Intesi Group Trust Service Provision Policy (TSPP)

Data: 20 dicembre 2017

Storia

Protocollo	Modifiche	Rev.	Data	Autore	Approvatore
TSPP	Prima versione in italiano. Viene mantenuta la versione 1.4 per avere coerenza di versione col documento scritto in Inglese.	1.4	20/12/2017	G. Damiano	F. Catullo

Indice

1 INTRODUZIONE

1.1 Quadro generale

Il presente Trust Service Provision Policy (di seguito solo TSPP) copre i requisiti tecnici, di sicurezza e organizzativi adottati da Intesi Group S.p.A. (di seguito denominato "Intesi Group") per la fornitura di servizi fiduciari conformi al regolamento (UE) n. 910/2014 (regolamento eIDAS).

Il presente TSPP contiene indicazioni su “cosa deve essere rispettato", mentre le specifiche adottate per attuare il presente TSPP ("come si è aderito a"), sono descritte nel documento Trust Service Provider Practice Statement (TSPPS). I documenti sono pubblicati e liberamente accessibili sul sito web istituzionale di Intesi Group al seguente URI:

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

La conformità ai requisiti di sicurezza e alle policy specificate negli standard ETSI EN 319 401, ETSI EN 319 411 e ETSI EN 319 421 garantisce che Intesi Group adotti lo “Stato dell’arte” per l’erogazione di servizi fiduciari e il rispetto dei requisiti contenuti nel regolamento eIDAS.

Il presente documento descrive le policy adottate dal Intesi Group, per dimostrare a soggetti, sottoscrittori ed utilizzatori (Relying Parties) il corretto funzionamento e la corretta gestione dei servizi fiduciari.

1.1.1 Scopo

Il presente documento specifica le policy adottate per soddisfare i requisiti generali per i servizi fiduciari di Intesi Group.

Le policy definite nel seguente documento si applicano ai seguenti certificati e alle marche temporali emesse da Intesi Group:

- Certificati di root CA (autofirmati);
- Certificati qualificati per firme elettroniche e sigilli;

- Certificati per firme di marche temporali (Time Stamp Unit - TSU);
- Marche temporali qualificate (Time Stamp Token qualificati, QTST).

Gli OID definiti in questo TSPP ed inseriti nel campo “Certificate Policies” dei certificati qualificati emessi da Intesi Group sono conformi ai requisiti del regolamento eIDAS relativi ai TSP che emettono certificati qualificati.

Gli OID definiti in questo TSPP ed inseriti nell’estensione Policy delle marche temporali qualificate emesse da Intesi Group sono conformi ai requisiti del regolamento eIDAS riguardanti l’emissione di marche temporali qualificate.

Il presente documento è pubblicamente disponibile. La sua distribuzione è regolata come descritto nella sezione "diritti di proprietà intellettuale".

1.1.2 Livello di specificità

Il presente documento descrive solo le regole generali di emissione e gestione dei certificati qualificati (QC) e delle marche temporali (TST). La descrizione dettagliata dell'infrastruttura e delle relative procedure operative sono contenute nel documento “piano della sicurezza” che è disponibile solo per il personale autorizzato di Intesi Group, per gli Auditor del Conforment Assessment Body e all’organismo di vigilanza (AgID).

1.1.3 Riferimenti

1. "regolamento eIDAS": Regolamento (UE) n. 910/2014 del Parlamento europeo, del 23 luglio 2014, relativo ai servizi di identificazione elettronica e di fiducia per le operazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
2. IETF RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol – August 2001.
3. EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
4. ETSI EN 319 422 “Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp profiles.

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

1.2 Nome e identificativo del documento

Policy Name: Intesi Group Qualified Trust Service Provision Policy

Tutte gli Object Identifier (OID) definiti da Intesi Group nel presente documento hanno come prefisso il valore 1.3.6.1.4.1.48990.1 che nelle definizioni di seguito è abbreviato in TSPP.

Gli OID per i certificati TSU per la firma di marche temporali è:

- TSPP.1.5.1

OID per Best Practices Time Stamp Policy (BTSP):

- 0.4.0.2023.1.1

Nota: Questa OID è definito come Best Practices Policy definito nello standard EN 319 421 e viene inserito nel campo Policy delle marche temporali and indicarne la conformità allo standard.

OID per i certificati qualificati per firme digitali:

- TSPP.1.1.1 e
- 0.4.0.194112.1.2 (QCP-n-qscd definito nell'ETSI EN 319 411-2)

OID per i certificati qualificati per sigilli elettronici:

- TSPP.1.2.1 e
- 0.4.0.194112.1.3 (QCP-l-qscd definito nell'ETSI EN 319 411-2)

1.3 Partecipanti alla PKI

Le policy descritte nel presente documento si applicano a:

- I certificati di root di Intesi Group per l'emissione di firme digitali, sigilli e certificati per la firma di marche temporali ed in particolare:
  - alla sua infrastruttura logistica e tecnica;
  - al suo personale.
- Ai soggetti a cui sono rilasciati i certificati, le marche temporali in conformità alle policy contenute in questo documento.
- Gli utilizzatori (Relying parties) che fanno affidamento sui certificati e le marche temporali di Intesi Group emesse in conformità al presente documento.

Un elenco dettagliato dei partecipanti alla PKI si trova descritto nel paragrafo 1.3 del TSPPS

1.4 Utilizzo dei certificati e dei sigilli

1.4.1 Usi appropriati del certificato

1.4.1.1 Uso dei certificati qualificati

I certificati qualificati rilasciati da Intesi Group possono essere utilizzati per apporre firme elettroniche qualificate (in caso di certificati di firma qualificata) e sigilli elettronici qualificati (in caso di certificati sigillo elettronico) nel pieno rispetto del presente documento e del relativo TSPPS.

1.4.1.2 Uso dei Certificati per TSU

I certificati TSU emessi da Intesi Group possono essere utilizzati solo per firmare le marche temporali con attraverso l'infrastruttura di marcatura di Intesi Group.

1.4.1.3 Uso delle marche temporali

Le marche temporali rilasciate da Intesi Group possono essere utilizzate:

- per dimostrare che il dato da cui è stato ricavato il digest esisteva prima dell'istante di tempo contenuto nella marca temporale con la precisione prevista nella sezione 7.3.3;
- per estendere la validità della firma oltre la data di scadenza contenuta nel certificato del firmatario;
- Se non diversamente indicato, in tutti i casi definiti nelle norme di legge e nei termini e condizioni concordati tra Intesi Group e il sottoscrittore.

1.4.2 Utilizzi vietati del certificato

1.4.2.1 Utilizzo vietato dei certificati qualificati

I Certificati rilasciati nell'ambito di questa policy non possono essere usati dalle applicazioni:

- In modo differente da quanto stabilito nella clausola 1.4.1.1 e fuori dai limiti di utilizzo specificati nel presente documento e nel TSPPS;
- in modo incompatibile ai termini e condizioni accettati dal Sottoscrittore.

I certificati rilasciati ai soggetti non possono essere utilizzati per operazione di autenticazione e operazioni di crittografia dei dati e delle chiavi.

1.4.2.2 Utilizzo vietato dei certificati di TSU

I certificati TSU emessi da Intesi Group non possono essere utilizzati per scopi diversi dalla verifica di marche temporali emesse con la corrispondente chiave privata e utilizzando l'infrastruttura di marcatura temporale di Intesi Group.

1.4.2.3 Utilizzo vietato dei certificati di CA

I certificati di root CA non devono essere utilizzati per scopi diversi dalla validazione dei certificati utente.

1.4.2.4 Utilizzo vietato delle marche temporali

Le marche temporali emesse non possono essere utilizzate per scopi diversi dall'utilizzo definito in questo documento, nel TSPPS e da quanto stabilito nei "Termini & Condizioni" accettati dall'utente.

1.5 Amministrazione del CP

1.5.1 Amministrazione del documento

Questa Policy è rilasciata sotto la responsabilità di:

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

1.5.2 Contatto

La persona responsabile della stesura di questa policy è:

Giuseppe Damiano, Security and RA Officer

1.6 Definizioni e acronimi

AES	Advanced Electronic Signature
ARL	Authority Revocation List
B2B	Business to Business
CA	Certification Authority
CRL	Certificate Revocation List
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
ISO	International Organisation for Standardisation
ITU	International Telecommunications Union
LDAP	Lightweight Directory Access Protocol
NCP	Normalised Certificate Policy
NCP+	Normalised Certificate Policy +
OID	Object Identifier
PKCS	Public Key Certificates Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
QES	Qualified Electronic Signature
RFC	Request for Comments
RSA	A specific Public Key algorithm
TSA	Time Stamping Authority
TSP	Trust Service Provider
TSPP	Certificate Policy
TSPPS	Certification Practice Statement
TSS	Time Stamping Service
TST	Time Stamp Token
TSU	Time Stamping Unit
UTC	Coordinated Universal Time

2 PUBBLICAZIONE E ARCHIVIAZIONE

2.1 Repository

2.2 Pubblicazione delle informazioni di certificazione

I seguenti documenti sono disponibili all'URL http://www.intesigroup.com/en/Documents:

- Questo TSPP,
- il TSPPS corrispondente a questo TSPP,
- PKI Disclosure Statement (PDS)
- Termini & Condizioni di contratto dei servizi.
- Modulistica varia.

Certificati di root e CRL sono pubblicati attraverso il sito www.time4mind.com con modalità e frequenza descritti nel TSPPS.

2.3 Data e frequenza delle pubblicazioni

Fare riferimento al paragrafo 2.3 del TSPPS.

2.4 Controllo all'accesso

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

3 IDENTIFICAZIONE E AUTENTICAZIONE

3.1 Nomi

Il soggetto deve essere identificato attraverso un nome in formato x. 500 inserito nel campo Subject del certificato x. 509.

3.2 Verifica dell'identità

La verifica dell'identità di persone fisiche e persone giuridiche viene effettuata dai RAO attraverso processi RA definiti con modalità descritte all'interno del TSPPS.

Il certificato TSU è rilasciato solamente a personale di Intesi Group.

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

L'operazione di re-key non è disponibile per qualificati emessi a persone fisiche, giuridiche e per certificati di TSU.

3.4 Identificazione e autenticazione per richieste di revoca

La revoca e la sospensione di certificati qualificati avviene dopo autenticazione secondo le procedure specificate nel TSPPS.

Il certificato TSU può essere revocato secondo le procedure interne di Intesi Group eseguite sotto la supervisione del "Security and RA Officer" e del "TSP Operation Officer".

4 REQUISITI GESTIONE DEL CICLO DI VITA DEL CERTIFICATO

4.1 Richiesta di certificato

La richiesta del certificato può essere effettuata dal:

- Soggetto titolare del certificato per certificati di firma qualificata.
- Da una persona fisica autorizzata a rappresentare la persona giuridica per certificati per sigillo

I certificati di TSU possono essere richiesti da operatori Intesi Group appositamente autorizzati.

La procedura di richiesta è descritta all'interno del TSPPS.

4.2 Processo di emissione

Il processo di emissione per certificati qualificati, certificati di TSU e TimeStampToken è descritto nel paragrafo 4.2 del TSPPS.

4.3 Emissione del certificato

Le modalità di emissione del certificato sono descritte nel paragrafo 4.3 del TSPPS.

4.4 Accettazione del certificato

Il certificato viene considerato accettato dopo essere stato consegnato al titolare o all'operatore. I destinatari possono controllare il contenuto del certificato e nel caso in cui individuino degli errori possono richiederne la revoca e la ri-emissione secondo le procedure descritte nel TSPPS.

4.5 Coppia di Chiavi e Utilizzo del Certificato

L'uso delle chiavi e l'utilizzo del certificato sono descritti nel paragrafo 4.5 del TSPPS.

4.6 Rinnovo del certificato

Il TSP mette a disposizione una procedura di rinnovo dei certificati di firma, sigillo e TSU secondo le modalità descritte nel paragrafo 4.6 del TSPPS.

Le chiavi dei certificati scaduti vengono cancellate secondo procedure adottate da Intesi Group.

4.7 Certificato re-Key

Il riutilizzo della chiave non è consentito in nessun caso.

4.8 Modifica del certificato

La modifica dei certificati qualificati può essere eseguita solamente revocando il certificato da modificare ed emettendone uno nuovo.

La ri-emissione del certificato di TSU avviene attraverso la esecuzione di una nuova key ceremony.

Dettagli procedurali si si trovano descritti nel paragrafo 4.8 del TSPPS.

4.9 Revoca e sospensione del certificato

La revoca determina la prematura cessazione della validità di un certificato, a partire da un dato momento nel tempo (data/ora). La revoca di un certificato è irreversibile.

La sospensione di un certificato ne determina la temporanea sospensione della validità, a partire da un dato momento nel tempo. Un certificato che è stato sospeso, può essere riattivato oppure revocato in qualsiasi momento.

L'esecuzione di una sospensione o di una revoca consiste nella generazione e pubblicazione di una nuova CRL (Certificate Revocation List) che include il numero di serie del certificato sospeso o revocato. La CRL è accessibile a chiunque debba verificare lo stato del certificato (vedere la sezione 4.10).

L'esecuzione di una riattivazione consiste nella generazione e pubblicazione di una nuova CRL da cui è stato rimosso il numero di serie del certificato precedentemente sospeso.

4.9.1 Circostanze per revoca

Le condizioni che possono causare una revoca di un certificato qualificato sono:

1. Il titolare richiede alla CA la revoca del certificato;
2. la chiave privata viene persa, rubata o potenzialmente compromessa;

3. vi è una condizione di non conformità del contratto da parte del titolare e l'autorità di certificazione.
4. il titolare non ha più il controllo esclusivo della chiave privata perché i dati di attivazione della chiave privata (codice PIN) sono stati compromessi.
5. l'utente non può più utilizzare la chiave del dispositivo protetto.
6. le informazioni del Titolare contenute nel certificato non sono più valide per esempio nel caso in cui subentri una perdita di qualifiche, la cessazione di poteri di rappresentanza, la cancellazione da albi o la cessata appartenenza ad organizzazioni.
7. termina la relazione tra il titolare e la CA.
8. la CA è resa consapevole di una possibile compromissione della chiave privata della CA;
9. L'organizzazione di appartenenza del titolare del certificato ha interrotto l'attività.

Nel caso di un certificato TSU le condizioni che possono portare ad una revoca sono:

1. il certificato non è corretto in termini di informazioni contenute.
2. il TSP cessa il servizio di marcatura temporale.
3. il TSP perde la sua qualifica ad operare, su richiesta dell'autorità di vigilanza.
4. È provata la compromissione della chiave privata.
5. il TSP ravvisa un possibile compromesso della chiave privata della CA TSS utilizzata per l'emissione del certificato TSU.

La revoca dei certificati di TSU deve essere autorizzata dalla direzione e deve essere resa pubblica attraverso CRL entro 24 ore dall’operazione.

La sospensione non è disponibile per certificati TSU e per i certificati di root CA.

4.10 Servizi informativi sullo stato del certificato

Lo stato dei certificati qualificati è reso disponibile tramite la pubblicazione di CRL, in conformità allo standard RFC 5280, e tramite un basato sul protocollo OCSP (Online Certificate Status Protocol) in conformità con la specifica [RFC2560].

Lo stato dei certificati TSU viene reso disponibile a tutte le parti interessate attraverso la pubblicazione di CRL, in conformità alla RFC 5280.

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 Key Escrow ed il ripristino non sono previsti, tranne nei casi descritti nel paragrafo 4.12 del TSPPS.

5 STRUTTURE, GESTIONE E CONTROLLI OPERATIVI

I controlli eseguiti sui servizi fiduciari qualificati devono essere conformi alle seguenti norme:

- EN 319 421 per emissione di marche temporali;
- EN 319 411-2 QCP-n-qscd policy per il rilascio di certificati di firma qualificata.
- EN 319 411-2 QCP-l-qscd policy per il rilascio di certificati di sigillo qualificato.

Il sistema di sicurezza del Intesi Group è conforme alla norma ISO/IEC 27001.

5.1 Sicurezza fisica

I sistemi e i dispositivi del gruppo intesi TSP (sia HW che SW) sono gestiti in ambienti protetti da accessi non autorizzati.

Caratteristiche sulle modalità di protezione adottate da Intesi Group sono descritte nel paragrafo 5.1 del TSPPS.

5.2 Controlli procedurali

Si applica quanto descritto nel paragrafo 5.2 del TSPPS.

5.3 Controlli del personale

Si applica quanto descritto nel paragrafo 5.3 del TSPPS.

5.4 Procedure di registrazione degli audit

Tutti i sistemi tengono traccia di tutte le operazioni rilevanti. Gli eventi registrati variano da operazioni normali (ad esempio: installazione e aggiornamento di SW, log-in e log-out da parte degli operatori) fino a operazioni anormali (es.: errori dell'operatore, tentativi non autorizzati).

Per ogni evento vengono registrate le informazioni sul tipo, la data e l'ora dell'occorrenza.

I file di log sono conservati per 20 anni secondo le norme di legge attualmente in vigore.

I file di log vengono conservati in un ambiente sicuro e anti-manomissione.

5.5 Archiviazione delle registrazioni

I log file generati dai servizi fiduciari e la documentazione relativa all'esecuzione di procedure interne viene raccolta e conservata in modo sicuro per un periodo di 20 anni. Dettagli sulle modalità di conservazione si trovano descritti paragrafo 5.5 del TSPPS.

5.6 Rinnovo dei certificati di CA

I certificati di root sono rinnovati almeno 5 anni pima della scadenza. La procedura di rinnovo è descritta all'interno del TSPPS e segue la procedura di keyceremony.

5.7 Compromissione e disaster recovery

Intesi Group S.p.A. ha stabilito tutte le misure necessarie atte a garantire un ripristino completo dei servizi di certificazione in caso di disastro, corruzione dei server, del software o dei dati. Tutte queste misure sono descritte nel "business continuity plan" e nella procedura ISO/IEC 27001.

5.8 Terminazione della CA

La CA è dotata di un piano di cessazione della CA i cui sono descritte le procedure di comunicazione della cessazione del servizio e le modalità di trasferimento delle informazioni sensibili sullo stato di certificati, i dati di registrazione, i file di log, i contratti e in generale le informazioni conservate in base alla normativa.

6 MISURE DI SICUREZZA TECNICA

Sono attuati i controlli contenuti in ETSI EN 319 411-1, ETSI EN 319 411-2 e ETSI EN 319 421 per proteggere i sistemi, le chiavi crittografiche, i repository.

6.1 Generazione e installazione di una coppia di chiavi

6.1.1 Root CA

Intesi Group è dotata di una procedura di generazione delle chiavi della CA che può essere eseguita solamente da personale. L'esecuzione della procedura è verbalizzata e conservata per 20 anni.

6.1.2 Certificato Utente

La procedura di generazione del certificato utente viene eseguita solo attraverso i processi definiti nel TSPPS.

6.1.3 Certificato TSU

Intesi Group è dotata di una procedura di generazione delle chiavi di TSU che può essere eseguita solamente da personale. L'esecuzione della procedura è verbalizzata e conservata per 20 anni.

6.2 Protezione della chiave privata e sicurezza del modulo crittografico

6.2.1 Root CA

La coppia di chiavi utilizzata dalle CA sono generate e mantenute su un HSM certificato FIPS Pub 140-2 Level 3 o Common Criteria (ISO 15408) EAL 4.

6.2.2 Certificato TSU

La coppia di chiavi utilizzata dalle CA sono generate e mantenute su un HSM certificato FIPS PUB 140-2 Level 3 o Common Criteria (ISO 15408) EAL 4.

6.2.3 Certificato qualificati

La coppia di chiavi per certificati di firma e sigilli è generata a bordo di un dispositivo certificato QSCD.

6.3 Altri aspetti sulla gestione delle coppie di chiavi

Tutti i certificati emessi sono archiviati da Intesi Group.

6.4 Dati di attivazione

L'accesso ai dati di attivazione dei dispositivi crittografici della CA e del TSS è riservato a operatori della CA autorizzati. Le quantità di attivazione sono conservate in un luogo sicuro.

Gli accessi ai dispositivi di attivazione è loggato e conservato a norma di legge.

6.5 Controlli di sicurezza informatica

Viene applicata la separazione dei ruoli. Tutte le attività eseguite vengono tracciate dai sistemi e dalle funzionalità di conservazione dei log.

6.6 Controlli tecnici sul ciclo di vita

Intesi Group applica procedure conformi agli standard ISO 9001 e 27001.

6.7 Controlli di sicurezza della rete

L'architettura dei sistemi di Intesi Group comprende sistemi per la protezione della rete. La protezione della rete è garantita anche dei processi definiti nella procedura ISO 27001 di Intesi Group.

6.8 CA e marcatura temporale

Tutti i server hanno gli orologi sincronizzati attraverso una fonte di tempo sicura. Il sistema di monitoraggio verifica l'allineamento degli orologi e, in caso di grave disallineamento, esclude dal servizio le macchine con orologi disallineati.

7 PROFILI DEI CERTIFICATI E DELLE CRL

7.1 Profilo certificato

I certificati sono conformi allo standard ISO/IEC 9594-8:2005 [X. 509] versione 3 e alla specifica [RFC 5280].

I certificati qualificati sono conformi alla norma EN 319 412-2 per la firma elettronica e EN 319 412-3 per i certificati per sigillo. I certificati qualificati sono conformi anche alla norma EN 319 412-5 e alle leggi italiane.

I Certificati per TSU sono conformi alla EN 319 412-3 e EN 319 422.

Per quanto riguarda gli algoritmi crittografici, la lunghezza minima delle chiavi e le funzioni di hashing sono conformi ETSI TS 119 312.

7.2 Profilo CRL

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

Per quanto riguarda gli algoritmi crittografici, la lunghezza minima delle chiavi, le funzioni di hashing e le CRL sono conformi allo standard ETSI TS 119 312.

8 VERIFICHE DI CONFORMITÀ

Intesi Group controlla tutte le procedure descritte nel presente TSPP e nelle relative TSPPS, con lo scopo di verificarne:

- l'osservanza da parte del personale
- la loro efficacia

- la loro effettiva applicazione.

L'obiettivo è quello di migliorare la sicurezza generale di Intesi Group adottando procedure che possono essere rispettate e che non presentino buchi di sicurezza riconosciuti.

8.1 Frequenza o circostanze di valutazione

Le verifiche vengono eseguire mensilmente o annualmente a seconda delle procedure verificate.

La verifica di conformità è effettuata ogni 12 mesi da un Conformity Assessmnet Body (CAB) accreditato secondo il regolamento di eIDAS.

Gli audit interni sono effettuati seguendo una procedura che prevede periodi diversi di verifica (dal trimestrale all'anno) in base ai vari aspetti tecnico-operativi del servizio CA.

8.2 Identità e qualificazione degli auditor

Il controllo interno è effettuato da personale interno di Intesi Group.
Il controllo esterno è effettuato da un organismo di valutazione della conformità alla normativa eIDAS secondo quando definito in ISO/IEC 17065 e in EN 319 403.

8.3 Relazioni tra la CA e gli ispettori

Non esistono relazioni gerarchiche tra gli uffici di Intesi Group ed i revisori interni.

Il controllo esterno viene eseguito da un ente indipendente.

8.4 Argomenti coperti dalle verifiche

L'audit copre le procedure e gli obblighi elencati nel presente TSPP e nel relativo TSPPS.

8.5 Misure adottate in seguito a non conformità

Le azioni da intraprendere per risolvere le non conformità vengono definite dal personale di Intesi Group con l'obiettivo di risolverle nel più breve tempo possibile.

8.6 Comunicazione dei risultati

Le non conformità e le gravi violazioni della sicurezza sono segnalati a responsabili del servizio TSS e della CA o al management di Intesi Group in base alla gravità della non conformità.

Se previsto dal regolamento eIDAS le non conformità più possono essere comunicate ad AgID e agli organismi competenti.

9 CONDIZIONI GENERALI DI SERVIZIO

I termini e le condizioni generali dei servizi TSP sono messi a disposizione agli utenti e pubblicati sul sito Web della CA.
In caso di discrepanze con questo documento, il documento "termini e condizioni" ha la precedenza.

9.1 Tariffe del servizio

Si applica quanto descritto nel corrispondente paragrafo 9.1 del TSPPS e quanto pubblicato sul sito www.intesigroup.com.

9.2 Responsabilità finanziaria

Intesi Group ha un capitale e una assicurazione adeguati per adempiere agli obblighi previsti per i TSP.

9.3 Riservatezza delle informazioni commerciali

Nessuna clausola aggiuntiva.

9.4 Riservatezza delle informazioni personali

I dati personali raccolti sono ritenuti confidenziali e trattati secondo il regolamento (UE) 2016/679 e la privacy policy di Intesi Group.

9.5 Diritti di proprietà intellettuale

Il presente documento (TSPP) è di proprietà di Intesi Group che si riserva tutti i diritti associati allo stesso.

9.6 Obblighi e garanzie

9.6.1 Certification Authority

La CA deve operare in conformità al presente TSPP e al relativo TSPPS.

9.6.2 Registration Authority

Le LRA devono operare in conformità al presente TSPP e al relativo TSPPS.

Il servizio RA 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

Fare riferimento al paragrafo 9.7 del TSPPS.

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

Questo TSPP è valido dal momento in cui è pubblicato sul sito Web della CA (Vedi capitolo 2) e rimarrà in valido fino a quando non verrà sostituito con una nuova versione.

9.11 Emendamenti

Intesi Group si riserva il diritto di modificare questo TSPP in qualsiasi momento senza alcuna previa notifica.

9.12 Risoluzione Dispute

La risoluzione delle dispute verrà trattata da Intesi Group secondo quanto descritto nel TSPPS.

9.13 Legge Applicabile

Questo TSPP è soggetto alla legge italiana e come tale sarà interpretata ed eseguito. Per questo non espressamente prescritto in questa documento o nel relativo TSPPS, si applica la normativa vigente.

9.14 Conformità con le norme applicabili

Le leggi vigenti prevalgono sulle disposizioni del presente TSPP.

9.15 Disposizioni varie

La CA Intesi Group incorpora in tutti i certificati che emette e che rispettano questa policy gli OID definiti al paragrafo 1.2 di questo documento ad indicare che si applica il presente TSPP ed il TSPPS.