certificati e le informazioni in essi contenute;
- le liste dei certificati sospesi o revocati (CRL);
- le informazioni sullo stato dei certificati erogate on-line dalla CA (es. via OCSP);

9.3.3 Responsabilità di protezione delle informazioni confidenziali

La CA assicura che le informazioni confidenziali siano protette fisicamente e/o logicamente da accessi non autorizzati (anche se per sola lettura) nonché dal rischio di perdita a seguito di disastri.

Tutte le informazioni confidenziali sono trattate dalla CA nel rispetto delle norme applicabili, in particolare quelle in materia di trattamento dei dati personali.

9.4 Riservatezza delle informazioni personali

L'informativa sul trattamento dei dati e la modalità di elaborazione dei dati degli utenti dei servizi è pubblica e liberamente scaricabile dal sito istituzionale di Intesi Group all'url:

https://www.intesigroup.com/it/privacy/

9.5 Diritti di proprietà intellettuale

All'interno del servizio regolato dal presente TSPPS, la CA non raccoglie e non elabora dati sensibili o dati giudiziari (in riferimento all'articolo 4 del suddetto Decreto [DLGS196]). Il presente TSPPS è proprietà di Intesi Group, il quale si riserva tutti i diritti associati allo stesso. Il sottoscrittore mantiene tutti i diritti sul proprio marchio commerciale (nome di marca) e il proprio nome di dominio. Per quanto riguarda di diritti di proprietà di altri dati e informazioni, si applica la legge vigente.

9.6 Obblighi e garanzie

9.6.1 Certification Authority

La CA si impegna a:

- operare in conformità con il presente TSPPS;
- identificare il sottoscrittore come descritto nel presente TSPPS;
- emettere e gestire i certificati come descritto nel presente TSPPS;
- fornire un servizio di sospensione e revoca efficiente per i certificati;
- garantire che il sottoscrittore, al momento dell'emissione del certificato, sia in possesso della chiave privata corrispondente;
- fornire informazioni tempestive rispetto a ogni eventuale compromissione della propria chiave privata;
- fornire informazioni chiare riguardo alle procedure e i requisiti del servizio;
- fornire una copia del presente TSPPS a chiunque ne faccia richiesta;
- garantire l'elaborazione dei dati personali in conformità con la legge vigente;
- fornire un servizio di informazione efficiente e affidabile rispetto allo stato dei certificati.

9.6.2 Registration Authority

Le attività RA vengono eseguite dai RAO e dalle LRA sotto l'obbligo contrattuale di attenersi scrupolosamente al presente TSPPS alle parti del relativo TSPP e alle procedure interne RA di Intesi Group.

Il servizio di Registration Authority non è applicabile per il servizio di Marcatura Temporale.

9.6.3 Sottoscrittori

Fare riferimento al documento "Termini e Condizioni" al capitolo 5.

9.6.4 Utilizzatori

Fare riferimento al documento “Termini e Condizioni” al capitolo 7.

9.7 Esclusione delle garanzie

Ad eccezione di quando espressamente menzionato altrove nel TSPPS, nel TSPP vigente e nella normativa in vigore, Intesi Group S.p.A. come TSP, declina ogni garanzia e obbligo di qualsiasi tipo, incluso ogni tipo di garanzia su commerciabilità, su adeguatezza a un particolare scopo e su esattezza delle informazioni fornite (salvo il fatto che esse giungono da una fonte autorizzata); Intesi Group, inoltre, declina ogni responsabilità per quanto riguarda la negligenza e la mancanza di cura da parte dei Sottoscrittori e degli Utilizzatori. Intesi Group S.p.A. non garantisce il “non ripudio” di qualsiasi Certificato o messaggio. Intesi Group S.p.A. non garantisce alcun software.

9.8 Limiti di Responsabilità

Fare riferimento al documento “Termini e Condizioni” al capitolo 8

9.9 Indennità

Fare riferimento al documento “Termini e Condizioni” al capitolo 8.

9.10 Durata e Terminazione

Il presente TSPPS è effettivo dal momento in cui viene pubblicato sul sito web CA (vedi capitolo 2) e sul sito AgID e rimarrà in vigore fino al momento in cui viene sostituito da una nuova versione.

9.11 Emendamenti

Intesi Group si riserva il diritto di modificare il presente TSPPS in qualunque momento senza previa notifica.

9.12 Risoluzione Dispute

I Sottoscrittori possono presentare le proprie richieste e reclami inviando una email all'indirizzo:

tsp@intesigroup.com.

I reclami ricevuti da Intesi Group saranno esaminati dal personale addetto di Intesi Group allo scopo di risolvere ogni disputa con efficienza e rapidità.

Ogni controversia che non possa essere risolta direttamente da Intesi Group verrà presentata presso la competenza esclusiva della Corte di Milano, ad eccezione per le condizioni applicabili nel caso in cui il Sottoscrittore sia qualificabile come Cliente in base al Decreto Legislativo italiano 206/2005.

9.13 Legge Applicabile

Il contratto è soggetto alla Legge Italiana ed Europea e come tale sarà interpretato ed eseguito. Per quanto non espressamente previsto dal contratto, il servizio di CA sarà regolato dalle norme vigenti.

9.14 Conformità con le norme applicabili

Le leggi vigenti prevalgono sulle disposizioni del presente TSPPS.

9.15 Disposizioni Varie

Intesi Group incorpora mediante riferimento le seguenti informazioni in tutti i certificati che emette:

- Qualsiasi altra Certificate Policy in vigore può essere dichiarato nel Certificato emesso;
- Gli elementi obbligatori ed elementi personalizzati degli standard in vigore;
- Il contenuto di estensioni ed enhanced naming non trattati altrove;
- Qualsiasi altra informazione dichiarata in un campo del Certificato.

Per includere informazioni mediante riferimento, Intesi Group, attraverso le proprie CA, utilizza suggerimenti computerizzati o testuali, i quali includono URL, OID, etc.

PAOLO SIRONI
2018-07-23T11:36:56+0200
signed by VALID_SIGN