Trust Service Practice Statement

Ver. 2.1

11 novembre 2026

History

Cambiamenti	Rev.	Data	Autore	Verificato	Approvato
Prima versione in italiano.	1.4	15/09/17	F.Barcellini	G.Damiano	P.Sironi
Revisione generale del documento	1.5	22/11/17	F.Barcellini	G.Damiano	P.Sironi
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	P.Sironi
Modifiche al paragrafo 3.1.4.	1.7	17/01/18	F.Barcellini	G.Damiano	P.Sironi
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	P.Sironi
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	P.Sironi
Modifica paragrafi 4.2, 6.1.1.2, 6.1.2	1.10	08/07/2019	F.Barcellini	G.Damiano	P.Sironi
Modificati i paragrafi 1.3, 1.3.2, 1.3.6, 1.4, 1.6, 2.2, 3.1.1, 3.1.2, 3.1.3, 3.1.6, 3.1.7, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 4.1.2, 4.3.1, 4.4.1, 4.4.2, 4.9.1, 4.9.2, 5.1,5.2, 5.3, 5.4.1, 5.8, 6.1.5, 6.1.6, 6.2.1, 6.2.2, 6.6, 8. Aggiunti i paragrafi 1.3.7, 3.2.8, 4.3.1.1, 4.3.2, 7.1.7, 7.1.8, 7.2.1, 7.2.2, 7.2.3, 7.2.4	1.11	09/03/2020	F.Barcellini V.Manaila	G.Damiano	P.Sironi
Aggiunto paragrafo 3.2.9	1.12	12/01/2021	F.Barcellini	P.Sironi	P.Sironi
Aggiunto paragrafo 6.9	1.13	30/03/2021	F.Barcellini	P.Sironi	P.Sironi
Modificati i paragrafi 1.1, 1.3.2, 1.4, 1.5, 3.1.4, 3.2.6, 3.2.8, 3.2.10, 4.1.1, 4.5.1.1, 4.6, 4.9.1, 6.8, 9.4	1.14	04/01/2022	B.Tafini	F.Barcellini	P.Sironi
Modificati i paragrafi 1.3, 3.2.3, 3.2.9, 3.2.10, 3.2.11. 3.2.12, 4.1.2, 4.2, 4.3 4.9.15	1.15	25/06/2024	F.Barcellini	F.Barcellini	P.Sironi

Aggiunto paragrafo 4.3.4, 4.11, 7,1 Modificati i paragrafi: 1.3.1, 1.4, 3.2.5, 3.2.7, 4.6, 4.9.1, 4.9.3.3, 4.11, 9.12	1.16	17/07/2025	D.Saccò, M.Menghini	F.Barcellini	P.Sironi
Modifiche for “management of remote qualified electronic signature creation devices” e “Identity Proofing Identity Provider” Adaption for Modified paragraph: 1.4, 3.2, 5.1, 6.1.5, 6.2.1, 6.5, 6.7, 7.1	2.0	04/03/2026	D. Saccò, M. Menghini	F. Barcellini	P.Sironi
Modifica al paragrafo 3.3.3, 5.4.3, 5.5.2, 6.1.1.2, 9.6.1, 9.6.6, 9.11	2.1	11/11/2026	D. Saccò	F. Barcellini	P.Sironi

Indice

1 INTRODUZIONE 12
1.1 Quadro generale 12
1.2 Nome e identificativo del documento 13
1.3 Partecipanti alla PKI 13
1.3.1 Intesi Group come Autorità di Certificazione e Marcatura Temporale 13
1.3.2 Local Registration Authority 14
1.3.3 Sottoscrittori o richiedenti 15
1.3.4 Soggetti 15
1.3.5 Titolari 15
1.3.6 RAO (Registration Authority Officer) 15
1.3.7 Relying parties o utilizzatori 16
1.3.8 Altri partecipanti 16
1.4 Politiche applicabili 16
1.4.1 Emissione certificati, sigilli e marche temporali 16
1.4.2 Servizio di gestione 17
1.5 Amministrazione del TSPPS 18
1.6 Definizione e acronimi 18
2 PUBBLICAZIONE E ARCHIVIAZIONE 19
2.1 Repository 19
2.2 Informazioni pubblicate 19
2.3 Data e frequenza delle pubblicazioni 19
2.4 Controllo all'accesso 20
3 IDENTIFICAZIONE E AUTENTICAZIONE 20
3.1 Nomi 20
3.1.1 Tipi di nomi 20

3.1.2 Necessità di dare nomi significativi 20
3.1.3 Anonimato e pseudonimia dei titolari 20
3.1.4 Abilitazioni professionali, ruolo e organizzazione 21
3.1.5 Regole di interpretazione dei nomi 21
3.1.6 Univocità dei nomi 21
3.1.7 Riconoscimento, autenticazione e ruolo dei marchi commerciali 22
3.2 Verifica dell'identità - eIDAS 22
3.2.1 Prova del possesso di una chiave privata 22
3.2.2 Validazione dell'identità di una organizzazione 22
3.2.3 Validazione delle identità individuali 22
3.2.4 Acquisizione dati di identificazione 24
3.2.5 Identificazione e registrazione de-visu 24
3.2.6 Identificazione tramite processi LRA 26
3.2.7 Identificazione e registrazione IDentify Web. 26
3.2.8 Identificazione attraverso verifica firma elettronica qualificata. 27
3.2.9 Identificazione attraverso norme antiriciclaggio 27
3.2.10 Identificazione attraverso identità digitali SPID 27
3.2.11 Identificazione attraverso carta d'identità elettronica CIE 28
3.3 Verifica dell'identità – eIDAS2 28
3.3.1 Metodi di Identificazione e OID Associati 29
3.3.2 Requisiti e Procedure di Verifica 29
3.3.3 Gestione delle Evidenze e Conservazione 30
3.3.4 Ruoli di Fiducia e Formazione 30
3.4 Identificazione e autorizzazione per riutilizzo chiave (re-key) 30
3.5 Identificazione e autenticazione per richieste di revoca 30
4 REQUISITI GESTIONE DEL CICLO DI VITA DEL CERTIFICATO 30
4.1 Richiesta di certificato 30
4.1.1 Chi può richiedere il certificato 30
4.1.2 Processo di emissione e responsabilità 31
4.2 Processo di emissione 31
4.2.1 Informazioni del soggetto richieste 32

4.2.2 Registrazione e autenticazione 32

4.3 Emissione del certificato 33

4.3.1 Emissione del certificato di firma remota 33

4.3.2 Emissione del certificato su dispositivo fisico QSCD 34

4.3.3 Emissione del certificato TSA 35

4.3.4 Emissione di un certificato di test 35

4.4 Accettazione del certificato 36

4.4.1 Accettazione del Certificato 36

4.4.2 Pubblicazione del Certificato da parte del QTSP 36

4.4.3 Notifica dell'emissione del Certificato da parte del QTSP ad altre entità 36

4.5 Coppia di Chiavi e Utilizzo del Certificato 36

4.5.1 Utilizzo della chiave privata e del Certificato 36

4.5.2 Utilizzo della chiave pubblica e del certificato 37

4.5.3 User notice 37

4.6 Rinnovo del certificato 38

4.6.1 Procedura per elaborare la richiesta di rinnovo 38

4.6.2 Notifica al titolare 38

4.6.3 Accettazione del certificato 39

4.6.4 Pubblicazione del Certificato 39

4.6.5 Notifica dell'emissione del Certificato da parte del QTSP ad altre entità 39

4.7 Re-key del Certificato 39

4.8 Modifica del Certificato 39

4.9 Revoca e sospensione del certificato 39

4.9.1 Circostanze per la revoca 39

4.9.2 Chi può richiedere la revoca 40

4.9.3 Procedura per la richiesta di revoca 40

4.9.4 Periodo di grazia della richiesta di revoca 42

4.9.5 Termine entro il quale il QTSP deve elaborare la richiesta di revoca 42

4.9.6 Esigenza di controllo per la revoca per gli Utilizzatori 42

4.9.7 Frequenza di emissione CRL / periodo di validazione della risposta OCSP 42

4.9.8 Latenza massima della CRL 42
4.9.9 Controllo della disponibilità dello stato di revoca on-line 42
4.9.10 Altre forme disponibili di pubblicazione della revoca 42
4.9.11 Esigenze speciali per quanto riguarda la compromissione della chiave 42
4.9.12 Circostanze per la sospensione 42
4.9.13 Chi può richiedere la sospensione 43
4.9.14 Procedura di sospensione e richieste di riattivazione 43
4.9.15 Limiti al periodo di sospensione 43
4.10 Servizi informativi sullo stato del certificato 43
4.10.1 Disponibilità del Servizio 43
4.11 Servizi verifica marca temporale 43
4.12 Cessazione del contratto 44
4.13 Key Escrow e Ripristino 44
5 CONTROLLI DELLE STRUTTURE DI GESTIONE E OPERATIVI 44
5.1 Sicurezza fisica 44
5.2 Controlli procedurali 45
5.3 Controlli di sicurezza del personale 46
5.4 Procedure di registrazione degli audit 47
5.4.1 Tipo di eventi registrati 47
5.4.2 Frequenza di elaborazione del registro 47
5.4.3 Periodo di conservazione del registro audit 47
5.4.4 Protezione di un registro audit 48
5.4.5 Procedure di backup del registro audit 48
5.4.6 Sistema di raccolta di audit (interno vs. esterno) 48
5.4.7 Notifica al soggetto di evento scatenante 48
5.4.8 Vulnerability assessment 48
5.5 Archiviazione delle registrazioni 48
5.5.1 Tipi di informazioni archiviate 48
5.5.2 Periodo di conservazione di un registro audit 48

5.5.3 Protezione dell'archivio 49
5.5.4 Procedure di backup degli archivi 49
5.5.5 Marcatura temporale degli archivi 49
5.5.6 Procedura di recupero e verifica delle informazioni archiviate 49
5.6 Rinnovo della Chiave CA 49
5.7 Compromissione e disaster recovery 49
5.7.1 Procedure di gestione degli incidenti e delle compromissioni 49
5.7.2 Corruzione di risorse informatiche, software e/o dati 50
5.7.3 Procedure in caso di compromissione della chiave privata 50
5.7.4 Continuità operative a fronte di un disastro 50
5.8 Terminazione del QTSP 50
6 MISURE DI SICUREZZA TECNICA 51
6.1 Generazione e installazione di una coppia di chiavi 51
6.1.1 Generazione di una coppia di chiavi 51
6.1.2 Consegna della chiave privata al titolare 52
6.1.3 Consegna della chiave pubblica all'emittente del certificato 52
6.1.4 Distribuzione della chiave pubblica della CA 52
6.1.5 Dimensioni delle chiavi 52
6.1.6 Generazione dei parametri e qualità della chiave pubblica 52
6.1.7 Key Usage (estensione X.509 v3) 53
6.2 Protezione della Chiave Privata e Sicurezza del Modulo Crittografico 53
6.2.1 Norme e controlli del modulo crittografico 53
6.2.2 Controllo multi-utente della chiave privata (n di m) 54
6.2.3 Ripristino della chiave privata 54
6.2.4 Backup della chiave privata 54
6.2.5 Archivio della chiave privata 54
6.2.6 Trasferimento della chiave privata tra moduli crittografici 54
6.2.7 Conservazione della chiave privata su un modulo crittografico 54
6.2.8 Metodo di attivazione della chiave privata 54
6.2.9 Metodo di disattivazione della chiave privata 55
6.2.10 Metodo di distruzione della chiave privata 55

6.2.11 Valutazione del modulo crittografico 55
6.3 Altri Aspetti sulla gestione delle coppie di chiavi 55
6.3.1 Archivio delle chiavi pubbliche 55
6.3.2 Periodi operativi del certificato e di utilizzo della coppia di chiavi 55
6.4 Dati di attivazione 55
6.5 Controlli di sicurezza informatica 56
6.6 Controlli tecnici sul ciclo di vita 56
6.7 Controlli di sicurezza di rete 56
6.8 CA e marcatura temporale 57
6.9 Inventario delle risorse 57
7 PROFILI DEI CERTIFICATI E DELLE CRL 57
7.1 Profilo del certificato 57
7.1.1 CA per il certificato di Marcatura Temporale 57
7.1.2 CA per il certificato di Firma Elettronica Qualificata 58
7.1.3 CA per il Sigillo Elettronico Qualificato 59
7.1.4 Certificato per TSU 60
7.1.5 Certificato Utente per Firma Elettronica Qualificata 61
7.1.6 Certificato Utente per il Sigillo Elettronico Qualificato 62
7.1.7 OCSP Certificate for Qualified Electronic Signature 64
7.1.8 OCSP Certificate for Qualified Electronic Seal 65
7.2 Profilo CRL 66
7.2.1 Parametri emissione CRL 67
7.2.2 CRL per il certificato di Marcatura Temporale 67
7.2.3 CRL per il certificato di Firma Elettronica Qualificata 68
7.2.4 CRL per il certificato di Sigillo Elettronico Qualificato 68
7.3 Profilo Timestsamp 69
8 VERIFICHE DI CONFORMITÀ 69
8.1 Identità e qualificazione degli auditor 70

8.2 Relazioni tra il QTSP e gli ispettori 70
8.3 Argomenti coperti dalle verifiche 70
8.4 Misure adottate in seguito a non conformità 70
8.5 Comunicazione dei risultati 71
9 CONDIZIONI GENERALI DI SERVIZIO 71
9.1 Tariffe del servizio 71
9.2 Responsabilità finanziaria 71
9.3 Riservatezza delle informazioni commerciali 71
9.3.1 Ambito di applicazione delle informazioni confidenziali 71
9.3.2 Informazioni considerate non confidenziali 72
9.3.3 Responsabilità di protezione delle informazioni confidenziali 72
9.4 Riservatezza delle informazioni personali 72
9.5 Diritti di proprietà intellettuale 72
9.6 Obblighi e garanzie 73
9.6.1 Certification Authority 73
9.6.2 Registration Authority 73
9.6.3 Sottoscrittori 73
9.6.4 Utilizzatori 73
9.6.5 Timestamp Authority 74
9.6.6 Fornitori esterni 74
9.7 Esclusione delle garanzie 74
9.8 Limiti di Responsabilità 74
9.9 Indennità 74
9.10 Durata e Terminazione 74
9.11 Emendamenti 74
9.12 Risoluzione Dispute 75

9.13 Legge Applicabile 75

9.14 Conformità con le norme applicabili 75

9.15 Disposizioni Varie 76

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" o "QTSP" o "CA") 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 elencate nel paragrafo 1.3.1 e i relativi servizi di emissione OCSP;
- generazione marche temporali;
- gestione dei dispositivi di creazione di firme elettroniche qualificate da remoto;
- gestione dei dispositivi di creazione di sigilli elettronici qualificati da remoto.

I servizi fiduciari qualificati sono conformi Regolamento (UE) 2024/1183 che modifica il regolamento (UE) n. 910/2014 (eIDAS2), D. lgs. 7 marzo 2005 n. 82 "*Codice dell'Amministrazione Digitale",* DPCM 22 febbraio 2013 *"Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71"* e soddisfano i requisiti previsti dai 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.
- ETSI TS 119 431-1 Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP services operating a remote QSCD / SCDev.
- ETSI TS 119 461 Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects.

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 C.A. dedicato all'emissione di certificati di firma qualificata;
- Il certificato di root C.A. dedicato all'emissione di certificati per sigilli elettronici;

- Il certificato di root C.A. 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 (https://www.intesigroup.com/it/qtsp/documenti/) e pubblicato in copia sul sito web di AgID (http://www.agid.gov.it/).

1.3 Partecipanti alla PKI

Intesi Group è un fornitore di servizi fiduciari ed emette certificati digitali con le modalità descritte in questo TSPPS. Intesi Group gestisce diverse Certification Authority (CA) che emettono certificati digitali per firme elettroniche, marche temporali e sigilli elettronici secondo il Regolamento (UE) 2024/1183 che modifica il regolamento (UE) n. 910/2014. Intesi Group ospita i propri servizi di PKI in data center altamente protetti. Tutti i dispositivi usati per l'erogazione di servizi PKI, inclusi ma non limitati a CA, OCSP, server RA, Server Signing Application (SSA come definito in [CEN / TS 419 241]) e HSM godono degli stessi controlli descritti nelle sezioni 5 e 6 per i dati, il personale e la sicurezza procedurale e tecnica. La posizione e la costruzione della struttura che ospita le CA e le apparecchiature sono adeguate a essere utilizzate ad ospitare informazioni sensibili e di alto valore.

1.3.1 Intesi Group come Autorità di Certificazione e Marcatura Temporale

Il QTSP 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 TSPPS sono indicate con i seguenti subjectDistinguishedName:

SubjectDistinguishedName	**Uso**
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	Usata per certificati di firma qualificata
CN=Intesi Group EU Qualified Electronic Signature CA G3 ECC, OrganizationIdentifier=VATIT-02780480964, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., C=IT	Usata per certificati di firma qualificata
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	Usata per sigilli qualificati
CN=Intesi Group EU Qualified Electronic Seal CA G3 ECC, OrganizationIdentifier=VATIT-02780480964, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., C=IT	Usata per sigilli qualificati
CN=Intesi Group Qualified Time-Stamp CA G2, OrganizationIdentifier=VATIT-02780480964, O=Intesi Group S.p.A., OU=Qualified Trust Service Provider, C=IT	Usata per certificati di marcatura temporale

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 (ed eventualmente Conservazione), 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 e/o autorizzati da Intesi Group;
- validazione e gestione di eventuali richieste di sospensione, revoca e riattivazione;

L'identificazione dei soggetti che richiedono un certificato può avvenire presso le sedi di Intesi Group o presso le sedi di una delle LRA abilitate. L'identificazione di soggetti che richiedono un certificato può essere eseguita in altre sedi da RAO abilitati che operano per conto di Intesi Group.

Le LRA sono soggette a specifiche verifiche e ispezioni (*audit*) da parte di Intesi Group finalizzati a verificare che le attività poste in essere rispondano a quanto previsto dal presente TSPPS e agli accordi sottoscritti con il QTSP Intesi Group.

Intesi Group si riserva il diritto di Interrompere il servizio qualora, a seguito dei predetti audit, emergesse che le attività di identificazione non siano state espletate in maniera idonea e conforme alle indicazioni ricevute dal QTSP e/o in conformità alla normativa vigente.

1.3.3 Sottoscrittori o richiedenti

Nell'ambito di questo TSPPS 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 (Registration Authority Officer)

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 del QTSP oppure tra il personale di una LRA e vengono abilitati ad operare in seguito alla stipula di un mandato con il QTSP 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 del QTSP.

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 dal QTSP Intesi Group sono soggette alla supervisione di AgID (Agenzia per l'Italia Digitale).

Qualora Intesi Group si avvalga di fornitori esterni che supportino l'erogazione dei servizi fiduciari disciplinati dal presente TSPPS, le attività e le responsabilità loro attribuite sono definite mediante accordi contrattuali. I relativi obblighi sono descritti nel paragrafo 9.6.6.

1.4 Politiche applicabili

1.4.1 Emissione certificati, sigilli e marche temporali

Le policy dei certificati per l'apposizione di firme e l'apposizione di sigilli contenute in questo TSPPS sono identificate dai seguenti OID

Intesi OID	ETSI OID	AgID OID	Descrizione
1.3.6.1.4.1.48990.1.1.1.1	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons using Remote QSCD.
1.3.6.1.4.1.48990.1.1.1.3	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons using Remote QSCD - Customer user notice.
1.3.6.1.4.1.48990.1.1.1.4	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons using Local QSCD.
1.3.6.1.4.1.48990.1.1.1.5	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons using Local QSCD - Customer user notice.
1.3.6.1.4.1.48990.1.1.1.6	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons identified with qualified signature using Remote QSCD
1.3.6.1.4.1.48990.1.1.1.7	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons using Remote QSCD used only to sign agreement with Intesi Group

1.3.6.1.4.1.48990.1.1.1.8	QCP-n-qscd	agIDcert	Qualified Certificates for Natural Persons issued using the eID based on National ID card (CIE).
1.3.6.1.4.1.48990.1.1.2.1	QCP-l-qscd	agIDcert	Qualified Certificates for Qualified Seal using remote QSCD
1.3.6.1.4.1.48990.1.1.5.1	baseline-ts-policy	agIDcert	Qualified TSA
1.3.6.1.4.1.48990.1.3.2.1	QCP-n-qscd	agIDcert	Qualified remote signature Certificates issued only for test purposes
1.3.6.1.4.1.48990.1.3.3.1	QCP-n-qscd	agIDcert	Qualified automatic signature Certificates issued only for test purposes
1.3.6.1.4.1.48990.1.3.4.1	QCP-l-qscd	agIDcert	Qualified remote seal Certificates for issued only test purposes

Dove:

1. QCP-n-qscd è 0.4.0.194112.1.2 definito all'interno dello standard ETSI EN 319 411-2;
2. QCP-l-qscd è 0.4.0.194112.1.3 definito all'interno dello standard ETSI EN 319 411-2;
3. baseline-ts-policy è 0.4.0.2023.1.1 definito come Best Practices Policy definito nello standard EN 319421 e viene inserito nel campo Policy delle marche temporali ad indicarne la conformità allo standard;
4. agIDcert 1.3.76.16.6 indica l'adesione alle "Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate";

1.4.2 Servizio di gestione

Il servizio di gestione della creazione di firme e sigilli qualificati a distanza è conforme ai requisiti definiti nella norma ETSI 119 431-1 e, pertanto, fa riferimento ai seguenti OID:

OID	Descrizione
0.4.0. 19431.1.1.2	Normalized SSAS Policy
0.4.0.19431.1.1.4	EU SSAS Policy

Il sistema di firma remota adottato per tale servizio è PkBox versione 3.4, certificato come QSCD da A-Sit. Il relativo certificato di conformità è pubblicamente disponibile sul sito istituzionale di Intesi Group, nella

sezione aziendale (https://www.intesigroup.com/it/azienda/), e può essere consultato anche sul sito di A-Sit al seguente indirizzo:

https://www.a-sit.at/wp-content/uploads/2025/06/VIG-25-036_QSCD-Certificate_Intesi_PkBox34-Update1_Final_sig-HL.pdf

1.5 Amministrazione del TSPPS

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 e dall'Agenzia per l'Italia Digitale. Richieste di informazioni o chiarimenti riguardo al presente TSPPS possono essere inviate scrivendo una e-mail all'indirizzo **tsp@intesigroup.com.**

1.6 Definizione e acronimi

Acronimi	Definizione
CA	Certification Authority
CAO	Certificate Authority Officer
CRL	Certificate Revocation List
eIDAS2	Regolamento (UE) 2024/1183 del parlamento europeo e del consiglio dell'11 aprile 2024 che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo ad un'identità digitale.
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
OTP	One Time Password
PKI	Public Key Infrastructure – componente per l'emissione dei certificati
QTSA	Qualified Time-Stamping Authority
RAO	Registration Authority Officer
RFC	Request For Comments
TIN	cTax Identification Number
TLS	Transport Layer Security
TSA	Time-Stamping Authority
TSP	Trust Service Provider
TSPP	TSP Policy

Acronimi	Definizione
TSPPS	TSP Practice Statement
TSU	Time-Stamping Unit

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 99.8%. 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:

[1] Manuale Operativo (TSPPS).
[2] PKI Disclosure Statement (PDS)
[3] Identity Proofing Service Practice Statement (IPPS)
[4] Termini & Condizioni di contratto dei servizi.
[5] I certificati di CA.
[6] CRL – Liste di revoca dei certificati per tutte le CA.
[7] 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).

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 Regolamento (UE) eIDAS2 e alle Norme 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, alla normativa EU eIDAS2 ed 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.

Intesi Group emette solo certificati che contengono un DN (Distinguished Name) non nullo e conforme allo standard X.500. I certificati possono anche includere altri nomi nel campo SubjectAlternativeName.

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.

Intesi Group genera il subjectDistinguishedName dell'utente per renderlo conforme agli standard ed ai requisiti normativi. Il nome deve comprendere informazioni comunemente comprensibili (nome completo, nome dell'azienda, indirizzo di posta elettronica) per consentire alle terze parti di determinare l'identità della persona e/o dell'organizzazione. L'utente può scegliere di inserire nel certificato qualificato uno pseudonimo invece del proprio nome.

3.1.3 Anonimato e pseudonimia dei titolari

Durante il processo di un'identificazione (cfr.3) o al momento della richiesta del certificato, 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 sarà chiaramente indicato nel campo PSEUDO del subjectDistinghishedName.

L'uso dello pseudonimo è accettato esclusivamente per certificati emessi a persona fisica. L'utilizzo di pseudonimi non è applicabile ai sigilli digitali ed ai certificati TSU.

Intesi Group conserva, in conformità alla normativa vigente, 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.

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.

Fermo restando l'obbligo per il QTSP di valorizzare il campo, relativo all'appartenenza o affiliazione del titolare all'organizzazione, solo dopo aver ricevuto esplicita richiesta e/o indicazione da quest'ultima ed effettuato 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.

Uno stesso utente può avere certificati diversi tutti con lo stesso subjectDistinguishedName, ma due utenti diversi non possono avere lo stesso subjectDistinguishedName rilasciato dalla stessa CA.

Allo scopo di evitare conflitti, Intesi Group aggiunge nel subjectDistinguishedName il campo DNQualifier contenente un codice di registrazione univoco.

Quando il soggetto usa uno pseudonimo, l'unicità dei nomi è garantita dal campo DNQualifier.

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.

Intesi Group non è responsabile per la risoluzione di cause sull'utilizzo dei marchi tra soggetti diversi.

3.2 Verifica dell'identità - eIDAS

Questi metodi saranno gradualmente eliminati e sostituiti dai processi descritti nella sezione seguente. Non saranno più utilizzati a partire dal 22 maggio 2026 e saranno completamente dismessi entro il 19 agosto 2027.

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, utilizzando strumenti di Intesi Group che attivano una connessione sicura, invia la propria chiave pubblica al QTSP sotto forma di CSR nel formato PKCS#10 [RFC2314] e il QTSP dovrà verificare che la firma digitale del CSR sia valida.

Nel caso in cui le chiavi private siano generate all'interno delle sedi di Intesi Group, la verifica viene fatta attraverso un processo interno.

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 al QTSP (tramite RAO) adeguata documentazione emessa da un organismo di autorità come, per esempio, una certificazione (o un documento comparabile) emessa da una camera del commercio o un ufficio pubblico competente.

Quando la persona giuridica è un ente pubblico devono fornire documentazione che dimostri il loro rapporto con l'ente superiore (ad esempio una regione, un ministero) su carta intestata timbrata e firmata da un dirigente autorizzato.

La documentazione deve contenere almeno il nome completo della persona giuridica e informazioni rilevanti come, per esempio, un codice di registrazione della società.

3.2.3 Validazione delle identità individuali

Intesi Group supporta tutti i meccanismi di verifica dell'identità come definito dall'art.24 del regolamento europeo eIDAS che richiede che l'identità ed eventuali attributi specifici della persona fisica o giuridica a cui viene rilasciato il certificato qualificato siano verificati da Intesi Group direttamente o affidandosi a terzi in conformità al diritto nazionale:

a. mediante la presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica; o
b. a distanza, mediante mezzi di identificazione elettronica, che garantiscano una presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica e che soddisfano i requisiti fissati all'articolo 8 del regolamento eIDAS2 riguardo ai livelli di garanzia «significativo» o «elevato»; o
c. mediante un certificato di firma elettronica qualificata o di un sigillo elettronico qualificato o rilasciato a norma della lettera a) o b); o
d. utilizzando altri metodi di identificazione riconosciuti a livello nazionale che forniscono una garanzia equivalente in termini di affidabilità alla presenza fisica. La garanzia equivalente è confermata da un organismo di valutazione della conformità.

I seguenti processi di Identificazione sono condotti dai RAO (cfr. 1.3.6) o da un Pubblico Ufficiale (in base a quanto disposto dalle normative che disciplinano la loro attività) che devono operare secondo le seguenti procedure di identificazione applicate da Intesi Group:

- Identificazione de-visu che avviene con un incontro fisico 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 Corporate IDentity[1].

Per i seguenti processi di identificazione applicati da Intesi Group, l'attività di identificazione RAO viene sostituita da automatismi atti a validare la fonte dei dati:

- Identificazione attraverso verifica firma elettronica qualificata.
- Identificazione attraverso norme antiriciclaggio.
- Identificazione attraverso identità digitali SPID/CIE, ovvero schemi di identità digitale notificati di livello substantial oppure high.

Intesi Group garantisce che tutti i metodi di riconoscimento applicati sono conformi all'articolo 24 della normativa eIDAS2 e ai corrispondenti standard ETSI.

Per la verifica dell'identità con operatore il richiedente deve presentare un documento di riconoscimento. Per i cittadini italiani sono ammessi i seguenti documenti di identità:

- carta d'identità
- passaporto
- patente di guida

Per i richiedenti con cittadinanza di un paese appartenente all'unione europea e diversa da quella italiana sono ammessi i seguenti documenti di riconoscimento:

- passaporto
- carta d'identità nazionale.

[1] Per Corporate IDentity si intendono le credenziali personali di autenticazione di un titolare di account aziendale.

Per i cittadini con cittadinanza extra UE è ammesso:

- passaporto

Per i cittadini con residenza negli Stati Uniti è ammesso:

- un documento di riconoscimento con fotografia rilasciato dal governo nazionale che attesta l'identità del titolare (ad es. carta d'identità, passaporto, carta d'ingresso globale, carta PIV o simile),
- due carte d'identità governative non nazionali, una delle quali deve essere un documento d'identità con fotografia (ad es. patente di guida)[2].

Ogni documento presentato deve avere una data di scadenza e non essere scaduto.

Nel caso di identificazione tramite SPID e CIE, e più in generale schemi di identità digitale notificati, l'acquisizione dei documenti di identità è sostituita dall'acquisizione della asserzioni SAML (o equivalenti) ricevute dai rispettivi identity providers.

Nel caso di identificazione attraverso verifica firma elettronica qualificata viene acquisito il solo documento di contratto firmato digitalmente.

3.2.4 Acquisizione dati di identificazione

Per facilitare gli operatori nell'acquisizione e verifica dei documenti di identificazione, Intesi Group ha introdotto uno strumento che, previa acquisizione del consenso e visualizzazione dell'informativa sulla privacy, utilizza algoritmi di intelligenza artificiale per la verifica biometrica dei candidati, consentendo di:

1. La raccolta delle immagini dei documenti tramite foto eseguita in tempo reale e l'immediata verifica della genuinità dei documenti acquisiti.
2. La verifica della corrispondenza tra la persona che si sta identificando e la fotografia acquisita dal documento d'identità presentato.
3. La presenza fisica del sottoscrittore durante il processo di acquisizione immagini e la prova che sia in possesso del documento di identità presentato.

I dati acquisiti vengono elaborati da un servizio di convalida automatica che consente di stabilire, sulla base di soglie, se possono essere accettati, devono essere rifiutati o necessitano di un ri-controllo da parte di un responsabile Intesi Group.

L'operatore RAO che ha in carico il processo viene informato dell'esito della valutazione e, in caso di esito negativo, non può proseguire con l'approvazione dell'identificazione.

3.2.5 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 documenti di identità validi (non

2 Esempi di documenti di identità accettabili possono essere trovati nel seguente sito https://www.fedidcard.gov/document/acceptable-forms-id

scaduti) che possono essere acquisiti manualmente dall'operatore RAO o attraverso lo strumento definito in 3.2.4 .

I documenti di identificazione devono contenere:

- nome e cognome,
- data e luogo di nascita,
- un numero di serie o altri attributi che possono essere utilizzati per risolvere casi di omonimia.

È inoltre consentito controllare indirettamente l'identità del richiedente utilizzando mezzi che forniscono un livello di garanzia equivalente alla presenza fisica (ad esempio se il richiedente è già in possesso di un certificato qualificato, il che implica che il richiedente è stato già identificato).

Nel caso in cui il soggetto stia richiedendo:

- un certificato per sigillo elettronico,
- un certificato contenente l'appartenenza/affiliazione ad una società 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 acquisita e nel caso in cui la ritenga sufficiente e o risulti valida anche sulla base delle valutazioni automatiche restituite dal servizio descritto in 3.2.4, può 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.

Il RAO dovrà trattenere con sé la copia cartacea firmata che dovrà poi consegnare in un secondo tempo ad Intesi Group.
Intesi Group avrà cura di conservare sia le copie digitali che quella cartacea secondo quanto previsto dalla normativa vigente.

Le informazioni registrate per il rilascio di ciascun certificato sono:

- L'identità del RAO o della LRA.
- Una dichiarazione firmata dal RAO di aver verificato l'identità del richiedente.
- La data e l'ora della verifica.
- Una dichiarazione di identità firmata dal richiedente con una firma autografa o una firma elettronica appropriata.

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 può approvare l'emissione del certificato di firma o del sigillo.

3.2.6 Identificazione tramite processi LRA

Intesi Group può accettare modalità di identificazione differenti da quelle previste dai propri processi ed adottate da aziende clienti autorizzate a svolgere attività di LRA dopo avere attentamente verificato che la procedura adottata sia adeguata ed aderente con le modalità previste dalla normativa eIDAS2, dalla normativa italiana e dal presente TSPPS.

3.2.7 Identificazione e registrazione IDentify Web.

Questa modalità di identificazione viene svolta da un operatore RAO tramite videoconferenza con il richiedente del certificato. Il sistema di videoconferenza è fornito da Intesi Group, che provvede a mettere a disposizione del richiedente tutte le istruzioni necessarie per l'accesso, l'informativa sulla privacy e la documentazione contrattuale, il cui consenso viene acquisito dall'operatore durante la video-intervista. Il richiedente, da parte sua, deve essere in possesso 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 video intervista guidata volta a verificare la reale presenza del richiedente e l'autenticità dei documenti presentati.

Il RAO che effettua l'identificazione accerta l'identità del Titolare verificando uno o più documenti di riconoscimento, che possono essere stati precedentemente acquisiti mediante inserimento manuale da parte dell'utente o attraverso lo strumento descritto al paragrafo 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 e/o se il processo in 3.2.4 restituisce una valutazione negativa.

Il RAO può inoltre non avviare o interrompere il processo di identificazione nel caso in cui la sessione 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 l'operatore riassume le volontà dell'utente in relazione ai trattamenti dei dati personali e all'erogazione del servizio di firma e ne raccoglie conferma.

L'utente viene preventivamente informato circa le modalità e i propri diritti in relazione al servizio in quanto lo stesso riceve tutta la relativa documentazione prima della sessione video con operatore.

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.

3.2.8 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 il modulo di richiesta certificato e firmarlo digitalmente con il certificato qualificato in suo possesso.
2. Inviarlo ad un RAO abilitato o direttamente ad intesi Group attraverso uno dei canali messi a disposizione.

Alla ricezione del documento firmato, il RAO o il servizio Intesi Group verificano 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 ha successo viene approvata l'emissione del certificato, in caso contrario la richiesta verrà rigettata informandone l'utente. In questo caso la copia del contratto firmato verrà conservata secondo quanto previsto dalla normativa vigente.

3.2.9 Identificazione attraverso norme antiriciclaggio

L'identificazione può essere eseguita da uno dei soggetti destinatari della normativa Antiriciclaggio, più precisamente a livello EU Direttiva 815/2015 (c.d. IV Direttiva) e Direttiva 2018/843 (c.d. V Direttiva), a livello Nazionale dal D. lgs. 21 novembre 2007, n. 231, come modificato dal D.lgs. 25 maggio 2017 n. 90 e dalle *Disposizioni in materia di Adeguata Verifica della Clientela per il contrasto del riciclaggio e del finanziamento del terrorismo* del 30 luglio 2019.

Tali soggetti devono provvedere ad identificare in maniera certa le persone fisiche in conformità alle summenzionate disposizioni. In ogni caso, la modalità con cui l'identificazione viene posta in essere dall'Istituto Bancario/Finanziario deve essere preventivamente concordata con il QTSP Intesi Group.

L'Istituto Bancario/Finanziario agendo in qualità di Local Registration Authority si impegna ad acquisire tutte le informazioni ed i relativi consensi necessari e pertinenti al fine di permettere al QTSP Intesi Group di emettere certificati di firma qualificata.

In ogni caso il QTSP Intesi Group si riserva la facoltà di verificare ed eventualmente adottare processi differenti rispetto a quanto sopra esposto in conformità alle disposizioni e regolamenti che disciplinano tali servizi.

3.2.10 Identificazione attraverso identità digitali SPID

Questa modalità di identificazione avviene attraverso una autenticazione sul portale Intesi Group utilizzando una credenziale SPID almeno di livello 2. L'accesso alla pagina di autenticazione avviene attraverso un link univoco e non riutilizzabile generato dal portale stesso su richiesta di un operatore o di una applicazione integrata con i servizi Intesi Group.

Il servizio Intesi Group, ricevendo dall'Identity Provider SPID la risposta all'autenticazione in formato SAML, verifica che:

1. non contenga messaggi di errore e che contenga l'asserzione di autenticazione;
2. sia firmato col certificato dell'identity provider contenuto nel metadata;
3. sia conforme alle "Regole tecniche SPID";
4. contenga tutti i dati necessari per l'emissione del certificato;

Se la risposta risulta valida allora viene salvata e conservata come dato di identificazione, l'utente viene registrato ed invitato ad eseguire la procedura di generazione del certificato.

Il certificato qualificato rilasciato conterrà l'OID 1.3.76.16.5, registrato a cura dell'Agenzia, con la seguente descrizione: "*Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity*". Se la risposta invece non è valida, all'utente viene presentato un messaggio che lo informa sulla causa dell'errore fornendo eventuali indicazioni su come procedere con la loro risoluzione.

3.2.11 Identificazione attraverso carta d'identità elettronica CIE

Questa modalità di identificazione avviene attraverso una autenticazione sul portale Intesi Group utilizzando la propria Carta d'identità elettronica (CIE) secondo le modalità previste dal portale CieID. L'accesso alla pagina di autenticazione avviene attraverso un link univoco e non riutilizzabile generato dal portale stesso su richiesta di un operatore o di una applicazione integrata con i servizi Intesi Group.

Il portale Intesi Group, ricevendo dal server CieID la risposta all'autenticazione in formato SAML, verifica che:

1. non contenga messaggi di errore e che contenga l'asserzione di autenticazione;
2. la firma sia valida e apposta usando il certificato dell'identity provider CIE contenuto nel metadata;
3. contenga tutti i dati necessari per l'emissione del certificato;

Se la risposta risulta valida allora viene salvata e conservata come dato di identificazione, l'utente viene registrato ed invitato ad eseguire la procedura di generazione del certificato.

Se la risposta invece non è valida, all'utente viene presentato un messaggio che lo informa sulla causa dell'errore fornendo eventuali indicazioni su come procedere con la loro risoluzione.

Lo stesso processo si applica in generale agli schemi di identità digitale notificati al livello UE, fatte salve le specificità tecniche dell'Identity Provider che eroga il servizio nell'ambito di uno specifico schema e Stato Membro.

3.3 Verifica dell'identità – eIDAS2

A partire dal 22 maggio 2026, Intesi Group agisce come Identity Proofing Service Provider (IPSP), fornendo il servizio di verifica dell'identità come componente del servizio fiduciario qualificato per il rilascio di certificati digitali. Tutte le pratiche, le misure tecniche e organizzative e le procedure operative relative alla verifica dell'identità dei soggetti (persone fisiche e giuridiche) sono descritte nel documento separato denominato "Identity Proofing Service Practice Statement (IPSPS)" [3] liberamente scaricabile dal sito istituzionale Intesi Group all'URL https://www.intesigroup.com/it/qtsp/documenti/.

Il servizio di Identity Proofing è denominato IG Persona ed è progettato per garantire l'Extended Level of Identity Proofing (LoIP), in conformità con l'articolo 24 del Regolamento (UE) 2024/1183 (eIDAS 2) e allo standard ETSI TS 119 461.

Tali processi di identificazione saranno introdotti a partire dal 22 maggio 2026 e diventeranno gli unici metodi utilizzati per la verifica dell'identità a partire dal 19 agosto 2027.

3.3.1 Metodi di Identificazione e OID Associati

Le politiche applicate per ciascun metodo di identificazione adottato da Intesi Group sono identificate dai seguenti **Object Identifier (OID)**, come dettagliato nell'IPSPS [3]

Descrizione del Metodo di Identificazione	Intesi OID
Identificazione in presenza con funzionamento ibrido manuale/automatizzato (Rif. ETSI TS 119 461 par. 9.2.1.3).	1.3.6.1.4.1.48990.1.1.9.1
Identificazione da remoto non presidiata con funzionamento ibrido manuale/automatizzato (Rif. ETSI TS 119 461 par. 9.2.3.3).	1.3.6.1.4.1.48990.1.1.9.2
Identificazione tramite mezzi eID notificati con livello di garanzia "Elevato" (SPID Livello 3 e CIE) (Rif. ETSI TS 119 461 par. 9.2.4).	1.3.6.1.4.1.48990.1.1.9.3
Identificazione basata su Firma Elettronica Qualificata o sigillo elettronico qualificato esistente (Rif. ETSI TS 119 461 par. 9.2.5).	1.3.6.1.4.1.48990.1.1.9.4
Identificazione persona giuridica (Rif. ETSI TS 119 461 par. 9.3).	1.3.6.1.4.1.48990.1.1.9.5
Identification persona fisica in rappresentanza di una persona giuridica (Rif. ETSI TS 119 461 par. 9.4).	1.3.6.1.4.1.48990.1.1.9.6

3.3.2 Requisiti e Procedure di Verifica

Per i dettagli relativi alle seguenti fasi del processo di verifica dell'identità, si rimanda integralmente alle sezioni corrispondenti dell'**IPSPS**:

- **Fase preliminare**: Informazioni al richiedente e raccolta del consenso.
- **Raccolta dei dati**: Tipologia di prove di identità accettate (documenti fisici, eID, certificati qualificati) e modalità di acquisizione.
- **Validazione**: Verifiche di sicurezza sui documenti, *liveness detection*, video identificazione e controlli antifrode.
- **Binding al Richiedente**: Procedure per stabilire il legame certo tra l'identità verificata e il richiedente.
- **Rilascio del Risultato**: Generazione dello score di affidabilità e approvazione finale

3.3.3 Gestione delle Evidenze e Conservazione

Le evidenze raccolte durante il processo di identificazione (dati estratti, registrazioni multimediali, log degli operatori) sono conservate in modo sicuro per garantire l'integrità e l'immodificabilità. In conformità alla normativa vigente, tali prove sono conservate per un periodo di 20 anni dal completamento del processo al termine del quale i dati vengono cancellati.

3.3.4 Ruoli di Fiducia e Formazione

Il personale addetto alla verifica (Registration Officer -RAO) opera secondo i mandati e le procedure definite nell'IPSPS, ricevendo una formazione specialistica continua su tecniche di prevenzione delle frodi, analisi morfologica del volto e protezione dei dati personali

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

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

3.5 Identificazione e autenticazione per richieste di revoca

Per le richieste di sospensione e di revoca attraverso il portale CA è necessario che l'utente effettui il 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 al QTSP o ad una LRA autorizzata. Il certificato di firma elettronica qualificata può contenere, ove richiesto dal titolare di firma elettronica o dal terzo interessato, le seguenti informazioni: le qualifiche specifiche del titolare di firma elettronica, quali l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza.

La richiesta per un certificato qualificato emesso a persona giuridica può essere fatta da una persona fisica che è autorizzata a rappresentare la persona giuridica purché presenti al QTSP o ad una LRA autorizzata la domanda corredata da apposita documentazione che attesti tale qualifica.

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 emissione e responsabilità

Il processo di registrazione viene svolto a valle del processo di identificazione (cfr. par 3) e 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 del QTSP;
  4. Dichiarare di avere preso visione del presente TSPPS e di averlo compreso e accettato;
  5. Eseguire la procedura di generazione chiavi ed emissione del certificato secondo le indicazioni fornite dal QTSP;
- dove richiesto, il RAO che deve effettuare:
  1. il riconoscimento dell'utente come descritto ai paragrafi 3.2 e 3.3;
  2. approvare l'emissione del certificato di firma o del sigillo.
  3. Laddove previsto, inviare copia dei documenti acquisiti al QTSP;
- Il QTSP deve:
  1. emettere il certificato di firma o di sigillo;
  2. conservare i dati di identificazione dell'utente e tutte le informazioni raccolte durante il processo di registrazione per l'emissione dei certificati di firma o di sigillo;
  3. mantenere e diffondere informazioni sullo stato di certificati di firma e di sigillo.

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 Intesi Group.

4.2 Processo di emissione

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

1. L'utente viene identificato secondo uno dei processi descritti ai paragrafi 3.2 e 3.3.
2. Il QTSP, acquisiti e validati i dati e la documentazione, comunica all'utente (ad. esempio attraverso e-mail) l'approvazione della richiesta e le informazioni necessarie per emettere il certificato.
3. Il titolare emette il certificato eseguendo uno dei processi definiti in 4.3 entro sette giorni. Oltre tale intervallo temporale, l'utente deve rivolgersi al supporto Intesi Group.

La procedura di emissione dei certificati qualificati può essere eseguita solamente dall'utente titolare del certificato o, nel caso di emissione dei certificati qualificati, dal RAO in presenza dell'utente titolare . 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 di residenza;
- Numero di telefono mobile;
- Indirizzo e-mail;
- Codice fiscale o codice equivalente;

Per richiedere un certificato per persona giuridica deve fornire anche:

- Nome della società;
- Codice tributario della società (es. partita IVA per le aziende italiane);
- Indirizzo della società (stato, provincia, città ed indirizzo);
- E-mail e numero di telefono della società;
- Informazioni necessarie per dimostrare i poteri di rappresentanza.

4.2.2 Registrazione e autenticazione

La registrazione e la convalida dei dati sono descritte nel documento 'Identity Proofing Service Practice Statement' (IPSPS) **Errore. L'origine riferimento non è stata trovata.** ai paragrafi 3.2, 3.3 e 3.4.

4.2.2.1 Credenziali autenticazione soggetto

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

Le credenziali di accesso possono già essere in possesso dell'utente oppure possono essere generate automaticamente durante il processo di identificazione e registrazione. In quest'ultimo caso, al primo accesso, il sistema richiederà all'utente la definizione della password.

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 raggiungibile all'url https://pkra.time4mind.com 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 client certificate authentication per ottenere l'accesso ai servizi. I certificati di autenticazione sono generati e distribuiti da personale interno Intesi Group a seguito delle procedure di incarico delle LRA definite dal QTSP Intesi Group.

4.3 Emissione del certificato

4.3.1 Emissione del certificato di firma remota

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 il dispositivo fornito dal RAO a seguito della registrazione.
- gli utenti che fanno uso di token OTP generati tramite App Mobile IG You, prima di avviare la procedura di emissione certificato devono assicurarsi di avere installato l'App sul proprio dispositivo mobile, nel caso in cui non l'abbiano ancora installata la procedura di emissione fornisce indicazioni su dove trovarla. 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 dai frontend Time4Mind di Intesi Group oppure, nei casi in cui si applica, direttamente dall'App mobile IG You.

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 o SMS per autenticare la richiesta di emissione. In alternativa l'utente può saltare questi passi cliccando sul link ricevuto con l'e-mail di conferma registrazione. L'indirizzo e-mail o il numero di telefono utilizzati per l'invio delle security code sono quelli verificati in fase di identificazione del soggetto.

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 IG You per cui la procedura, una volta avviata proseguirà dall'interno dell'App dopo avere effettuato un login tramite username e password (cfr 4.2.2.1) e usando il security code inviato tramite e-mail.

Quest'ultima 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 processo di emissione del certificato si completa con l'invio di un messaggio di conferma avvenuta emissione all'indirizzo e-mail fornito in fase di identificazione.

Intesi Group verifica l'accuratezza e la validità di tutti i dati necessari per il rilascio di un certificato qualificato in base al Regolamento UE eIDAS2 ed ai corrispondenti standard ETSI. Intesi Group rilascerà il certificato al termine del processo sopra descritto oppure informerà il richiedente di eventuali problemi o incongruenze.

4.3.1.1 Emissione di certificato short-term

Per certificati di firma remota cloud-based di tipo short-term i processi di identificazione, emissione della credenziale e apposizione della firma avvengono nello stesso momento. L'emissione della credenziale e l'apposizione della firma avvengono a seguito dell'inserimento da parte dell'utente di un codice OTP ricevuto via SMS o e-mail sul numero di telefono fornito in fase di identificazione.

4.3.2 Emissione del certificato su dispositivo fisico QSCD

Per rilasciare i certificati di firma e di sigilli qualificati su dispositivo fisico (smartcard o token), Intesi Group fornisce direttamente o attraverso fornitori selezionati, solamente dispositivi approvati e pubblicati nell'elenco dei QSCD degli Stati membri, disponibile qui:

https://esignature.ec.europa.eu/efda/notification-tool/#/screen/browse/list/QSCD_SSCD.

Il processo di personalizzazione avviene attraverso software selezionati da Intesi Group e prevede verifiche sui codici seriali dei dispositivi allo scopo di controllare che siano contenuti negli elenchi dei QSCD riconosciuti da Intesi Group. Nel caso in cui il dispositivo non sia tra questi elenchi la personalizzazione viene interrotta. Gli utenti che richiedono un certificato su dispositivo QSCD (smartcard o token USB) devono prima installare

sul proprio PC il software necessario per la gestione del dispositivo e per l'emissione del certificato. Indicazioni su dove scaricare il software e la procedura di installazione verranno fornite dal QTSP o dal RAO a seguito del processo di identificazione. La procedura di personalizzazione del token di firma e l'emissione del certificato avviene attraverso questi passi:

1. Il richiedente deve inserire il dispositivo QSCD nell'apposito lettore di smartcard o nella porta USB del proprio PC e quindi deve avviare il software IG Desk per la gestione del dispositivo QSCD.
2. Deve quindi avviare la procedura di personalizzazione del proprio token di firma selezionando l'apposito menu. All'avvio della procedura gli verrà richiesto di inserire le credenziali di autenticazione ed il "security code" che ha ricevuto tramite SMS a seguito della identificazione.
3. Si avvia così la generazione di una coppia di chiavi sul dispositivo QSCD e la generazione di una richiesta di certificato in formato PKCS#10. La richiesta di certificato e le credenziali di autenticazione sono inviate al QTSP attraverso un canale sicuro protetto dal protocollo TLS (Transport Layer Security).
4. Alla ricezione della richiesta Intesi Group verificherà l'accuratezza e la validità di tutti i dati necessari per il rilascio di un certificato qualificato seguendo quanto definito nel Regolamento eIDAS2 ed ai corrispondenti standard ETSI.
5. Se il processo di verifica si conclude con successo, Intesi Group rilascerà il certificato che verrà restituito al chiamante oppure risponderà con un messaggio di errore contenente le ragioni del rifiuto.
6. Alla ricezione del certificato il software di personalizzazione lo installerà sul token di firma completando così la procedura di personalizzazione.

Il processo di emissione del certificato si completa con l'invio di un messaggio di conferma avvenuta emissione all'indirizzo email fornito in fase di identificazione.

4.3.3 Emissione del certificato TSA

La richiesta di certificato viene eseguita manualmente da un operatore TSP dopo avere informato il TSP Operation Officer che supervisiona l'intera attività. Il processo si svolge come segue:

- l'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 e genera la richiesta di certificato in formato PKCS#10.
- l'operatore TSP si collega alla console di amministrazione della PKI Intesi Group ed utilizzando il PkCS#10, genera il certificato di marcatura.
- l'operatore TPS, agendo sul software di generazione marche, procederà con l'installazione del certificato sull'HSM e alla attivazione sul servizio di marcatura temporale.

4.3.4 Emissione di un certificato di test

Nel caso sia necessario emettere certificati in ambiente di produzione per eseguire specifici test, la richiesta deve essere approvata dal Responsabile della CA.

Per questa particolare tipologia di emissioni, viene utilizzato un O.I.D. specifico (vedere paragrafo 1.4 per maggiori dettagli), e all'interno del certificato, è sempre presente la seguente limitazione d'uso: "*Le firme apposte con questo certificato sono valide solamente a scopo di test. Signatures created with this certificate are only valid for testing*."

All'interno del Common Name del certificato viene inserito il prefisso *"[TEST] {NAME} {SURNAME} for testing purpose only*"

I certificati debbono poi essere prontamente revocati al termine della sessione di test.

4.4 Accettazione del certificato

4.4.1 Accettazione del Certificato

4.4.1.1 Accettazione del certificato

Alla ricezione del certificato il titolare deve verificarne il contenuto. Nel caso in cui rilevi difetti o errori tali da renderlo inaccettabile deve immediatamente informare Intesi Group che provvederà a revocarlo e ad eseguire le procedure per una nuova emissione.

Se un certificato non viene rifiutato entro 7 giorni dalla data di ricezione viene considerato accettato.

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 del QTSP

I certificati qualificati non sono resi disponibili a terze parti e vengono conservati nel repository interno del QTSP.

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

Una e-mail contenente un messaggio di conferma emissione viene inviata all'indirizzo e-mail fornito in fase di identificazione. 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.
- utilizzare la chiave privata solamente per apporre firme digitali o sigilli a seconda del certificato associato. Non è possibile usare le chiavi per altri scopi (es. crittografia dei dati).
- 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 di certificato se ha fondate ragioni di credere che la chiave sia stata compromessa.
- 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 al QTSP 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 periodo massimo di 3 mesi.

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 dal QTSP attraverso i propri repository ed i cui riferimenti sono contenuti nel certificato 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.

Inoltre, devono essere verificate eventuali limitazioni d'uso.

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.

Il QTSP 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 e solo se:

- il certificato è valido quindi non scaduto e non revocato o sospeso.
- I dati personali, contenuti all'interno del certificato, non sono modificati.

La procedura di rinnovo può essere avviata solo trenta 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 IG You (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. Inserire le quantità di sblocco della credenziale.

Fatto questo, il QTSP 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 un operatore 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:

- Trenta giorni prima della scadenza, il server può inviare al soggetto una e-mail 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 emissione del 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 del QTSP 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 dal QTSP 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. Un certificato viene revocato quando il legame tra il titolare e la chiave pubblica contenuta all'interno del certificato non sono più validi. Alcuni esempi per cui il legame è da considerarsi invalido, a titolo esemplificativo ma non esaustivo sono:

- I dati di identificazione contenuti nel certificato diventano invalidi.
- E' dimostrata una violazione del contratto di sottoscrizione o del presente TSPPS.
- Il titolare o un operatore autorizzato chiedono la revoca del certificato.
- Segnalazioni da parte delle autorità.

Ogni qualvolta si verifica una di queste circostanze il certificato sarà revocato ed inserito nella CRL e in tutte le nuove pubblicazioni delle informazioni sullo stato del certificato.

A seguito della revoca del certificato la coppia di chiavi non può più essere utilizzata per apporre firme e non potrà più essere riutilizzata per emettere un nuovo certificato o un nuovo sigillo.

Infine, se una chiave privata utilizzata per approvare le richieste di emissione di uno o più certificati risulta essere stata compromessa, tutti i certificati autorizzati dalla data della compromissione effettiva o sospetta

e direttamente o indirettamente collegati a quella chiave privata saranno revocati o comunque ne sarà verificata la corretta emissione. L'operazione di revoca è irreversibile.

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. QTSP se ne ravvisa la necessità.

Per i certificati che contengono il nome di una organizzazione (terzo interessato), Intesi Group accetta richieste di revoca anche da parte della persona (punto di contatto) indicata dall'organizzazione. L'organizzazione deve altresì informare Intesi Group di eventuali cambiamenti sullo stato di appartenenza di un soggetto all'organizzazione e qualora il titolare non sia più autorizzato ad utilizzarne il nome, Intesi Group provvederà a revocare tutti i certificati rilasciati al soggetto e contenenti il nome dell'organizzazione.

Per i certificati TSU la revoca può essere eseguita solamente dai TSP Operator Officer 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 "Revoca" 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 e-mail 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.
- QTSP.

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 e-mail inviata al titolare.

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, aprendo un ticket all'URL:

https://support.intesigroup.com

Quando a richiedere la revoca è un RAO, il ticket deve essere aperto entro otto ore dal momento del ricevimento della richiesta di revoca da parte del soggetto.

Ogni richiesta 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'e-mail, un operatore di Intesi Group prenderà in carico l'attività verificando la correttezza delle informazioni fornite. 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 e-mail inviata al titolare.

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

Il QTSP 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 il QTSP deve elaborare la richiesta di revoca

Quando il QTSP riceve una richiesta di revoca prova ad eseguire l'operazione immediatamente e comunque non oltre le 24h dalla data di ricezione della richiesta. 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 viene informato tramite un messaggio e-mail.

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, il QTSP 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. Il QTSP riceve una richiesta di revoca che non contiene le informazioni necessarie per autenticare il richiedente.
2. Il QTSP, 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.

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 almeno trenta giorni, dopo i quali il certificato viene automaticamente riattivato.

Fermo restando quanto sopra, il personale di Intesi Group si riserva di estendere il periodo di sospensione qualora debba attendere specifiche indicazioni nel merito da parte delle forze dell'ordine o da parte dell'organismo di vigilanza.

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 [RFC6960].

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 Servizi verifica marca temporale

Le marche temporali emesse da Intesi Group sono qualificate ai sensi della normativa eIDAS (Regolamento UE n. 910/2014) e conformi alla versione aggiornata eIDAS2.

Esse rispettano pienamente le specifiche tecniche previste dalla RFC 3161 e dallo standard ETSI EN 319 422, e possono quindi essere verificate:

- tramite gli strumenti messi a disposizione da Intesi Group, come PkBox;
- oppure mediante qualsiasi altro verificatore che supporti la verifica di marche temporali qualificate secondo la normativa UE.

4.12 Cessazione del contratto

Il contratto tra il QTSP 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.

4.13 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, il QTSP 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, EN 319 411-2 e EN 319 421 e la certificazione ISO/IEC 27001 (Sistema di Gestione della Sicurezza delle Informazioni certificato) di Intesi Group.

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

Per garantire la sicurezza fisica tutti i sistemi usati per le attività QTSP sono fisicamente separati dagli altri sistemi di Intesi Group in modo da garantire l'accesso al solo personale con ruolo System Administrator e in possesso di badge abilitato all'apertura del rack.

Le chiavi private utilizzate per l'emissione dei certificati qualificati e per la firma delle risposte OCSP sono conservate su dispositivi non vulnerabili all'accesso fisico (HSM e server antitampering), a prova di manomissione e che soddisfano i requisiti del regolamento (UE) eIDAS2 e delle corrispondenti norme ETSI.

Tutti i dispositivi sono protetti da accessi non autorizzati sia durante l'installazione che durante il periodo di attivazione. I controlli sono applicati in modo tale da ridurre il rischio di manomissione anche quando i dispositivi non sono installati o non sono attivi.

Intesi Group effettua con regolarità dei test di sicurezza per garantire che tutti questi controlli funzionino correttamente. L'accesso a qualsiasi area fisica in cui si trovano informazioni o apparecchiature sensibili e per le operazioni di CA è limitato e monitorato dal sistema di allarme interno.

Tutti i sistemi informatici utilizzati per la prestazione di servizi fiduciari qualificati descritti nel presente documento sono ospitati nel datacenter di Intesi Group, che è protetto da:

- un sistema di **controllo all'accesso fisico**, in modo tale che l'accesso all'edificio e ai rack in cui sono ospitati i servizi QTSP sia permesso esclusivamente a personale autorizzato in possesso di un pass personale e del PIN corrispondente;
- da un sistema di video sorveglianza che consente, al solo personale autorizzato, di verificare l'integrità dei dispositivi QTSP.
- da un **sistema di protezione antincendio** che include **antifumo** (VEWASD) e impianto di estinzione apposito;
- da un **sistema di alimentazione** completamente ridondante a tutti i livelli (trasformatori, centri di energia, generatori, UPS, pannelli di distribuzione, etc.)
- da un sistema di **aria condizionata** (HVAC) che garantisce condizioni di lavoro ottimali;
- da una **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 e le procedure operative necessarie. L'analisi del rischio viene eseguita con pieno supporto e collaborazione di tutti i fornitori di servizi componenti ed è regolarmente revisionata e corretta. 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.

Gli strumenti ed i sistemi utilizzati per lo sviluppo ed il test sono fisicamente separati dalle strutture operative. In Intesi Group sono definite procedure per la segnalazione di malfunzionamenti del software e per garantire che le segnalazioni siano prese in carico e vengano intraprese azioni correttive. Gli utenti che hanno accesso ai sistemi del QTSP sono inoltre tenuti a segnalare eventuali problemi di sicurezza dei sistemi o dei servizi che hanno verificato o di cui hanno il sospetto. Tutta la documentazione prodotta è protetta da accessi non autorizzati.

Le risorse richieste in termini di potenza di calcolo delle macchine e di dimensione degli storage sono costantemente monitorate. Intesi Group esegue proiezioni d'uso allo scopo di garantire che siano sempre disponibili risorse adeguate.

Sono attuate procedure per la sensibilizzazione degli utenti all'uso di strumenti per il rilevamento e la prevenzione da virus e software malevolo.

Esiste infine una procedura per la gestione degli incidenti che stabilisce le responsabilità e le azioni da intraprendere a fronte di una rilevazione di un incidente. Questa procedura è definita in modo tale da garantire una risposta rapida ed efficace agli incidenti di sicurezza che dovessero verificarsi

Tutte le procedure operative sono documentate nel Sistema di Gestione della Qualità aziendale, certificato in conformità con lo standard ISO 9001, e nelle procedure operative del QTSP.

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.

Tutto il personale del QTSP ha adeguate conoscenze ed esperienza riguardo le operazioni che vengono eseguite all'interno di un QTSP. Il personale viene autorizzato ad operare solo dopo aver dimostrato consapevolezza sulla sicurezza riguardo ai propri compiti come operatore QTSP.

Periodicamente vengono effettuate verifiche sull'affidabilità di tutto il personale. Nessun utente non autorizzato ha accesso ai sistemi in cui sono memorizzati dati sensibili. Tutti i sistemi che conservano tali dati si trovano all'interno di un'area protetta ad accesso controllato; l'accesso ai dati è consentito solo alle persone autorizzate.

I dipendenti firmano un accordo di riservatezza (non divulgazione) come parte dei loro termini e condizioni di lavoro. Tutti i dipendenti del QTSP ed eventuali utenti terzi ricevono un'adeguata formazione sulle procedure organizzative.

Intesi Group ha definito delle sanzioni disciplinare per azioni che violano le policy e le procedure di sicurezza dell'organizzazione. Le procedure definite da Intesi Group specificano le sanzioni nei confronti del personale che compie azioni non autorizzate, uso non autorizzato dell'autorità e uso non autorizzato dei sistemi.

Intesi Group ha previsto sanzioni disciplinari per azioni che violano gli accordi contrattuali e le policy di sicurezza. In caso di cessazione del rapporto di lavoro di una delle persone autorizzate ad operare vengono intraprese azioni appropriate per garantire che la sicurezza non venga compromessa.

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

1. **Head of QTSP**: 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 della verifica della conformità dei servizi TSP ai requisiti normativi e agli standard.
7. **Registration Officer**: è autorizzato ad approvare l'emissione o la revoca di certificati. Queste persone non ricoprono altri ruoli nell'ambito delle operazioni QTSP.

Tutto il personale che opera 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 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.
Nessuna persona può individualmente modificare o cancellare i log file o file di audit.

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 conservazione del registro audit

I file di log vengono conservati per 20 anni al termine del quale i dati vengono cancellati.

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

Il QTSP 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 al termine del quale i dati vengono cancellati.

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 e-mail 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 del QTSP

In caso di terminazione verrà applichata la procedura di cessazione definita come procedura interna. Tale procedura prevede apposite comunicazioni inviate ai titolari dei certificati, alle terze parti e agli organismi di controllo.

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 140-3 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 gestito da Intesi Group o dislocato nella sala macchine di clienti di Intesi Group e viene registrata dal sistema di auditing interno.
- su un dispositivo certificato QSCD (SmartCard o dispositivo USB) in possesso dell'utente.
- Su un QSCD gestito da un cliente che figura nella Trusted List applicabile come prestatore di servizi fiduciari qualificato per la gestione di dispositivi qualificati per la creazione di firme elettroniche qualificate da remoto e/o di sigilli elettronici qualificati da remoto. Questa opzione è subordinata a una verifica preventiva e documentata della conformità a tutte le condizioni applicabili per la certificazione del QSCD

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.

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 140-3 Level 3 e Common Criteria (ISO 15408) EAL 4.

6.1.2 Consegna della chiave privata al titolare

Le chiavi private possono essere generate e conservate:

1. su un dispositivo QSCD sito nella sala macchine di Intesi Group o nella sala macchine di clienti 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.
2. su un dispositivo certificato QSCD (SmartCard o dispositivo USB) in possesso dell'utente.

6.1.3 Consegna della chiave pubblica all'emittente del certificato

Le chiavi pubbliche vengono inviate al QTSP attraverso i software messi a disposizione da Intesi Group sotto forma di una richiesta PKCS#10 utilizzando un canale HTTP protetto da un protocollo TLS v 1.2.

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 coppie di chiavi sono generate in accordo alla normativa eIDAS, allo standard ETSI TS 119 312 e alle indicazioni ENISA *Agreed Cryptographic Mechanisms*.

In particolare:

- Le chiavi Root CA vengono generate con l'algoritmo RSA ed hanno lunghezza 4096 bits o l'algoritmo NIST ECDSA P-521.
- Le chiavi per i certificati utente e per certificati di TSU vengono generate con l'algoritmo RSA ed hanno lunghezza 3072 bits o l'algoritmo NIST ECDSA P-256.
- I certificati per la firma di CRL, OCS e marcatura temporale dal 1 gennaio 2026 vengono generate con l'algoritmo RSA e hanno lunghezza di 3072 bit.

6.1.6 Generazione dei parametri e qualità della chiave pubblica

Gli algoritmi ed i parametri utilizzati da Intesi Group per la generazione delle coppie di chiavi per certificati e sigilli qualificati sono conformi allo standard ETSI 119 312, alla normativa eIDAS2 e alla normativa Italiana.

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

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

Intesi Group garantisce la gestione sicura delle chiavi private della CA usate per l'emissione di certificati qualificati e delle chiavi private utilizzate per la firma delle informazioni sullo stato di revoca (CRL, OCSP). Intesi Group impedisce la divulgazione, la copia, la cancellazione, la modifica e l'utilizzo non autorizzato delle chiavi private. Le chiavi private della CA sono conservate in un Hardware Security Modules (HSM) custodito in un luogo fisicamente sicuro.

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 140-3 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 dispositivi certificati 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 consentita solo a System Administrator e sotto la supervisione del TSP Operation Officer. Nessuna singola persona ha tutti i dati di attivazione necessari per accedere alle chiavi private della CA.

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 applicati 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.

Il meccanismo di attivazione delle chiavi private gestite da Intesi Group è gestito dal componente SAM (Security Access Module) facente parte dell'architettura PkBox e oggetto di certificazione QSCD.

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, ETSI EN 319 411-2 e ETSI EN 119 431-1 e alle procedure ISO/IEC 27001 di Intesi Group. Le configurazioni dei sistemi sono controllate dal sistema di monitoraggio interno e dal SOC (Security Operation Center). Qualsiasi modifica non pianificata e rilevata dai sistemi di monitoraggio viene valuta e, nel caso, gestita come incidente.

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.

Intesi Group utilizza solamente:

- hardware e software commerciali progettati e sviluppati con una metodologia di progettazione documentata, oppure;
- hardware e software proprietari sviluppati da un soggetto affidabile in un ambiente controllato e utilizzando metodi di sviluppo strutturati, oppure;
- software open source conformi ai requisiti di sicurezza e la cui adeguatezza è garantita da processi interni di verifica e convalida del software.

Tutti i nuovi componenti vengono prima testati in un apposito ambiente di test prima di essere utilizzati in ambiente di produzione. Gli ambienti di produzione e di sviluppo sono totalmente separati. L'hardware viene acquistato in modo da ridurre la probabilità di manomissione durante la spedizione. L'hardware utilizzato è dedicato alle sole operazioni QTSP.

6.7 Controlli di sicurezza di rete

I controlli di sicurezza della rete sono effettuati attraverso l'uso di: firewall, comunicazioni protette da autenticazione, protezione antivirus, 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, ETSI EN 319 411-2 e ETSI 119 431-1.

Intesi Group si avvale di un Security Operations Center (SOC) che monitora i sistemi 24 ore su 24, 7 giorni su 7, segnalando tempestivamente al gruppo CISO eventuali anomalie, manomissioni o tentativi di intrusione.

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. Le marche temporali sono emesse con una accuratezza di 1 secondo.

6.9 Inventario delle risorse

Con cadenza semestrale, Intesi Group esegue un audit interno per verificare se sono state apportate modifiche significative agli asset allo scopo di accertare che la security policy in termini di idoneità, adeguatezza ed efficacia sia rispettata. Il risultato di ogni audit viene registrato in un internal audit report.

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>

Campo	Valore
Estensioni 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

Campo	Valore
Version Number	V3
Signature	RSA with SHA-256 EC-DSA with SHA-256
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> <ECDSA public key of 521bits>
Signature Value	<Root CA signature>
Estensione 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

Campo	Valore
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	RSA with SHA-256 EC-DSA with SHA-256
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> <ECDSA public key of 521bits>
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
Validity	<10 years>
SubjectDistinguishedName	CN=Time-Stamping Authority TSU1, O=Intesi S.p.A., OrganizationIdentifier=VATIT-02780480964, C=IT
SubjectPublicKeyInfo	<RSA public key of 3072 bits> <ECDSA public key of 256 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 PolicyOID = 1.3.76.16.6 (agidCert) 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>

Campo	Valore
IssuerAlternativeName	<not included>
Subject directory attributes	<not included>

7.1.5 Certificato Utente per Firma Elettronica Qualificata

Campo	Valore
Version Number	V3 (2)
Signature	RSA with SHA-256 EC-DSA with SHA-256
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 3072 bits> <ECDSA public key of 256 bits>
Signature Value	<Root CA signature>
Estensione 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 = 0.4.0.194112.1.2 (QCP-n-qscd) • PolicyOID = 1.3.76.16.6 (agidCert) • 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 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 Utente per il Sigillo Elettronico Qualificato

Campo	Valore
Version Number	V3 (2)
Signature	RSA with SHA-256 EC-DSA with SHA-256

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 3072 bits> <ECDSA public key of 256 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 = 1.3.76.16.6 (agidCert) • 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)
	ETSI retention period esi4-qcStatement-3 (0.4.0.1862.1.3) QcEuRetentionPeriod: 20
	ETSI QCS SSCD

Campo	Valore
	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>

7.1.7 OCSP Certificate for Qualified Electronic Signature

Campo	Valore
Version Number	V3 (2)
Signature	RSA with SHA-256 EC-DSA with SHA-256
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	CN=OCSP, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., C=IT
SubjectPublicKeyInfo	<RSA public key of 3072 bits> <ECDSA public key of 256 bits>
Signature Value	<Root CA signature>

Estensione del certificato	Valore
Authority Key Identifier (AKI)	<included>
Subject Key Identifier (SKI)	<included>
KeyUsage	Critical: Digital Signature
ExtendedKeyUsage	Not Critical: OCSP Signer
CertificatePolicies	<not included>
CRLDistributionPoints (CDP)	<not included>
Authority Information Access (AIA)	<not included>
QCStatement	<not included>
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>

7.1.8 OCSP Certificate for Qualified Electronic Seal

Campo	Valore
Version Number	V3 (2)
Signature	RSA with SHA-256 EC-DSA with SHA-256
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	CN=OCSP, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., C=IT
SubjectPublicKeyInfo	<RSA public key of 3072 bits> <ECDSA public key of 256 bits>
Signature Value	<Root CA signature>
Estensione del certificato	**Valore**
Authority Key Identifier (AKI)	<included>
Subject Key Identifier (SKI)	<included>
KeyUsage	Critical: Digital Signature
ExtendedKeyUsage	Not Critical: OCSP Signer
CertificatePolicies	<not included>
CRLDistributionPoints (CDP)	<not included>
Authority Information Access (AIA)	<not included>
QCStatement	<not included>
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).

7.2.1 Parametri emissione CRL

Campo	Valore
Periodo emissione CRL	6 ore
Durata CRL	24 ore
CRL Grace Period	600 secondi

7.2.2 CRL per il certificato di Marcatura Temporale

Campo	Valore
Version Number	V2
CRL Number	<included>
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
Signature	RSA with SHA-256 EC-DSA with SHA-256
thisUpdate	<included>
nextUpdate	<included>
Estensioni	**Valore**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
expireCertsOnCrl	<Same as the notBefore date of the CA certificate>
Revoked Certificate List Entries	
Certificate Serial Number	<included>
Revocation Date	<included>
Revocation Reason Code	<included when reason code different from unspecified>

7.2.3 CRL per il certificato di Firma Elettronica Qualificata

Campo	Valore
Version Number	V2
CRL Number	<included>
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Signature CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., 2.5.4.97=VATIT-02780480964, C=IT
Signature	RSA with SHA-256 EC-DSA with SHA-256
thisUpdate	<included>
nextUpdate	<included>
Estensioni	**Valore**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
expireCertsOnCrl	<Same as the notBefore date of the CA certificate>
Revoked Certificate List Entries	
Certificate Serial Number	<included>
Revocation Date	<included>
Revocation Reason Code	<included when reason code different from unspecified>

7.2.4 CRL per il certificato di Sigillo Elettronico Qualificato

Campo	Valore
Version Number	V2
CRL Number	<included>
IssuerDistinguishedName	CN=Intesi Group EU Qualified Electronic Seal CA G2, OU=Qualified Trust Service Provider, O=Intesi Group S.p.A., 2.5.4.97=VATIT-02780480964, C=IT
Signature	RSA with SHA-256 EC-DSA with SHA-256
thisUpdate	<included>

Campo	Valore
nextUpdate	<included>
Estensioni	**Valore**
Authority Key Identifier (AKI)	<Same value as the CA SKI extension>
expireCertsOnCrl	<Same as the notBefore date of the CA certificate>
Revoked Certificate List Entries	
Certificate Serial Number	<included>
Revocation Date	<included>
Revocation Reason Code	<included when reason code different from unspecified>

7.3 Profilo Timestsamp

Version		V1
Policy		0.4.0.2023.1.1
MessageImprint	hashAlgorithm	2.16.840.1.101.3.4.2.1 (sha-256) or upper
	hashedMessage	<included>
SerialNumber		<included>
accuracy		1 second
genTime		<included>
qcStatement		"esi4-qtstStatement1

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 direttiva europea eIDAS2 ed ai corrispondenti standards ETSI per i servizi fiduciari.

Intesi Group è sottoposta annualmente ad audit esterni eseguiti per certificare la conformità al regolamento eIDAS2.

Gli audit sono svolti ai sensi del regolamento eIDAS2, dello standard ETSI EN 319 401 e alle norme ETSI relative ai servizi fiduciari forniti. Gli audit hanno come obiettivo la dimostrazione della conformità delle procedure adottate alle policy ed ai processi QTSP documentati e l'applicazione dei criteri di sicurezza. L'audit viene eseguito da un Conformity Assessment Body (CAB) accreditato e presente nell'elenco pubblicato e mantenuto dalla Commissione europea.

Intesi Group svolge anche audit interni con cui vengono svolti controlli di verifica della corretta attuazione delle policy di certificazione, controlli approfonditi sulle policy di gestione delle chiavi, controlli di sicurezza, verifica sui profili dei certificati e in generale sulle attività eseguite nell'ambito QTSP.

Intesi Group effettua ispezioni periodiche e audit di qualsiasi struttura delle LRA per verificare che stiano operando in conformità alle policy e alle procedure di sicurezza definite nel presente TSPPS, nei documenti interni e nel contratto.

Intesi Group è un Qualified Trust Service Provider (QTSP); pertanto, Intesi Group opera sotto la supervisione di AgID (https://www.agid.gov.it) in qualità di National Supervisory Body. 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 eIDAS2.

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.

8.1 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 eIDAS2.

8.2 Relazioni tra il QTSP e gli ispettori

Tra il QTSP 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.

8.3 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 eIDAS2.

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

8.4 Misure adottate in seguito a non conformità

In caso di non conformità, AgID richiederà al QTSP 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.

8.5 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 eIDAS2, 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 è 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 sono pubblicate sul sito web di Intesi Group all'indirizzo store.intesigroup.com. Le modifiche alle tariffe applicabili ai Contratti in essere saranno comunicate ed entreranno in vigore in conformità a quanto previsto dalla Sezione 10 delle Condizioni Generali del Contratto per il Servizio di Certificazione.

Condizioni differenti potranno essere negoziate caso per caso, in funzione dei volumi richiesti.

9.2 Responsabilità finanziaria

Intesi Group ha stipulato le seguenti assicurazioni:

- 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:

- le liste dei certificati sospesi o revocati (CRL);
- le informazioni sullo stato dei certificati erogate on-line dal QTSP (es. via OCSP);

9.3.3 Responsabilità di protezione delle informazioni confidenziali

Il QTSP 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 dal QTSP 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_policy/

9.5 Diritti di proprietà intellettuale

All'interno del servizio regolato dal presente TSPPS, il QTSP 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

Il QTSP 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.

Intesi Group assicura una disponibilità dei servizi descritti nel presente TSPPS pari ad almeno il 99,8%, misurata separatamente per ciascun servizio su base trimestrale, con erogazione prevista 24 ore al giorno, 7 giorni alla settimana.

La disponibilità è calcolata come rapporto percentuale tra il tempo di effettiva disponibilità del servizio e il tempo totale del trimestre solare di riferimento. Le indisponibilità sono rilevate mediante i sistemi di monitoraggio aziendali.

Il medesimo livello di disponibilità si applica ai repository delle informazioni pubbliche e ai servizi di consultazione dello 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 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 capitolo 5 del documento "Condizioni Generali di contratto del servizio di certificazione" pubblicato sul sito istituzionale Intesi Group.

9.6.4 Utilizzatori

Fare riferimento al capitolo 7 del documento "Condizioni Generali di contratto del servizio di certificazione" pubblicato sul sito istituzionale Intesi Group.

9.6.5 Timestamp Authority

Per gli obblighi degli utilizzatori e delle terze parti far riferimento al documento “Condizioni Generali di contratto del servizio di marcatura temporale” pubblicato sul sito istituzionale Intesi Group.

9.6.6 Fornitori esterni

Intesi Group mantiene la responsabilità complessiva della conformità dei propri servizi fiduciari alle politiche e ai requisiti di sicurezza applicabili, comprese le attività svolte da fornitori esterni.

I rapporti con i fornitori che supportano i servizi fiduciari qualificati sono disciplinati da accordi scritti che definiscono le attività affidate, le responsabilità, i requisiti applicabili e i livelli di servizio, in misura proporzionata ai rischi associati.

Quando un fornitore tratta dati personali per conto di Intesi Group, il rapporto è disciplinato da un accordo conforme all’articolo 28 del GDPR.

9.7 Esclusione delle garanzie

Ad eccezione di quando espressamente menzionato altrove nel TSPPS 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 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 8.4 e 8.5.

9.10 Durata e Terminazione

Il presente TSPPS è pubblicato sul sito web del QTSP (si veda il Capitolo 2) e sul sito web di AgID e rimane in vigore fino alla sua sostituzione con una nuova versione. La data di entrata in vigore delle modifiche che incidono sui Contratti in essere è soggetta alle modalità di notifica e accettazione descritte nella Sezione 9.11.

9.11 Emendamenti

Intesi Group si riserva il diritto di modificare il presente TSPPS.

Le modifiche sostanziali, ossia quelle che possono incidere sulle condizioni di utilizzo o sull'accettazione del servizio da parte dei titolari, dei sottoscrittori o delle relying parties, sono comunicate prima della loro entrata in vigore, nel rispetto dei termini e delle modalità previsti dalla Sezione 10, «Notifiche e modifiche contrattuali», delle Condizioni Generali del Contratto per il Servizio di Certificazione. Rientrano, a titolo esemplificativo, le modifiche alle modalità di identificazione, ai servizi di sospensione e revoca, alle policy dei certificati e alle condizioni economiche applicabili.

Per i servizi erogati nell'ambito di accordi con clienti che gestiscono il rapporto con i propri utenti, Intesi Group trasmette la comunicazione ai referenti designati dal cliente. Il cliente provvede a informare tempestivamente gli utenti interessati, secondo quanto previsto dagli accordi contrattuali e in tempo utile rispetto alla decorrenza delle modifiche.

Per gli utenti che intrattengono un rapporto diretto con Intesi Group, le comunicazioni sono effettuate secondo le modalità previste dalla Sezione 10 delle medesime Condizioni Generali.

Le modifiche esclusivamente editoriali, le correzioni di refusi e gli aggiornamenti dei riferimenti che non incidono sui diritti, sugli obblighi, sulla sicurezza o sulle condizioni di utilizzo del servizio possono essere pubblicati senza una comunicazione individuale, fatti salvi gli obblighi contrattuali applicabili.

Ogni nuova versione del TSPPS è pubblicata nel repository documentale di Intesi Group, con indicazione della versione, della data e delle modifiche apportate. Gli utenti sono tenuti a consultare periodicamente il repository per verificare eventuali aggiornamenti. Tale consultazione non sostituisce gli obblighi di comunicazione previsti per le modifiche sostanziali.

9.12 Risoluzione Dispute

I sottoscrittori e i richiedenti i certificati sono invitati a fare riferimento al Capitolo 11 delle "Condizioni Generali di contratto del servizio di certificazione" e/o alle "Condizioni Generali di contratto del servizio di marcatura temporale", pubblicate sul sito istituzionale di Intesi Group.

Tutte i clienti o le terze parti possono presentare reclami o inviare segnalazioni scrivendo una e-mail, preferibilmente PEC, all'indirizzo, tsp@ig-trustmail.com.

L'e-mail dovrà contenere i dati identificativi del mittente (nome, cognome, indirizzo e codice fiscale o partita IVA) e una descrizione dettagliata delle motivazioni alla base del reclamo o della segnalazione.

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.