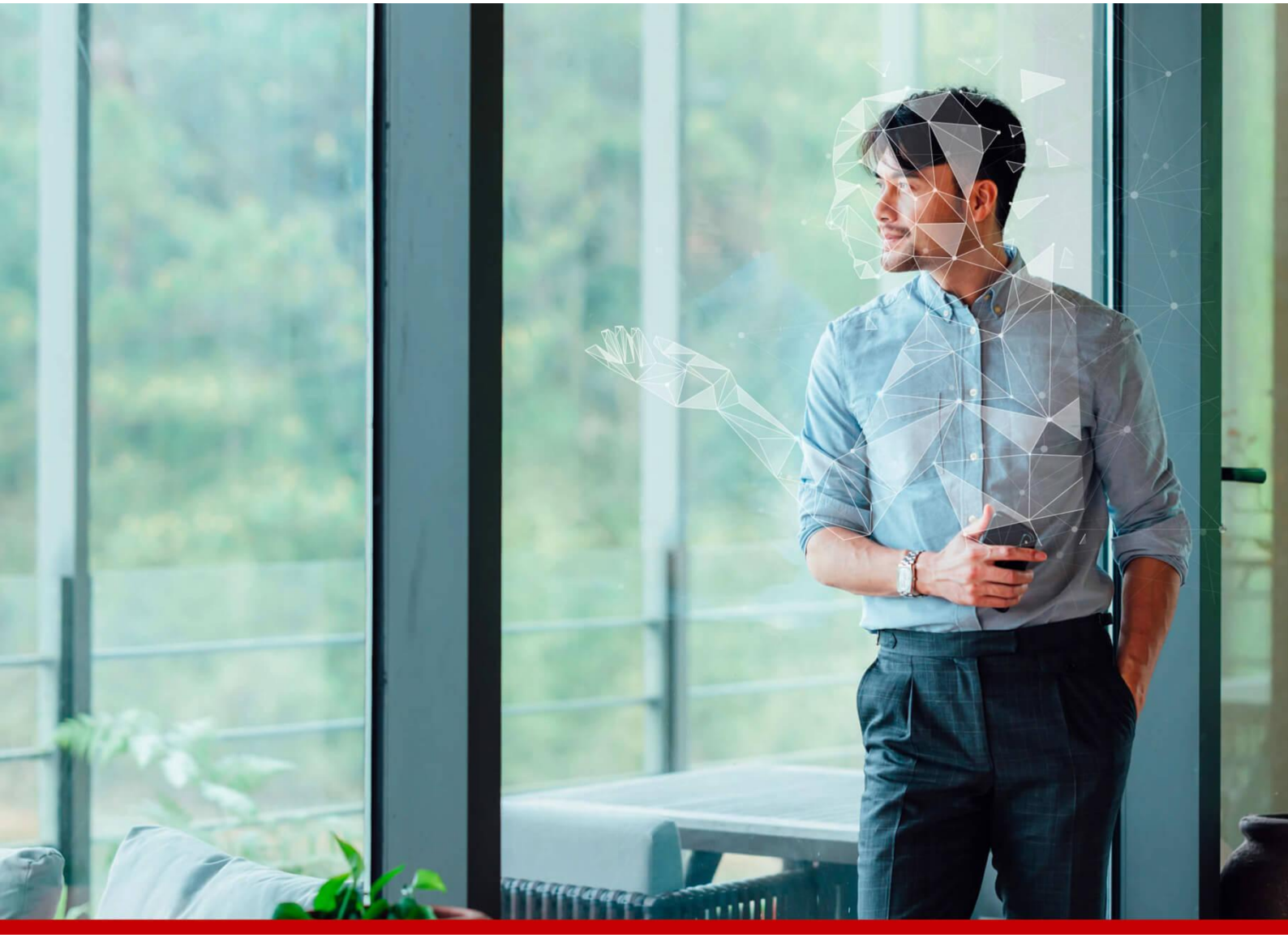


Manuale Operativo

CERTIFICATE PRACTICE STATEMENT /
CERTIFICATE POLICY

RELEASE 1.0 – 19-03-2026

INDICE

INFORMAZIONI GENERALI 8

Controllo documentale 8

Controllo delle versioni 8

1. INTRODUZIONE 9

1.1. Presentazione 9

1.2. Nome e identificativo del documento 10

1.2.1. OID (Object Identifier) 10

1.3. Partecipanti ai servizi di certificazione 12

1.3.1. Prestatore Qualificato di Servizi Fiduciari (Qualified Trust Service Provider - QTSP) 12

1.3.2. Uffici di Registrazione (Registration Authorities – R.A.) 14

1.3.3. Utenti finali 15

1.3.3.1. Richiedenti 15

1.3.3.2. Titolare del certificato 16

1.3.3.3. Relying parties (R.P.) 16

1.3.4. Terzo interessato 17

1.3.5. Autorità 17

1.3.5.1. Agenzia per l'Italia Digitale - AgID 17

1.3.5.2. Organismo di valutazione della conformità (CAB) 17

1.4. Utilizzo dei certificati 17

1.4.1. Uso previsto dei certificati 17

1.4.1.1. Certificato qualificato di sottoscrizione 18

1.4.1.2. Certificato qualificato di sottoscrizione "One-Shot" 19

1.4.1.3. Certificato qualificato di sigillo elettronico 19

1.4.1.4. Certificato qualificato di Time Stamping Unit 20

1.4.2. Limiti e divieti nell'utilizzo dei certificati 20

1.5. Amministrazione del Manuale Operativo 21

1.5.1. Organizzazione responsabile 21

1.5.2. Procedura di approvazione e gestione 21

1.6. Definizioni e acronimi 21

2. PUBBLICAZIONE DELLE INFORMAZIONI E REPOSITORY 26

2.1. Repository ... 26
2.2. Elenco delle informazioni pubblicate dalla CA ... 26
2.3. Frequenza delle pubblicazioni ... 26
2.4. Controllo degli accessi ... 27
3. IDENTIFICAZIONE E AUTENTICAZIONE ... 28
3.1. Nomi ... 28
3.1.1. Tipologia dei nomi ... 28
3.1.2. Significato dei nomi ... 29
3.1.3. Impiego di dati anonimi e pseudonimi ... 29
3.1.4. Regole di interpretazione dei nomi ... 30
3.1.5. Unicità dei nomi ... 30
3.1.6. Eventuali limitazioni d'uso ... 31
3.1.7. Soluzione dei conflitti relativi ai nominativi ... 31
3.2. Verifica iniziale dell'identità ... 31
3.2.1. Modalità di Identificazione per Persone Fisiche ... 32
3.2.2. Prova del possesso della chiave privata ... 34
3.2.3. Verifica dell'identità di una persona fisica ... 35
3.2.3.1. Procedura di identificazione De Visu ... 35
3.2.3.2. Procedura di identificazione da remoto ... 38
3.2.3.3. Procedura di identificazione tramite AML (Anti-money Laundering) ... 39
3.2.3.4. Procedura di identificazione tramite CIE ... 40
3.2.3.5. Procedura di identificazione tramite firma digitale rilasciata da altro QTSP ... 41
3.2.3.6. Procedura di identificazione tramite identità digitale SPID ... 41
3.2.3.7. Rafforzamento dell'identificazione - Adeguamento ai requisiti eIDAS 2 ... 42
3.2.4. Verifica dell'identità di una persona giuridica ... 43
3.2.5. Misure anticontraffazione ... 43
3.2.6. Informazioni non verificate ... 44
3.2.7. Autorizzazione di un Ufficio di Registrazione e dei suoi Operatori ... 44
3.3. Identificazione e autenticazione per le richieste di rinnovo ... 44
3.3.1. Rinnovo periodico dei certificati ... 44
3.3.2. Richieste di rinnovo dopo la revoca ... 45
3.4. Identificazione e autenticazione per le richieste di revoca ... 45
4. REQUISITI OPERATIVI RELATIVI AL CICLO DI VITA DEI CERTIFICATI ... 46
4.1. Domanda di emissione del certificato ... 46
4.1.1. Legittimazione della richiesta ... 46
4.1.2. Procedure e responsabilità ... 46

4.2. Elaborazione della richiesta 46
4.2.1. Svolgimento delle funzioni di identificazione ed autenticazione 46
4.2.2. Approvazione o rifiuto della richiesta 46
4.2.3. Termine per l'elaborazione della richiesta 47
4.3. Emissione del certificato 47
4.3.1. Processo e modalità di emissione 47
4.3.1.1. Emissione del certificato su Smartcard/Token 48
4.3.1.2. Emissione del certificato dispositivo HSM (firma remota) 48
4.3.1.2.1. Componenti del servizio SSAS (firma remota) 49
4.3.2. Emissione del certificato di TSU 49
4.3.3. Notifica di emissione del certificato 50
4.4. Consegna e accettazione del certificato 50
4.4.1. Responsabilità della R.A. 50
4.4.2. Processo di accettazione del certificato 51
4.4.3. Notifica dell'emissione a terzi 51
4.5. Uso della coppia di chiavi e del certificato 51
4.5.1. Utilizzo da parte del Richiedente e/o Titolare 51
4.5.2. Utilizzo da parte delle Relying Parties 52
4.5.2.1. Obblighi delle Relying Parties 52
4.5.2.2. Responsabilità civile delle Relying Parties 53
4.5.3. Limiti d'uso e di valore 53
4.6. Rinnovo di chiavi e certificati 54
4.6.1. Cause di rinnovo di chiavi e certificati 54
4.6.2. Procedura di rinnovo 55
4.7. Key Changeover (re-key dei certificati) 55
4.8. Modifica dei certificati 55
4.9. Revoca e sospensione di un certificato 55
4.9.1. Ipotesi di revoca di un certificato 56
4.9.2. Chi può richiedere la revoca 57
4.9.3. Procedura di revoca 57
4.9.4. Periodo di grazia della richiesta di revoca 58
4.9.5. Durata dell'elaborazione della richiesta di revoca 58
4.9.6. Verifica delle informazioni relative alla revoca dei certificati 58
4.9.7. Frequenza di emissione della CRL 59
4.9.8. Pubblicazione delle CRL 59
4.9.9. Disponibilità dei servizi di verifica on-line della revoca 59
4.9.10. Altre forme disponibili di pubblicazione della revoca 59

4.9.11. Condizioni speciali in caso di compromissione/corruzione della chiave privata .. 59
4.9.12. Circostanze per la sospensione 59
4.9.13. Chi può richiedere la sospensione 60
4.9.14. Procedura per la sospensione 60
4.10. Servizi informativi sullo stato del certificato 60
4.11. Cessazione del contratto 61
4.12. Key escrow e recupero della chiave privata 61
4.12.1. Politica e servizi di deposito e recupero delle chiavi 61
4.12.2. Politica e servizi sui contenuti e recupero chiavi di sessione 61
5. MISURE DI SICUREZZA FISICA E OPERATIVA 62
5.1. Sicurezza fisica 62
5.1.1. Localizzazione e implementazione delle strutture 62
5.1.2. Accesso fisico 63
5.1.3. Elettricità ed aria condizionata 63
5.1.4. Esposizione all'acqua 64
5.1.5. Prevenzione e protezione antincendio 64
5.1.6. Dispositivi di archiviazione 64
5.1.7. Smaltimento dei rifiuti 64
5.1.8. Copia di riserva esterna alle strutture 64
5.2. Controlli sulle procedure e sicurezza operativa 64
5.2.1. Ruoli di fiducia 64
5.2.2. Numero di persone per attività 66
5.2.3. Identificazione e autenticazione per i diversi ruoli 66
5.2.4. Mansioni che richiedono separazione di compiti 66
5.2.5. Sistema di gestione PKI 66
5.3. Sicurezza del personale 67
5.3.1. Qualifica, esperienza ed autorizzazioni richieste 67
5.3.2. Procedure di verifica delle informazioni relative al personale 67
5.3.3. Requisiti di formazione 68
5.3.4. Requisiti e frequenza dei corsi di aggiornamento 68
5.3.5. Rotazione delle mansioni 68
5.3.6. Sanzioni per azioni non autorizzate 68
5.3.7. Requisiti di assunzione di personale qualificato 68
5.3.8. Somministrazione della documentazione al personale 69
5.4. Procedure di controllo per la sicurezza 69
5.4.1. Tipi di eventi registrati 69

5.4.2. Frequenza di elaborazione del giornale di controllo 70
5.4.3. Periodo di conservazione del giornale di controllo 70
5.4.4. Protezione dei registri di verifica 71
5.4.5. Procedure di backup 71
5.4.6. Sistema di memorizzazione del giornale di controllo 71
5.4.7. Notifica in caso di evento sospetto 71
5.4.8. Analisi di vulnerabilità 71
5.5. Archiviazione delle informazioni 72
5.5.1. Tipologie di documenti archiviati 72
5.5.2. Periodo di archiviazione dei registri 73
5.5.3. Protezione degli archivi 73
5.5.4. Procedure di back-up 73
5.5.5. Requisiti della marcatura temporale 73
5.5.6. Localizzazione del sistema di archiviazione 73
5.5.7. Procedure per ottenere e verificare le informazioni di archiviazione 73
5.6. Rinnovo delle chiavi 74
5.7. Compromissione delle chiavi e disaster recovery 74
5.7.1. Procedure di gestione degli incidenti e delle compromissioni 74
5.7.2. Corruzione di risorse, applicazioni o dati 74
5.7.3. Compromissione della chiave privata della CA 74
5.7.4. Continuità operativa dopo una criticità 75
5.8. Cessazione del servizio 75
6. MISURE DI SICUREZZA TECNICA 77
6.1. Generazione e installazione della coppia di chiavi 77
6.1.1. Generazione della coppia di chiavi 77
6.1.1.1. Chiavi della CA 77
6.1.1.2. Chiavi dei Titolari 78
6.1.1.3. Chiavi di TSU 78
6.1.2. Consegna della chiave privata al Titolare 78
6.1.3. Distribuzione della chiave pubblica della CA 79
6.1.4. Dimensioni delle chiavi 79
6.1.5. Generazione dei parametri della chiave pubblica 79
6.1.6. Controllo di qualità dei parametri della chiave pubblica 79
6.1.7. Generazione delle chiavi in applicazioni informatiche o in beni strumentali 79
6.1.8. Scopo delle chiavi 79
6.2. Protezione delle chiavi private e sicurezza moduli 80
6.2.1. Standard e sicurezza dei moduli crittografici 80

6.2.2. Controllo da parte di più di una persona (n di m) sulla chiave privata 80
6.2.3. Ripristino della chiave privata 80
6.2.4. Backup della chiave privata 80
6.2.5. Archivio della chiave privata 80
6.2.6. Trasferimento della chiave privata tra moduli crittografici 81
6.2.7. Memorizzazione della chiave privata sul modulo crittografico 81
6.2.8. Modalità di attivazione della chiave privata 81
6.2.9. Modalità di distruzione della chiave privata 81
6.2.10. Modalità di disattivazione della chiave privata 81
6.2.11. Classificazione dei moduli crittografici 81
6.3. Altri aspetti della gestione della coppia di chiavi 81
6.3.1. Archiviazione della chiave pubblica 81
6.3.2. Periodi di utilizzo delle chiavi pubbliche e private 82
6.4. Dati di attivazione 82
6.4.1. Generazione dei dati di attivazione 82
6.4.2. Protezione dei dati di attivazione 82
6.5. Controlli di sicurezza informatica 82
6.5.1. Requisiti tecnici specifici per la sicurezza informatica 83
6.5.2. Valutazione del livello di sicurezza informatica 83
6.6. Controlli tecnici del ciclo di vita 83
6.6.1. Controlli di sviluppo dei sistemi 83
6.6.2. Controlli di gestione della sicurezza 83
6.7. Controlli di sicurezza della rete 84
6.8. Controlli ingegneristici dei moduli crittografici 84
6.9. Riferimento temporale 84
6.10. Cambiamento di stato di un Dispositivo Sicuro di Creazione di Firma o Sigillo Elettronico (QSCD) 84
7. PROFILO DEI CERTIFICATI, CRL, OCSP 86
7.1. Profilo dei certificati 86
7.1.1. Numero di versione ed estensioni del certificato 86
7.1.2. Identificatori degli algoritmi 86
7.1.3. Forme dei nomi 86
7.1.4. OID (Object Identifier) 86
7.2. Profilo delle CRL 86
7.2.1. Numero di versione 87
7.3. Profilo OCSP 87

8. AUDIT DI CONFORMITÀ 88
8.1. Frequenza degli audit 88
8.2. Identità e qualificazione degli auditor 88
8.3. Relazione tra la CA e gli auditor 88
8.4. Elementi soggetti a verifica 88
8.5. Azioni successive alle non-conformità 89
8.6. Comunicazione dei risultati 89
9. CONDIZIONI ECONOMICHE E LEGALI 90
9.1. Tariffe 90
9.1.1. Tariffe per l'emissione o rinnovo del certificato 90
9.1.2. Tariffa per l'accesso ai certificati 90
9.1.3. Tariffa per l'accesso alle informazioni di stato dei certificati 90
9.1.4. Tariffa per altri servizi 90
9.1.5. Politica per il rimborso – Recesso 91
9.2. Capacità finanziaria 91
9.2.1. Copertura assicurativa 91
9.2.2. Altri asset 92
9.2.3. Copertura assicurativa per gli utenti finali 92
9.3. Tutela delle informazioni trattate 92
9.3.1. Informazioni confidenziali 92
9.3.2. Informazioni non confidenziali 92
9.3.3. Ipotesi di divulgazione delle informazioni 93
9.4. Trattamento e protezione dei dati personali 93
9.4.1. Informativa sulla Privacy 93
9.4.2. Emissione dei Certificati di CNS 94
9.5. Diritti di proprietà intellettuale 94
9.5.1. Proprietà dei certificati 94
9.5.2. Proprietà del Manuale Operativo – Servizi di Certificazione digitale 94
9.5.3. Proprietà dei marchi 94
9.6. Obblighi, Garanzie e responsabilità 95
9.6.1. Garanzie offerte da Bit4id 95
9.6.2. Esclusione di garanzie 96
9.6.3. Limitazioni di responsabilità 96
9.6.4. Erogazione del Servizio e Assistenza 97
9.6.5. Indennizzi a favore di Bit4id 97
9.6.6. Indennizzi ai contraenti 97

9.6.7. Durata e risoluzione del contratto 98
9.6.8. Cessione del contratto 98
9.6.9. Legge applicabile 98
9.6.10. Foro competente 98
9.7. Disposizioni finali 98
9.7.1. Modifiche al presente accordo 98
9.7.2. Intero accordo 99
9.7.3. Forza maggiore 99

INFORMAZIONI GENERALI

Controllo documentale

Livello di sicurezza:	Pubblico
Ente di Emissione:	Bit4id s.r.l.
Versione:	1.0
Data ultima edizione:	19/03/2026
Codice Documento:	Manuale_Operativo_Trust_Services_v.1.0_IT

Controllo delle versioni

Versione	Parti modificate	Descrizione delle modifiche	Data
1.0	Originale	Prima versione del documento	19/03/2026

1. INTRODUZIONE

1.1. Presentazione

Il presente documento pubblico, "*Manuale Operativo*" o anche "*Certification Practice Statement*" (CPS), descrive le procedure operative seguite da Bit4id s.r.l. (di seguito anche solo "Bit4id") - società con sede in Napoli alla Via Diocleziano n. 107 - nell'erogazione dei seguenti Servizi Fiduciari:

- emissione di certificati di firma elettronica qualificata a persone fisiche;
- emissione di certificati di sigilli elettronici qualificati a persone giuridiche;
- servizio di marcatura temporale.

Nell'ambito dei servizi di certificazione descritti nel presente Manuale Operativo, Bit4id eroga anche un servizio di firma remota basato su componente applicativa server e su dispositivo di creazione della firma/sigillo in ambiente remoto. Il servizio è progettato e gestito in modo da garantire che l'uso della chiave privata avvenga sotto il controllo esclusivo del Titolare, mediante una combinazione di un Signature Activation Module (SAM) certificato e un HSM certificato, che ospita e protegge le chiavi private impedendone l'esportazione. Le misure organizzative e tecniche a presidio del servizio sono descritte nei paragrafi dedicati alla firma remota e alla sicurezza tecnica.
I certificati emessi in conformità al presente Manuale sono i seguenti:

- **Certificato qualificato di sottoscrizione:**
  - Certificato qualificato di sottoscrizione su smart card o token;
  - Certificato qualificato di sottoscrizione su HSM (firma remota);
  - Certificato qualificato di sottoscrizione di tipo automatico;
  - Certificato qualificato di sottoscrizione di tipo one-shot.
- **Certificato qualificato di sigillo elettronico:**
  - Certificato qualificato di sigillo elettronico su smartcard o token;
  - Certificato qualificato di sigillo elettronico su HSM.
- **Certificato di Time Stamping Unit:**
  - Certificato di Time Stamping Unit per l'emissione di marche temporali qualificate.

I Servizi Fiduciari qualificati erogati da Bit4id soddisfano i requisiti del Regolamento EU N°910/2014 (eIDAS) e successive modificazioni introdotte dal Regolamento EU n. 1183/2024 (eIDAS2) e sono conformi agli 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 (1,2,3,4 e 5) : 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 119 461: Electronic Signatures and Trust Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects
- ETSI EN 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

Inoltre, Bit4id si conforma alle Linee Guida in materia di "*Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate*" di cui alla Determina n. 147 del 4 giugno 2019 emessa dall'Agenzia per l'Italia Digitale (AgID) che ha confermato il contenuto della sua precedente Determinazione n. 121/2019.
Il servizio di marcatura temporale qualificata è erogato nel rispetto della RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), che definisce il protocollo di richiesta e risposta utilizzato dalle Time Stamping Authority (TSA) per la generazione di marche temporali.
La struttura del presente Manuale si basa sulla specifica pubblica RFC 3647 "*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*".

1.2. Nome e identificativo del documento

Questo documento è il "*Manuale Operativo*" (o *Certification Practice Statement* / CPS) di Bit4id.
La versione vigente del presente Manuale è indicata nell'intestazione del documento e nella sezione "*Controllo delle versioni*".

1.2.1. OID (Object Identifier)

L'OID che identifica l'azienda Bit4id è 1.3.6.1.4.1.31898, mentre l'OID che identifica Bit4id come QTSP è **1.3.6.1.4.1.31898.10**

La gerarchia OID per i certificati end-entity segue una struttura a quattro sottolivelli, rispetto a quelli soprariportati:

1.3.6.1.4.1.31898.10.X.Y.Z.W

Dove:

X = Servizio

Y = Root

Z = Tipo di certificato

W = Tipo di dispositivo

Di seguito sono elencati gli OID ("*Object Identifier*") delle policy supportate da questo Manuale Operativo. Le Policy OID contraddistinguono ciascun profilo di certificato emesso da Bit4id e sono specificate all'interno di ciascun certificato nell'estensione Certificate Policy.

Bit4id ha stabilito i seguenti OID per i servizi qualificati offerti dal QTSP.

OID	Servizio
1.3.6.1.4.1.31898.10.1	**Servizio di emissione di certificati qualificati per firma digitale e sigillo elettronico**
1.3.6.1.4.1.31898.10.1.1.Z.W	Bit4id S.r.l. QTSP Qualified Certificates CA RSA 4096 G1
1.3.6.1.4.1.31898.10.1.2.Z.W	Bit4id S.r.l. QTSP Qualified Certificates CA ECC 256 G1
1.3.6.1.4.1.31898.10.1.3.Z.W	Bit4id S.r.l. QTSP Qualified One-Shot Certificates CA ECC 256 G1
1.3.6.1.4.1.31898.10.2	**Servizio di generazione di certificati per marche temporali qualificate**
1.3.6.1.4.1.31898.10.2.1.Z.W	Bit4id S.r.l. QTSP Qualified Time-Stamp CA RSA 4096 G1
1.3.6.1.4.1.31898.10.2.2.Z.W	Bit4id S.r.l. QTSP Qualified Time-Stamp CA ECC 256 G1

I certificati di autenticazione sono caratterizzati dagli OID 1.3.6.1.4.1.31898.10.3.1 e 1.3.6.1.4.1.31898.10.3.2 e sono descritti in un apposito manuale.

Ove applicabile da schema precedente, Z e W assumono i seguenti valori come da tabella:

Z	Tipo di certificato
.1	Certificati per OCSP Responder che forniscono informazioni sullo stato di revoca dei certificati.
.2	Certificati Time Stamping Unit
.3	Certificati qualificati di firma elettronica per persone fisiche
.4	Certificati qualificati per firma one-shot

.5	Certificati per firma automatica
.6	Certificati di Sigillo Elettronico

W	**Tipo di dispositivo**
.1	Qualified Signature Creation Device (QSCD) locale (es. smartcard, token USB)
.2	QSCD remoto (HSM)

OID aggiuntivi possono essere presenti nel certificato per indicare l'esistenza di limiti d'uso. Tali OID sono elencati nel paragrafo 4.5.3. La presenza dei limiti d'uso non modifica in alcun modo le regole stabilite nel resto del Manuale Operativo.

Nel caso di eventuali discrepanze tra il presente Manuale Operativo e l'ulteriore documentazione, contenente le condizioni di fornitura e/o le procedure relative ai servizi offerti da Bit4id, prevarrà quanto stabilito nel presente Manuale Operativo.

Bit4id si riserva di apportare modifiche al presente Manuale Operativo per esigenze tecniche o modifiche procedurali intervenute durante la gestione del servizio.

Al verificarsi di ogni variazione Bit4id notificherà ad AgID la versione aggiornata del Manuale Operativo che sarà pubblicata sul relativo sito web istituzionale.

Questo documento è anche pubblicato sul sito web di Bit4id al seguente indirizzo: https://www.bit4id.com/documentazione-qtsp.

1.3. Partecipanti ai servizi di certificazione

1.3.1. Prestatore Qualificato di Servizi Fiduciari (Qualified Trust Service Provider - QTSP)

Bit4id opera in qualità di Qualified Trust Service Provider (QTSP). I dati identificativi dell'Organizzazione sono i seguenti:

Ragione Sociale:	Bit4id s.r.l.
Partita IVA (IT):	04741241212
Sede legale	Via Diocleziano, 107 -80125 Napoli (Italia)
Tel:	+39 081/7625600

Email:	info@bit4id.com
Pec:	bit4id-tsp@sicurezzapostale.it

Bit4id eroga i seguenti servizi fiduciari:

a) rilascio e gestione dei certificati qualificati (firma elettronica qualificata e sigillo elettronico qualificato), in conformità alle disposizioni di cui al Regolamento (UE) n. 910/2014 (di seguito anche solo "*Regolamento eIDAS*"), alla normativa tecnica "ETSI" applicabile al rilascio e alla gestione dei certificati qualificati, con particolare riferimento allo standard "EN 319 411- 1" e "EN 319 411-2" nonché alla normativa Nazionale di riferimento (D.Lgs. 7 marzo 2005 n. 82 e s.m.i. – di seguito anche solo "Codice dell'Amministrazione Digitale" o "CAD").

b) rilascio di marche temporali qualificate, in conformità alle disposizioni di cui al Regolamento (UE) n. 910/2014 (più brevemente citato come "Regolamento eIDAS") e alla normativa tecnica "ETSI" applicabile al rilascio e alla gestione dei certificati qualificati, con particolare riferimento allo standard "EN 319 421";

In particolare, con riferimento ai certificati qualificati di firma elettronica qualificata di cui alla precedente lett. a) Bit4id può emettere anche tale tipologia di certificati in modalità "*One-Shot*" con durata e finalità limitate a specifici ambiti di applicazione e di utilizzo (v. Par. 1.4.1.2. infra).

Per la fornitura di servizi fiduciari qualificati, Bit4id si avvale dell'infrastruttura di Uanataca S.A. Unipersonal, società controllata da Bit4id s.r.l., nonché Prestatore di Servizi Fiduciari Qualificato in Spagna, i cui riferimenti sono riportati di seguito:

Ragione Sociale:	Uanataca Sociedad Anonima Unipersonal
Partita IVA (NIF):	A66721499
Sede legale	Avenida Meridiana, 350, 08027 Barcellona (Spagna)
Riferimento eIDAS	https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls/tl/ES/tsp/26

Bit4id, quale SSAS Provider (SSASP) nel contesto del presente Manuale, è responsabile della corretta gestione dei componenti SAM e HSM e delle misure di sicurezza e tracciabilità connesse al servizio di firma remota.

Bit4id, inoltre, opera in qualità di ente Certificatore per il rilascio dei certificati di Carta Nazionale dei Servizi (CNS), per conto dell'Ente Emettitore Università Parthenope, in conformità al Decreto interministeriale 9 dicembre 2004 e s.m.i. recante "*regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale dei Servizi*" e a tutta la relativa disciplina applicabile in ambito nazionale.

1.3.2. *Uffici di Registrazione (Registration Authorities – R.A.)*

Lo svolgimento delle attività di identificazione ed autenticazione dei Richiedenti (ovvero i soggetti che richiedono i certificati) può essere svolta sia dallo stesso personale della CA, sia da Uffici di Registrazione (RA - "*Registration Authorities*") di terze parti delegate da Bit4id, attraverso la stipula di appositi mandati.

Gli Uffici di Registrazione (RA) costituiscono, dunque, terze parti cui Bit4id affida, tramite mandati *ad hoc*, l'incarico per lo svolgimento delle attività di identificazione ed autenticazione dei soggetti che richiedono i certificati.

Gli Uffici di Registrazione nominati da Bit4id saranno adeguatamente formati e sottoposti a tutte le necessarie verifiche finalizzate alla verifica circa il regolare adempimento degli impegni e degli obblighi derivanti dal mandato.

In particolare, una RA può svolgere le seguenti attività:

- identificazione e autenticazione (I&A) del Richiedente;
- verifica dei requisiti necessari e dei dati identificativi di colui che figurerà come Titolare del certificato;
- registrazione dei dati del Richiedente;
- autorizzazione all'emissione di certificati digitali attraverso appositi strumenti messi a disposizione da Bit4id;
- trasmettere le richieste di revoca dei certificati alla CA;
- trasmettere le richieste di rinnovo dei certificati alla CA.

Nei casi in cui è previsto un accordo specifico tra la Certification Authority e la Registration Authority, quest'ultima ha l'onere di custodire la documentazione relativa:

a) all'identificazione del Richiedente;

b) alla registrazione del Richiedente;

c) alla gestione del ciclo di vita dei certificati.

Bit4id si impegna a formalizzare contrattualmente ogni tipo di rapporto intercorrente con i soggetti che agiranno per suo conto come Uffici di Registrazione.

La RA, a sua volta, potrà autorizzare uno o più soggetti ad agire come "Operatori di Registrazione" (RAO).

Gli Operatori di Registrazione della RA, previa stipula di un apposito accordo direttamente con la CA, potranno essere delegati a svolgere le attività di identificazione ed autenticazione dei Richiedenti direttamente per conto della CA.

È responsabilità della CA procedere alla definizione dei ruoli ed alla distribuzione dei compiti in capo agli Operatori di Registrazione.

È onere della RA nominata di fornire i nominativi degli eventuali incaricati nonché di tutto il personale impiegato nelle operazioni di identificazione in conformità al presente Manuale Operativo.
Affinché possano operare, i RAO devono partecipare alla formazione fornita dal certificatore.
L'abilitazione all'attività avviene esclusivamente dopo aver completato con successo il percorso formativo previsto.
Bit4id si riserva il diritto di non abilitare e/o di disabilitare uno o più Operatori di Registrazione che operino in maniera non conforme alle disposizioni del presente Manuale Operativo.
Le RA sono inoltre soggette a verifiche periodiche da parte di Bit4id con lo scopo di verificare il rispetto degli accordi sottoscritti con la CA e delle procedure definite nel presente documento.

1.3.3. Utenti finali

Gli utenti finali (di seguito anche solo "Utenti" o "Richiedenti") si identificano nelle persone fisiche o giuridiche destinatarie del servizio di emissione, gestione ed utilizzo dei certificati qualificati emessi da Bit4id.
In particolare, rientrano tra gli utenti finali, ai sensi del presente Manuale, le seguenti categorie:

1) **Richiedenti:** persone fisiche o giuridiche che domandano alla CA il rilascio di un certificato digitale (firma o sigillo elettronico);
2) **Titolari:** persone fisiche o giuridiche titolari del certificato qualificato, coincidono con i Richiedenti a seguito dell'emissione del certificato;
3) **Relying parties:** soggetti che ricevono un documento informatico sottoscritto con il certificato digitale del Titolare o a cui è apposta la marca temporale e che fanno affidamento sulla validità del certificato medesimo (e/o sulla firma/sigillo digitale ivi presente) per valutare la correttezza e la validità del documento stesso, nei contesti dove esso è utilizzato.

1.3.3.1. Richiedenti

Sono le persone fisiche o giuridiche che richiedono il rilascio di certificati digitali, rivolgendosi direttamente alla CA o ad una sua RA.
Il Richiedente, pertanto, può anche qualificarsi come "Cliente" della CA: questi, al momento della richiesta formale di certificato, dichiara di accettare le Condizioni Generali di contratto stabilite dalla CA e, pertanto, acconsente all'esercizio dei diritti e al rispetto degli obblighi dettati da quest'ultima.
Le condizioni contrattuali disposte dalla CA si aggiungono ed integrano i diritti e gli obblighi dei Richiedenti e/o Titolari sanciti nella normativa tecnica, di matrice europea, relativa all'emissione dei

certificati qualificati, con particolare riferimento allo standard "ETSI EN 319 411", sezioni 5.4.2 e 6.3.4.e.

A seguito dell'emissione del certificato, il Richiedente si identifica nel Titolare.

1.3.3.2. Titolare del certificato

Il Titolare del certificato è il soggetto che possiede ed utilizza la chiave privata relativa ad un certificato di firma o un certificato di sigillo elettronico corrispondente alla chiave pubblica contenuta nel certificato.

È evidente che il Titolare del certificato corrisponderà alla persona fisica che lo richiede in caso di certificato di firma, mentre corrisponderà alla persona giuridica (identificata attraverso la sua denominazione, il codice fiscale o la partita iva), nel caso di certificati di sigillo elettronico.

In caso di firma remota, il Titolare autorizza l'uso della chiave privata per la firma tramite attivazione su SAM (Signature Activation Module).

Il Titolare è identificato all'interno del certificato attraverso un "*Distinguished Name*" (DN), nel campo *Subject*, conforme allo standard ITU-T X.500.

Nel campo *Subject* sono inseriti i dati identificativi del Titolare del certificato, senza che sia possibile, in genere, l'utilizzo di pseudonimi.

La chiave privata di un Titolare, generata da Bit4id, non può essere recuperata o ricavata dalla CA una volta consegnata, in quanto i Titolari identificati nei rispettivi certificati sono gli unici responsabili della loro protezione.

Essi, pertanto, sono tenuti a tenere in debita considerazione le conseguenze derivanti dallo smarrimento della chiave privata indicate all'interno del presente Manuale.

1.3.3.3. Relying parties (R.P.)

Le Relying Parties (R.P.) si identificano nei soggetti che fanno affidamento sulle informazioni contenute nei certificati emessi da Bit4id.

In particolare, per quanto riguarda i servizi descritti nel presente Manuale, per R.P. si intendono:

- tutti i soggetti che verificano le firme elettroniche e/o i sigilli elettronici e/o le marche temporali apposte ai documenti informatici attraverso i certificati emessi secondo le modalità descritte nel presente Manuale.

Tutti coloro che devono fare affidamento sulle informazioni contenute nei certificati hanno l'obbligo, prima di accettare un certificato, di effettuare le necessarie verifiche, secondo quanto disposto nel presente Manuale Operativo.

1.3.4. Terzo interessato

Il Terzo Interessato coincide con la società o l'organizzazione a cui risulta collegato il Titolare, e viene identificato mediante il rappresentante legale che autorizza la CA ad inserire i dati dell'organizzazione all'interno del certificato del Titolare.

1.3.5. Autorità

1.3.5.1. Agenzia per l'Italia Digitale - AgID

L'Agenzia per l'Italia Digitale (AgID) è l'organismo che, ai sensi dell'articolo 17 del Regolamento eIDAS, svolge attività di vigilanza (*ex ante* ed *ex post*) sui Prestatori di servizi fiduciari qualificati stabiliti nel territorio italiano allo scopo di garantirne la rispondenza ai requisiti stabiliti dal Regolamento.

1.3.5.2. Organismo di valutazione della conformità (CAB)

L'organismo di valutazione della conformità (CAB, acronimo di Conformity Assessment Body) è un organismo accreditato, secondo quanto previsto dal Regolamento eIDAS, competente ad effettuare la valutazione della conformità del Prestatore di servizi fiduciari qualificati e dei servizi fiduciari qualificati da esso prestati alle normative e agli standard applicabili.

1.4. Utilizzo dei certificati

La presente sezione indica le possibili applicazioni di ciascuna tipologia di certificato emesso da Bit4id e i limiti caratterizzanti l'utilizzo di alcune tipologie di certificati.

1.4.1. Uso previsto dei certificati

I certificati emessi da Bit4id, secondo le modalità indicate dal presente Manuale Operativo, sono Certificati Qualificati ai sensi del CAD e del Regolamento eIDAS e rispettano le "*Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate*" di cui al regolamento pubblicato da AgID nella sua ultima versione.

Il certificato emesso dalla CA sarà usato per verificare la firma qualificata o il sigillo elettronico qualificato del Titolare cui il certificato appartiene o del Fruitore, nel caso di marca temporale.

Altri usi dei certificati non sono previsti e sono da evitarsi.

In particolare, è vietato l'utilizzo del certificato fuori dai limiti e dai contesti specificati nel presente Manuale Operativo, nella documentazione contrattuale e in violazione dei limiti d'uso e di valore (*key usage*, *extended key usage*, *user notice*) indicati nel certificato stesso.

Bit4id si riserva la facoltà di revocare i certificati qualora venga a conoscenza che questi siano utilizzati in modo improprio o contrario alle disposizioni del presente Manuale.

1.4.1.1. Certificato qualificato di sottoscrizione

Si tratta di certificati qualificati emessi per la firma elettronica qualificata che, sia in caso di emissione su Smartcard/Token (v. Par. 4.3.1.1. *infra*) sia in caso di emissione su HSM (v. Par. 4.3.1.2. infra) sono conformi alla politica di certificazione *QCP-n-qscd* con OID 0.4.0.194112.1.2, il quale viene dichiarato nei certificati.

Questi certificati (long term) sono contrassegnati dagli OID:

- in caso di emissione su smartcard/token
  - 1.3.6.1.4.1.31898.10.1.1.3.1
  - 1.3.6.1.4.1.31898.10.1.2.3.1
  - 1.3.6.1.4.1.31898.10.1.1.5.1
  - 1.3.6.1.4.1.31898.10.1.2.5.1
- in caso di emissione su HSM
  - 1.3.6.1.4.1.31898.10.1.1.3.2
  - 1.3.6.1.4.1.31898.10.1.2.3.2
  - 1.3.6.1.4.1.31898.10.1.1.5.2
  - 1.3.6.1.4.1.31898.10.1.2.5.2

Tali certificati, emessi in QSCD costituiscono certificati qualificati secondo quanto stabilito nell'art. 28 del Regolamento (UE) 910/2014 eIDAS.

Funzionano con dispositivi qualificati di creazione di firma (QSCD), nel rispetto degli articoli 29 e 51 del Regolamento (UE) 910/2014, e in accordo a quanto disposto dalla regolamentazione tecnica rilasciata dall'Istituto Europeo per gli Standard nelle Telecomunicazioni, identificata con il riferimento EN 319 411-2.

Inoltre, garantiscono l'identità del Titolare e consentono di generare una "*firma elettronica qualificata*", ossia una firma elettronica avanzata, basata su un certificato qualificato e generata impiegando un dispositivo qualificato, la quale è equiparata, per tutti gli effetti di legge, ad una firma autografa scritta senza che sia necessario la sussistenza di ulteriori requisiti.

Inoltre, il certificato in questione può essere utilizzato per quelle applicazioni che non richiedono una firma elettronica equivalente alla firma scritta, come ad esempio:

a) Firma di posta elettronica sicura;

b) Altre applicazioni di firma elettronica.

Il campo "*key usage*" consente di realizzare esclusivamente la funzione di "*Content commitment*" (Non ripudio).

1.4.1.2. Certificato qualificato di sottoscrizione "One-Shot"

Si tratta di un certificato qualificato di sottoscrizione emesso su dispositivo HSM (di firma remota) con un periodo di validità più limitato nel tempo, tipicamente non superiore a 60 giorni o come altrimenti concordato con il cliente / Terzo Interessato e, comunque, con una durata di utilizzo non superiore a 60 minuti decorrenti dall'emissione del certificato. Inoltre, il suo utilizzo è consentito mediante sistemi di autenticazione consentiti dalla normativa e solo nei modi e nei termini delle limitazioni di uso inserite nel certificato, stabilite da Bit4id ed accettate dal Titolare in fase di richiesta di emissione del certificato.

In questo caso l'OID della firma è 1.3.6.1.4.1.31898.10.1.3.4.2

In maniera congiunta all'apposizione della firma, viene inserita anche una marca temporale, per garantire un riferimento temporale certo secondo quanto previsto dalla normativa.

Per questa tipologia di certificato, non è prevista la revoca o la sospensione. È previsto uno specifico limite d'uso, da concordare con il cliente. Per i limiti d'uso si rimanda al paragrafo 4.5.3.

1.4.1.3. Certificato qualificato di sigillo elettronico

Questi certificati sono contrassegnato da rispettivamente dagli OID 1.3.6.1.4.1.31898.10.1.1.6.1 e 1.3.6.1.4.1.31898.10.1.2.6.1, per l'emissione su Smartcard/Token e da OID 1.3.6.1.4.1.31898.10.1.1.6.2 e 1.3.6.1.4.1.31898.10.1.2.6.2 per l'emissione su HSM (sigillo remoto).

Si tratta di certificati qualificati emessi per il sigillo elettronico qualificato, in conformità alla politica di certificazione QCP-l-qscd con OID 0.4.0.194112.1.3, il quale viene dichiarato nei certificati.

Tale certificato, emesso in "Qualified Seal Creation Device" (di seguito anche solo "QSealCD" o anche "QSCD", costituisce certificato qualificato ai sensi dell'art. 38 del Regolamento (UE) 910/2014 eIDAS: "Certificati Qualificati di Sigilli Elettronici".

Funzionano con dispositivi qualificati di creazione di firma e sigilli elettronici (QSCD), nel rispetto degli articoli 39 e 51 del Regolamento (UE) 910/2014, e in accordo a quanto disposto dalla regolamentazione tecnica rilasciata dall'Istituto Europeo per gli Standard nelle Telecomunicazioni, identificata con il riferimento EN 319 411-2.

Inoltre, garantisce la piena validità legale e riconducibilità ad una persona giuridica determinata (Titolare) e consente di generare un "sigillo elettronico qualificato", il quale è equiparato, a tutti gli effetti di legge, ad una sottoscrizione in forma scritta senza che sia necessaria la sussistenza di ulteriori requisiti.

Il sigillo elettronico qualificato, infatti, gode della presunzione di integrità dei dati e della correttezza delle origini di tali dati, cui è collegato il sigillo elettronico qualificato e fa piena prova circa il rilascio del documento da parte di una persona giuridica, garantendo la certezza dell'origine e dell'integrità del documento.

Il campo "key usage" consente di realizzare esclusivamente la funzione di Non ripudio.

1.4.1.4. Certificato qualificato di Time Stamping Unit

Questo certificato è contrassegnato dagli OID 1.3.6.1.4.1.31898.10.2.1.2.2 e 1.3.6.1.4.1.31898.10.2.2.2.2 e viene emesso in accordo con la politica di certificazione QCP-l-qscd recante l'OID 0.4.0.194112.1.3.

I certificati di Time Stamping Unit sono generati per emettere marche temporali.

La sincronizzazione del sistema di emissione di marche temporali di Bit4id si effettua attraverso il protocollo NTP.

1.4.2. Limiti e divieti nell'utilizzo dei certificati

I certificati emessi da Bit4id vengono impiegati per la funzione che gli è propria e per le finalità stabilite nel presente Manuale Operativo, essendo precluso un loro impiego per altre funzioni o altre finalità diverse rispetto a quelle per le quali sono stati rilasciati.

Allo stesso modo, i certificati emessi da Bit4id devono essere impiegati unicamente nel rispetto della normativa vigente.

I certificati rilasciati ad utenti finali non possono essere impiegati per firmare certificati di chiave pubblica di nessun tipo, né per firmare Liste di Revoca dei certificati (CRL).

Bit4id non sarà considerata in nessun caso responsabile per l'uso fatto dei certificati in relazione a situazioni critiche che comportino, a titolo esemplificativo, rischi specifici per l'incolumità delle persone, danni ambientali, rischi specifici in relazione a servizi di trasporto di massa, alla gestione di impianti nucleari e chimici e di dispositivi medici.

L'impiego dei certificati emessi da Bit4id in operazioni che contravvengono al presente Manuale Operativo, alle Condizioni Generali di Contratto, alla documentazione inerente a ciascuna tipologia di certificato, ai contratti tra la RA e i Richiedenti, costituisce un utilizzo indebito e contrario agli effetti di legge, esimendo, pertanto, Bit4id, da ogni responsabilità per ogni eventuale danno derivante da un utilizzo indebito dei certificati compiuto dal Titolare o da qualsiasi altra Parte.

Bit4id non assume, in nessun caso, alcuna responsabilità per le informazioni, i dati, i contenuti, immessi o trasmessi, associati all'utilizzo del certificato, essendo unicamente il Richiedente il soggetto responsabile dell'utilizzo del certificato e dei contenuti ad esso associati.

Parimenti, sarà imputabile al Richiedente ovvero al soggetto autorizzato alla custodia del certificato qualsiasi responsabilità che possa derivare dall'utilizzo del certificato al di fuori dei limiti e delle condizioni indicate nel presente Manuale Operativo, nelle Condizioni Generali di Contratto, nella documentazione inerente a ciascuna tipologia di certificato, nei contratti tra la RA e i Richiedenti, così come da qualsiasi altro utilizzo considerato indebito dalla normativa vigente in materia.

1.5. Amministrazione del Manuale Operativo

1.5.1. Organizzazione responsabile

Il presente documento CPS di Bit4id è aggiornato alla versione risultante dal "Controllo delle Versioni" o dal "Controllo Documentale" di cui alle "Informazioni Generali" del presente Manuale e viene redatto, pubblicato ed aggiornato da Bit4id e approvato dal Responsabile dei servizi di certificazione e validazione temporale.
I dati di contatto del TSP sono contenuti nel §1.3.1.

1.5.2. Procedura di approvazione e gestione

Bit4id esegue un controllo di conformità di questo Manuale Operativo al processo di erogazione del servizio di certificazione e alle condizioni associate al medesimo.
Il presente documento viene riesaminato (ed eventualmente aggiornato, se necessario) almeno con frequenza annuale.

In caso di modifiche maggiori al Manuale Operativo e/o alle procedure in esso indicate, Bit4id si sottoporrà alla valutazione del CAB prima di procedere alla pubblicazione.

1.6. Definizioni e acronimi

Di seguito una breve lista degli acronimi utilizzati; qualora, all'interno del Manuale, venga riscontrata la presenza di termini o acronimi non ricompresi nelle seguenti definizioni dovrà attribuirsi alle stesse il significato proprio secondo la normativa applicabile.

Termine/acronimo	Significato
AgID	Agenzia per l'Italia Digitale
CAB, "*Conformity Assessment Body*"	È l'organismo di certificazione accreditato che verifica la conformità dei servizi della CA.
CAD	Codice dell'Amministrazione Digitale (D.lgs. n.82/2005 e ss.mm.ii).
Certificato digitale	Documento elettronico attestante il legame tra dati di convalida della firma (chiave pubblica) e una persona fisica, giuridica o un dispositivo, verificato e firmato da un Qualified Trust Service Provider (QTSP), in conformità al Regolamento (UE) n. 910/2014 (eIDAS) e agli standard ETSI EN 319 411.
Certificato "*One-Shot*"	Certificato di Firma Qualificata con intervallo di validità limitato e intervallo di utilizzo di 60 minuti.

Certificatore, "Certification Authority" o "CA"	È l'ente, pubblico o privato, abilitato a rilasciare Certificati digitali tramite procedura di certificazione che segue standard internazionali e conforme alla normativa italiana ed europea in materia.
Chiave privata	È la chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave privata è associata ad una chiave pubblica, ed è solo in possesso dal Titolare che la utilizza per firmare digitalmente i documenti.
Chiave pubblica	È la chiave crittografica utilizzata in un sistema di crittografia asimmetrica; ogni chiave pubblica è associata ad una chiave privata, ed è utilizzata per verificare la firma digitale apposta su un documento informatico dal Titolare della chiave asimmetrica.
CIE	Carta d'Identità Elettronica.
CNS	Carta Nazionale dei Servizi.
CRL – Lista di revoca e sospensione dei Certificati	È una lista di Certificati che sono stati resi "non validi" dal Certificatore prima della loro naturale scadenza. La revoca rende i Certificati "non validi" definitivamente. La sospensione rende i Certificati "non validi" per un tempo determinato.
Dispositivo Sicuro per la Creazione della Firma	Un dispositivo per la creazione di una Firma elettronica che soddisfi i requisiti di cui all'allegato II di eIDAS.
eIDAS	Il Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
Ente Emettitore	Ente responsabile della formazione e del rilascio della Carta Nazionale dei Servizi, ai sensi del Decreto Interministeriale 9 dicembre 2004. Nell'ambito delle attività di rilascio dei certificati di CNS, rappresenta, quindi, la Pubblica Amministrazione, responsabile di tutto il circuito di emissione, garantendone in termini di sicurezza tutte le fasi del ciclo di vita.
ETSI	European Telecommunications Standards Institute.
Fruitore	Soggetto – persona fisica o giuridica – che utilizza il servizio di marcatura temporale messo a disposizione dal QTSP per associare una data e un'ora certe a uno o più documenti elettronici, ai fini della loro validazione temporale e opponibilità a terzi.

Giornale di controllo	Consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche di base.
GDPR	Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.
HSM	Hardware Security Module
Marca Temporale, "Timestamp"	È il riferimento temporale che consente la validazione temporale.
Manuale Operativo, "*Certification Practice Statement*" o "CPS"	È il documento pubblico depositato presso AgID che definisce le procedure applicate dal Certificatore nello svolgimento della propria attività.
Namirial Onboarding	Piattaforma di digital onboarding e identificazione remota, certificata ETSI TS 119 461, progettata da Namirial S.p.A. (società capogruppo, di cui Bit4id fa parte) per orchestrare in modo sicuro, conforme e flessibile l'intero processo di acquisizione e verifica dell'identità degli utenti finali.
OID, "*Object Identifier*"	È una sequenza di numeri, registrata secondo lo standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.
OCSP, "*Online Certificate Status Protocol*"	È un protocollo che consente di verificare la validità di un Certificato in tempo reale.
Organizzazione	È un gruppo organizzato di utenti (es. enti, aziende, società, ordini professionali, Associazioni, ecc.) che hanno stipulato accordi con il Certificatore per il rilascio di Certificati di firma digitale ai propri dipendenti e/o associati.
OTP	*One-Time-Password*. Codice numerico generato da un dispositivo fisico utilizzato per effettuare un'autenticazione a due fattori.
PIN [Personal Identification Number]	Codice associato ad un dispositivo sicuro di firma, utilizzato dal Titolare per accedere alle funzioni del dispositivo stesso
PUK	Codice personalizzato utilizzato dal Titolare per riattivare il proprio dispositivo in seguito al blocco dello stesso per errata digitazione del PIN.
QSCD	Dispositivo qualificato per la creazione della firma o del sigillo elettronico, progettato per garantire che i dati di creazione della firma (chiave privata) siano generati, gestiti e utilizzati sotto il controllo esclusivo del titolare, e protetti da compromissioni. È certificato secondo gli standard di sicurezza stabiliti dal Regolamento (UE) n. 910/2014 (eIDAS) e dagli schemi di valutazione previsti da ETSI e CEN,

	assicurando un livello avanzato di protezione contro l'accesso non autorizzato e la manipolazione dei dati di firma.
RAO	Registration Authority Officer/Operatore di Registrazione
Richiedente	È il soggetto che richiede al Certificatore il rilascio di Certificati Qualificati. Se il Soggetto è diverso dal Titolare del Certificato l'identità del Richiedente verrà inserito nel campo Organization del Certificato X.509.
RSA	Algoritmo di crittografia asimmetrica, basato su chiavi pubbliche e private.
SAD	Signature Activation Data
SAM	Signature Activation Module
SSAS	Server Signing Application Service
SSASP	Server Signing Application Server Provider
Servizio fiduciario	È un servizio elettronico definito nell'ambito del Regolamento eIDAS che può essere a) creazione, verifica e convalida di firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, servizi elettronici di recapito Certificato; Certificati relativi a tali servizi; b) servizi di creazione, verifica e convalida dei Certificati di autenticazione di siti web; c) servizi di conservazione di firme; sigilli o certificati elettronici relativi a tali servizi.
Servizio fiduciario qualificato	È un servizio fiduciario che soddisfa i requisiti stabiliti dal Regolamento eIDAS e ne fornisce le relative garanzie in termini di sicurezza e qualità.
Sigillo	È un insieme di dati in forma elettronica acclusi, o connessi, tramite associazione logica, ad altri dati in forma elettronica, per garantirne la provenienza e l'integrità.
Terzo Interessato	È la persona fisica o giuridica che dà il consenso, in conformità alle norme, al rilascio di Certificati Qualificati nei quali sia riportata l'appartenenza ad una Organizzazione ovvero eventuali poteri di rappresentanza o titoli e cariche rivestite. Ha il diritto/dovere di richiedere la revoca o sospensione del Certificato nel caso risultano modificati i requisiti in base ai quali lo stesso è stato rilasciato.
Titolare	Soggetto, persona fisica o giuridica, a cui è rilasciato un certificato di firma digitale o sigillo da parte di un Qualified Trust Service Provider (QTSP) e che detiene il controllo esclusivo dei dispositivi e delle

	credenziali di creazione della firma, assumendosi la responsabilità del loro corretto utilizzo.
Uffici di registrazione, "Registration Authority" o "RA"	È la persona giuridica delegata dal Certificatore allo svolgimento delle operazioni di identificazione e registrazione dei Richiedenti, secondo le modalità individuate e descritte nel presente Manuale. L'ente deve aver preventivamente stipulato accordi di servizio con il Certificatore. L'RA può avvalersi di ulteriori soggetti e/o di RAO per le operazioni identificazione e registrazione.

2. PUBBLICAZIONE DELLE INFORMAZIONI E REPOSITORY

2.1. Repository

Bit4id dispone di un archivio on-line (c.d. Repository) attraverso il quale rende pubbliche e liberamente accessibili le informazioni relative ai servizi di certificazione. Suddetto archivio è pubblicato sul sito di Bit4id https://bit4id.com/documentazione-qtsp.

Il "*Repository*" è accessibile in modo continuo (24x7x365).

Nell'ipotesi in cui si verifichi un arresto del sistema, al di fuori del controllo di Bit4id, quest'ultima si impegnerà nel miglior modo possibile affinché il servizio ritorni di nuovo disponibile nel termine stabilito nella sezione 5 del presente Manuale Operativo.

2.2. Elenco delle informazioni pubblicate dalla CA

Bit4id pubblica le seguenti informazioni:

- I riferimenti delle CRL aggiornate dal Certificatore (link alle CRL);
- *Il PKI Disclosure Statement* e il *TSA Disclosure Statement*;
- la *Certification Practice Statement* (CPS);
- Le Condizioni generali di contratto (Terms and Conditions);
- La Modulistica relativa ai Servizi Fiduciari;
- I certificati della PKI.

Il Titolare persona fisica o giuridica che voglia avere accesso al proprio certificato, per le finalità descritte all'articolo 34 co. 2 del DPCM 22 febbraio 2013, può farne richiesta inviando l'apposito modulo (disponibile sul sito), firmato digitalmente. La richiesta di accesso al certificato deve essere inoltrata all'indirizzo PEC del QTSP. Tale possibilità non è prevista per i certificati *OneShot*.

2.3. Frequenza delle pubblicazioni

Le informazioni relative alla CA, incluso il presente Manuale Operativo, e la documentazione correlata, sono pubblicate nella versione più recente sul sito del Certificatore.

L'ultima versione del Manuale Operativo viene puntualmente trasmessa preventivamente ad AgID per formale approvazione, prima della pubblicazione.

Le modifiche al Manuale Operativo sono soggette alle disposizioni di cui alla sezione 1 del presente documento.

Le informazioni relative allo stato di revoca dei certificati vengono pubblicate in accordo con quanto stabilito nella sezione 4 del presente Manuale Operativo.

2.4. Controllo degli accessi

Bit4id non limita l'accesso alle informazioni stabilite nella sezione 2, tuttavia predispone un sistema di controllo atto ad impedire che soggetti non autorizzati possano aggiungere, modificare o cancellare i dati dalla stessa registrati, allo scopo di tutelare l'integrità e l'autenticità delle informazioni.

3. IDENTIFICAZIONE E AUTENTICAZIONE

3.1. Nomi

3.1.1. Tipologia dei nomi

Tutti i certificati sono contraddistinti da un nominativo identificativo (DN o *Distinguished Name*), conforme allo standard X.500, inserito nel campo *Subject*, il quale include un componente *Common Name* (CN=), relativo all'identità del Richiedente, congiuntamente ad altre informazioni addizionali, inserite nel campo *SubjectAlternativeName*.

Le regole di valorizzazione degli attributi del DN rispettano le norme ETSI EN in relazione ai profili dei certificati per persone fisiche/giuridiche nonché le specifiche contenute nella RFC 5280 (Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile) e si conformano alle Raccomandazioni di cui alla Determinazione n. 147/2019 emessa dall'AgID.

Come previsto dagli standard ETSI EN 319 412-2 par. 4.2.4 e 319 412-3 par. 4.2.1, Bit4id ha fissato i limiti dei singoli campi givenName, surname, pseudonym, commonName, organizationName and organizationalUnitName a 250 (duecentocinquanta) caratteri.

In particolare, i certificati emessi secondo questo documento CPS sono conformi ai seguenti standard:

- **ETSI EN 319-401**: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- **ETSI EN 319 411-1**: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- **ETSI EN 319 411-2**: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- **ETSI EN 319 412-1**: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- **ETSI EN 319 412-2**: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- **ETSI EN 319 412-5**: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

I certificati di TSU sono emessi in conformità agli standard:

- **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.

3.1.2. Significato dei nomi

I valori contenuti nei certificati sono i seguenti:

- *Country;*
- *Organization;*
- *Organization Unit;*
- *Organization Identifier;*
- *Title;*
- *Surname;*
- *Given Name;*
- *Serial Number;*
- *Common Name;*

I nomi contenuti nei campi *SubjectName* e *SubjectAlternativeName* dei certificati sono comprensibili nel linguaggio naturale e dovranno essere significativi per consentire la corretta identificazione dei Titolari dei certificati di firma e sigillo elettronico qualificato.

Nei casi di certificati di *Time Stamp Unit*, l'attributo del certificato *Distinguished Name* contine il nome che identifica la TSU stessa.

Nell'ipotesi in cui i dati indicati nel campo *DN* o *Subject* siano fittizi (es. "*Organizzazione test*", "*Nome test*", "*Cognome test*") o vengano indicate parole che inequivocabilmente ne denotano l'invalidità (es. "TEST", "PROVA" o "NON VALIDO"), il certificato risulterà privo di valenza legale e, pertanto, si escluderà ogni responsabilità da parte di Bit4id circa il suo utilizzo.

I suddetti certificati vengono emessi al fine di realizzare prove tecniche di interoperabilità e permettere all'Organismo supervisore competente (AgID) di effettuare le sue valutazioni.

Possono essere emessi anche certificati con scopi di test con identità reali, in questo caso, vengono acquisiti i documenti reali della persona e il certificato viene revocato al termine del test.

3.1.3. Impiego di dati anonimi e pseudonimi

In nessun caso è possibile utilizzare pseudonimi al fine di identificare un Titolare persona fisica. Allo stesso modo, in nessun caso verranno emessi certificati anonimi.

Diversamente vale per il caso in cui Richiedente sia una persona giuridica: in questa circostanza è ammessa la possibilità di utilizzare uno pseudonimo per la sua identificazione all'interno del certificato.

3.1.4. Regole di interpretazione dei nomi

Per le regole di interpretazione dei nomi, viene rispettato lo standard ITU-T relativo ai servizi di directory (ITU-T X.500 ovvero ISO/IEC 9594).

3.1.5. Unicità dei nomi

Per garantire la correlazione univoca tra Titolare e certificato, la sezione *Subject* di quest'ultimo non può mai essere identica per due distinti titolari. Pertanto, secondo quanto indicato dalla norma ETSI EN 319 412 in merito ai profili di emissione dei certificati, il campo *Subject* (*SubjectDistinguishedName o SubjectDN*) contiene attributi identificativi specifici in base alla natura del Titolare stesso.

In particolare, l'unicità viene garantita dai seguenti attributi:

- il *SerialNumber* (OID 2.5.4.5) contenente il codice fiscale del soggetto (indicato con il prefisso *TIN*) o, in alternativa, un codice identificativo in ottemperanza alla norma ETSI EN 319 412-1 (come il numero del passaporto o della carta d'identità del titolare);
- l'*OrganizationName* (OID 2.5.4.10) utilizzato per indicare l'appartenenza o l'affiliazione del titolare all'organizzazione. Nel caso in cui l'*OrganizationName* sia presente, in medesimi vincoli si applicano anche all'eventuale codifica dell'attributo *Title*. Nel caso in cui il soggetto da identificare sia una persona giuridica l'attributo verrà valorizzato in accordo al paragrafo 4.2.1 della norma ETSI 319 412-3.
- il *Givenname* (OID 2.5.4.42) contenente il nome del soggetto;
- il *Surname* (OID 2.5.4.44) contenente il cognome del soggetto;

È, inoltre, prevista la possibilità di inserire nell'attributo *description* (OID 2.5.4.13) il codice EORI (*Economic Operator Registration and Identification*) di cui al Regolamento (UE) n. 312/2009 del 16 aprile 2009 e s.m.i.

Per le persone giuridiche, con riferimento all'uso della sintassi dell'identificatore "*legal person identifier*" di cui al capo 5.1.4. dello standard ETSI EN 319 412-1, in caso di organizzazioni non dotate di partita IVA, ma solo di codice fiscale si seguirà la modalità di cui al n. 3 del capo 5.1.4. citato (tramite l'utilizzo dei caratteri "CF").

L'unicità per i certificati qualificati di marca temporale (TSU) viene parimenti assicurata da Bit4id, che si conforma alla specifica RFC-5280 nonché alle Raccomandazioni di cui all'art. 4.2 della Determinazione n. 147/2019 di AgID rubricato "Profilo dei Certificati di certificazione e validazione temporale".

3.1.6. Eventuali limitazioni d'uso

Ulteriori limiti d'uso del certificato saranno inseriti nell'attributo *explicitText* del campo *userNotice* dell'estensione *certificatePolicies*.

Bit4id garantisce, in conformità all'art. 4.1 n. 7 della Determinazione n. 147/2019 di AgID e su richiesta del Titolare del Certificato, almeno i seguenti limiti di utilizzo:

- i titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato;
- il presente certificato è valido solo per firme apposte con procedura automatica;
- l'utilizzo del certificato è limitato ai rapporti con (indicare il soggetto).

Per ulteriori informazioni sulle limitazioni d'uso si rimanda al Par. 4.5.3. del presente Manuale.

3.1.7. Soluzione dei conflitti relativi ai nominativi

Bit4id non è tenuta a verificare previamente che un Richiedente il certificato sia titolare del diritto all'uso del nome che compare in una richiesta di certificato ma, salvo tale circostanza non risulti evidente, provvederà al rilascio del certificato.

La medesima modalità sarà applicata anche nel caso in cui il Richiedente agisca in rappresentanza di una persona giuridica.

Parimenti, non agirà come arbitro o mediatore né in nessun altro modo dovrà dirimere alcuna disputa riguardante la titolarità dei nomi delle persone fisiche o giuridiche, i nomi del dominio, i marchi o i nominativi commerciali.

Nel caso in cui Bit4id riceva una notifica relativa alla sussistenza di un conflitto sui nomi, sulla base della legislazione vigente nello Stato del Richiedente, potrà intraprendere le azioni pertinenti orientate a bloccare o ritirare il certificato emesso.

In ogni caso, la CA si riserva il diritto di rigettare una richiesta di certificato, nell'ipotesi in cui sussista un conflitto sui nomi.

3.2. Verifica iniziale dell'identità

La CA, anche mediante un Ufficio di registrazione (R.A.), verifica con certezza l'identità di ogni Richiedente alla prima richiesta di emissione di un certificato qualificato al fine di assicurare che quel certificato possa riferirsi in maniera accurata e completa al soggetto Richiedente (sia esso persona fisica o giuridica); prima di procedere al rilascio del certificato richiesto, dunque, la CA oppure la R.A. dovrà svolgere tutte le attività necessarie all'identificazione del Richiedente.

L'identità del Richiedente il certificato viene solitamente verificata tramite un documento di identità nonché tramite specifici attributi che possono essere: l'associazione con l'Organizzazione di appartenenza, il ruolo posseduto all'interno dell'organizzazione, il certificato di attribuzione di codice fiscale/partita iva, nel caso di persone giuridiche.

L'operazione di identificazione è svolta in ottemperanza a quanto previsto dalla vigente normativa: il soggetto incaricato ad effettuare le attività di identificazione sarà, quindi, tenuto a verificare l'identità del richiedente tramite il riscontro con uno dei documenti aventi validità legale ai sensi dell'art. 35 d.P.R. del 28 dicembre 2000 n. 445.

Tutta la documentazione così acquisita e verificata sarà conservata dalla CA, in conformità a quanto disposto dal Regolamento (UE) 2016/679 – GDPR - del Parlamento Europeo e del Consiglio del 27 aprile 2016 e s.m.i., per tutto il tempo necessario ad assicurare la fruizione e la continuità del servizio richiesto.

Per garantire la tutela e la gestione dei dati personali acquisiti nel corso delle procedure di registrazione, inoltre, sarà preventivamente fornita ad ogni richiedente l'informativa sulla privacy.

Per il dettaglio della procedura di identificazione di una persona fisica o di una persona giuridica è possibile fare riferimento ai par. 3.2.2. e seguenti.

3.2.1. Modalità di Identificazione per Persone Fisiche

L'identità del Titolare può essere accertata mediante le seguenti modalità ed in conformità con l'art. 24 del Regolamento eIDAS.

Modalità	**Soggetti abilitati ad eseguire l'identificazione**	**Condizioni tecnologiche di autenticazione richieste per l'identificazione**	**Tipo di certificato (pluriennale, One-Shot)**
De visu	Certification Authority (CA) Registration Authority (RA) Local Registration Authority (LRA) Registration Authority Officer (RAO)/ Incaricato alla Registrazione (IR)	Nessuna	Tutti

Namirial Onboarding	Certification Authority (CA) Registration Authority (RA) Local Registration Authority (LRA) Registration Authority Officer (RAO)/ Incaricato alla Registrazione (IR)	Utilizzo di una postazione dotata di webcam (in caso di videoriconoscimento/SelfID)	Tutti
FEQ	Certification Authority (CA) Registration Authority (RA) Local Registration Authority (LRA) Incaricato alla Registrazione (IR)	Firma elettronica qualificata emessa da un QTSP	Tutti
SPID/CIE	Certification Authority (CA) Registration Authority (RA)	Utilizzo di una identità digitale nazionale quale SPID (Sistema Pubblico di Identità Digitale) o Carta d'identità elettronica (CIE)	Tutti
Identificazione elettronica nazionale	Certification Authority (CA) Registration Authority (RA)	Utilizzo di un mezzo di identificazione elettronica nazionale preesistente, notificato dallo Stato Membro	Tutti
Processi ex. Art 24	Certification Authority (CA)	Nessuna	Tutti

	Registration Authority (RA) Local Registration Authority (LRA) Incaricato alla Registrazione (IR)		
Processi AML (Normativa PSD2)	Titolari destinatari degli obblighi Antiriciclaggio ai sensi delle normative di recepimento della Direttiva 2005/60/CE del Parlamento Europeo e del Consiglio relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, e delle successive normative comunitarie di esecuzione e s.m.i. (Normativa PSD2)	Utilizzo del processo AML per l'identificazione del richiedente	Tutti

3.2.2. Prova del possesso della chiave privata

Il possesso della chiave privata è comprovato dal corretto svolgimento del procedimento di rilascio ed accettazione del certificato da parte del Richiedente e/o Titolare.

In particolare, Bit4id verifica che il Richiedente sia in possesso della chiave privata corrispondente alla chiave pubblica da certificare.

3.2.3. Verifica dell'identità di una persona fisica

Questa sezione illustra i metodi di verifica dell'identità di una persona fisica identificata in un certificato.

Gli operatori incaricati di verificare l'identità delle persone fisiche che richiedono il Certificato eseguono le operazioni di identificazione secondo le modalità previste nel presente Manuale Operativo, in conformità alle linee guida di cui al Pr. 6.2 dell'ETSI EN 319 411-2 e s.m.i. e ai criteri di cui alla "*Baseline Requirements Guidelines*" e alla clausola 11 dell'"*Extended Validation Certificate Guidelines*" e ogni altra normativa nazionale ed europea applicabile.

L'identità delle Richiedenti, identificate nei certificati, è comprovata dalla presentazione di un documento di riconoscimento valido agli effetti di legge (Carta di identità, Passaporto, Patente di guida) o attraverso un metodo di identificazione forte, descritte al §3.2.1.

Qualora sia richiesto l'inserimento del Ruolo e del Terzo Interessato nel Certificato Qualificato deve, inoltre, essere fornito al Certificatore, documento dell'Organizzazione su carta intestata, recante data e numero di protocollo, che autorizza all'inserimento dei dati nel Certificato Qualificato del Richiedente, non antecedente a 30 (trenta) giorni dalla data di richiesta di registrazione.

3.2.3.1. Procedura di identificazione De Visu

Tale procedura di identificazione prevede la presenza fisica del Richiedente dinnanzi ad un Operatore o al personale autorizzato dalla RA di Bit4id, il quale provvede (avendo ricevuto apposita formazione in precedenza) ad accertare l'identità del Richiedente attraverso la verifica dei corrispondenti documenti di identità esibiti in originale.

È specifico onere dell'Operatore accertarsi che il documento di identità esibito risulti in corso di validità (e, dunque, che non sia scaduto al momento della presentazione della richiesta di emissione del certificato) e che quest'ultimo rechi in maniera chiara la fotografia del soggetto da identificare.

È necessario che il documento di riconoscimento valido agli effetti di legge, ai sensi della normativa su richiamata, sia in corso di validità (e dunque non scaduto al momento della presentazione della richiesta di emissione del certificato); inoltre, è necessario che al predetto documento sia acclusa una fotografia chiara che consenta la riconducibilità diretta al soggetto che lo esibisce.

Al tal riguardo l'art. 1 lett. c) D.P.R. 445/2000 attribuisce la qualifica di "*Documento d'identità*" ad ogni documento *"…munito di fotografia del titolare e rilasciato, su supporto cartaceo, magnetico o informatico, da una pubblica amministrazione italiana o di altri Stati, che consenta l'identificazione personale del titolare"*.

Inoltre, ai sensi dell'art. 35 D.P.R. 445/2000: *"In tutti i casi in cui nel presente testo unico viene richiesto un documento di identità, esso può sempre essere sostituito dal documento di riconoscimento equipollente ai sensi del comma 2. […]"*.
Per l'elenco completo dei documenti di identità accettati da Bit4id si rimanda all'allegato "B" al presente Manuale.

Il Richiedente, cittadino italiano, può identificarsi per mezzo di un documento d'identità in corso di validità, quali:

- Carta d'identità,
- Passaporto,
- Patente di guida.

Possono essere concordate tra Bit4id e la Registration Authority altre categorie di documenti di riconoscimento, tra quelle previste dal comma 2 dell'art. 35 del DPR 445/2000.

In caso di Uffici di registrazione operanti a livello internazionale o cittadini stranieri che richiedano un Certificato, i documenti che possono essere presentati sono contenute nell'allegato B del presente Manuale.

In tal caso, i suddetti documenti sono accettati esclusivamente a condizione che le relative caratteristiche siano verificabili all'interno del database PRADO (https://www.consilium.europa.eu/prado/en/prado-start-page.html).

È necessario che il Richiedente, cittadino italiano, sia in possesso del Codice Fiscale (Tessera Sanitaria, Tessera del Codice Fiscale, Certificato di attribuzione di Codice Fiscale ecc..) la cui esibizione può essere richiesta dai soggetti abilitati ad eseguire il riconoscimento; in mancanza sarà possibile utilizzare un analogo codice identificativo (es: codice di previdenza sociale) o il numero identificativo del passaporto.
Nel caso di persona fisica, il personale incaricato ed addetto all'identificazione provvederà all'accertamento delle seguenti tipologie di dati:

- Nome completo (prenome, nome e cognome);
- data e luogo di nascita;
- indirizzo di residenza e di domicilio;
- codice fiscale o altro codice identificativo univoco;
- indirizzo di posta elettronica;
- tipo e numero del documento di identità esibito;

- Autorità che ha rilasciato il documento, data e luogo di rilascio, data di scadenza;
- ogni altro dato ritenuto utile ai fini dell'identificazione;

Nel caso in cui il soggetto da identificare sia una persona fisica identificata in associazione con una persona giuridica (della quale è dipendente o legata da rapporto di collaborazione) l'addetto provvederà ad acquisire le seguenti informazioni:

- Nome completo (prenome, nome e cognome);
- data e luogo di nascita;
- indirizzo di residenza e di domicilio;
- codice fiscale;
- indirizzo di posta elettronica;
- tipo e numero del documento di identità esibito;
- Autorità che ha rilasciato il documento, data e luogo di rilascio, data di scadenza;
- nome completo e denominazione sociale della persona giuridica associata;
- qualsiasi informazione di registrazione esistente relativamente alla persona giuridica associata;
- tipo di affiliazione della persona fisica alla persona giuridica e documentazione comprovante tale rapporto.
- ogni altro dato ritenuto utile ai fini dell'identificazione;

Sarà onere del Richiedente fornire, al termine delle operazioni di identificazione, un indirizzo fisico o di domicilio dove poter essere contattato.

L'Ufficio di Registrazione verificherà, mediante la visualizzazione di documenti o attraverso le proprie fonti di informazione, il resto dei dati e degli attributi da includere nel certificato, conservando la documentazione che ne comprova la validità nei termini e per la durata previsti dalle normative applicabili.

La procedura di identificazione può essere svolta anche da un Pubblico Ufficiale in base a quanto disposto dalle normative che disciplinano la loro attività, ivi comprese le disposizioni di cui al D.L. 3 Maggio 1991, n. 143 e s.m.i.

La raccolta delle evidenze del riconoscimento nella procedura *Devisu* può essere eseguita tramite *web application* messa a disposizione da Bit4id ai propri Operatori, opportunamente formati; in questo caso l'archiviazione avviene direttamente sui sistemi del Certificatore, che provvederà all'invio in conservazione secondo i termini stabiliti nel presente Manuale e nell'Informativa Privacy.

In caso contrario, l'Operatore a ciò autorizzato è tenuto a raccogliere e ad archiviare in maniera sicura gli originali di tutta la documentazione inerente ogni singola richiesta di emissione dei

Certificati nonché tutta la documentazione relativa all'identificazione dei Richiedenti che sarà comunicata a Bit4id.

Bit4id si impegna a conservare e ad archiviare tutte le informazioni relative ai Dati Personali dei Richiedenti, in conformità con il Regolamento (UE) n. 679/2016 e la propria Politica sulla Privacy.

3.2.3.2. Procedura di identificazione da remoto

In alternativa alla procedura di identificazione "*de visu*", Bit4id, in armonia con gli obiettivi di cui al Regolamento eIDAS tesi a rafforzare la fiducia nelle transazioni elettroniche nel mercato interno fornendo una base comune per interazioni elettroniche sicure fra cittadini e imprese, ha previsto una procedura di identificazione dei richiedenti da remoto, tramite utilizzo di una apposita piattaforma telematica di video-identificazione messa a disposizione da Namirial S.p.A., società capogruppo che esercita il controllo su Bit4id s.r.l.

Bit4id garantisce l'utilizzo di procedure e strumenti in grado di garantire, sul piano giuridico, l'identificazione "*certa*" del Richiedente il certificato qualificato, in piena conformità a quanto richiesto dall'art. 19 del CAD secondo cui il certificatore che *"rilascia […] certificati qualificati deve […] provvedere con certezza alla identificazione della persona che fa richiesta della certificazione" e dal successivo art. 32 co. 3 lett. a).*

Gli Uffici di Registrazione che operano in altri Stati membri dell'Unione Europea, così come quelli che procedono all'identificazione di Richiedenti che risiedono in altri Stati membri dell'Unione Europea, possono ricevere autorizzazione da Bit4id ad accettare documenti di identità emessi dalle autorità competenti nel Paese in questione. La lista di questi documenti e le relative caratteristiche (in grado di fornire certezza dell'identità) viene analizzata da Bit4id, che procede alle comunicazioni opportune ad AgID prima di effettuare la pubblicazione della lista dei documenti accettati sul proprio sito internet (Allegato B al presente Manuale).

Una volta effettuata la richiesta di emissione di un certificato digitale qualificato da parte del Richiedente, Bit4id o un suo Ufficio di Registrazione (RA) autorizzato, provvederà alla fissazione della data e dell'ora del primo appuntamento disponibile, la quale sarà comunicata al Richiedente tramite i canali di comunicazione da quest'ultimo indicati in fase di richiesta.

Prima di procedere con tale modalità di identificazione il Richiedente viene informato che dovrà disporre di un Personal Computer, di uno smartphone o di un Tablet dotato di *webcam* (ovvero di videocamera che consenta la visualizzazione e l'ascolto di tutto ciò che avviene nel suo campo visuale) e, successivamente, gli verranno fornite le opportune indicazioni in relazione alla piattaforma da utilizzare per la video-identificazione.

Il sistema per la video-identificazione è messo a disposizione è in grado di garantire che le modalità di registrazione delle immagini e dei video assicurino la non alterabilità e/o sostituibilità del

soggetto ripreso e di tutte le immagini e/o suoni che vengono rilevati nel corso della sessione di ripresa tramite *webcam*.

Inoltre, è necessario che, durante la sessione di ripresa, l'immagine video sia a colori e consenta una chiara visualizzazione dell'interlocutore.

L'operatore, al fine di assicurare quanto sopra, potrà non avviare o sospendere in qualsiasi momento la procedura di identificazione qualora la qualità audio/video risulti tale da non garantire i requisiti sopra indicati nonché quelli di cui all'art. 32 comma 3 lett. a) del CAD.

Scegliendo di proseguire nella procedura di identificazione da remoto il Richiedente sarà informato sulle modalità e sul Trattamento dei Dati Personali, in conformità alla Privacy Policy prevista da Bit4id e che la sessione di identificazione tramite *webcam* sarà registrata; in questo modo il Richiedente potrà così scegliere se fornire o meno il consenso al Trattamento: resta inteso che, in caso di mancato consenso circa il Trattamento dei Dati Personali da parte del Richiedente, Bit4id non potrà procedere alla successiva identificazione.

In caso di manifestazione espressa del consenso, che potrà avvenire anche a seguito di esplicita richiesta dell'operatore incaricato all'inizio di ogni sessione, Bit4id o uno degli operatori a ciò autorizzati, potrà procedere con l'identificazione da remoto.

A questo punto, avviata la sessione tramite *webcam*, l'operatore incaricato, ai fini di una corretta identificazione personale tramite il documento di identità, provvederà, innanzitutto a verificare se:

a. il documento è stato rilasciato da un'Amministrazione dello Stato;
b. il documento reca la fotografia del soggetto;
c. nel documento sono presenti i dati anagrafici del soggetto;
d. il documento presenta il seriale identificativo;
e. il documento presenta idonei segni di anticontraffazione;

Bit4id garantisce che gli operatori incaricati di effettuare le operazioni sopra descritte sono adeguatamente formati; è facoltà dell'incaricato, dunque, escludere l'ammissibilità dei documenti esibiti dai Richiedenti, se carenti di una delle caratteristiche sopra elencate.

Una volta completata e chiusa la sessione di identificazione da remoto, il video così realizzato sarà conservato e protetto in modo adeguato, in conformità al Trattamento dei dati personali di cui alla Privacy Policy adottata da Bit4id.

3.2.3.3. Procedura di identificazione tramite AML (Anti-money Laundering)

Con il Decreto legislativo 21 novembre 2007, n. 231, di recepimento della Direttiva 2005/60/CE in materia di AML (*Anti-money Laundering*), come modificato dal Decreto Legislativo 25 maggio 2017, n. 90, di recepimento della direttiva (UE) 2015/849 (poi sostituita dalla Direttiva (UE) 2018/843) relativa alla prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del

terrorismo è stata data attuazione in Italia alle disposizioni europee in tema di AML nonché di In alternativa alla organizzazione, procedure e controlli interni in materia di comunicazioni oggettive ed in materia di adeguata verifica della clientela previsti dal D.Lgs. n. 90/2017 (di seguito anche solo "*Normativa AML*").

Importante menzione sul tema meritano anche gli orientamenti emanati congiuntamente dalle Autorità di Vigilanza europee (*EBA*, *ESMA e EIOPA*) sulle misure semplificate e rafforzate di adeguata verifica della clientela e sui fattori di rischio, pubblicati il 4 gennaio 2018 nonché le "*Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo*" emesse dalla Banca d'Italia (30/07/2019).

Allo scopo di semplificare e snellire le procedure di identificazione ed evitare che uno stesso soggetto, già identificato presso altra organizzazione o organismo, debba nuovamente effettuare la procedura di identificazione Bit4id, in accordo con la normativa italiana ed Europea sopra richiamata, ha adottato la seguente "*procedura di identificazione tramite AML (Anti-money laundering)*".

La predetta procedura può essere applicata unicamente nell'ipotesi in cui vi sia già stata la previa identificazione del Richiedente da parte di un soggetto a ciò autorizzato (Intermediario Finanziario o Soggetto Esercente Attività Finanziaria) che, in ossequio alla normativa su richiamata in materia di *AML* (o Antiriciclaggio) ha assolto precisi obblighi e osservato specifiche procedure nella fase di identificazione dei propri clienti.

I soggetti che, ai sensi della Normativa AML, identificano i Richiedenti sono tenuti ad accettare le disposizioni del presente Manuale e a stipulare appositi accordi con Bit4id al fine di operare quali Uffici di Registrazione (RA).

L'acquisizione dei dati identificativi dei Richiedenti, da parte dei soggetti abilitati ai sensi della Normativa AML, comporta che Bit4id potrà emettere certificati digitali qualificati a favore dei Richiedenti già identificati; tuttavia è necessario, al fine di completare correttamente la procedura di riconoscimento e di emissione del certificato in conformità alle disposizioni del presente Manuale, che il Richiedente sottoscriva le Condizioni Generali di Contratto per la fornitura dei servizi fiduciari qualificati predisposte da Bit4id e confermi i dati identificativi già precedentemente acquisiti.

3.2.3.4. Procedura di identificazione tramite CIE

Bit4id ha previsto, quale ulteriore modalità di identificazione, la possibilità di utilizzare la CIE "Carta di Identità Elettronica" per l'acquisizione certa dei dati identificativi dei Richiedenti.

Per CIE, ai sensi dell'art. 1 del D.M. 23 dicembre 2015 si intende: "il documento di identità personale rilasciato dal Ministero dell'Interno denominato "Carta di Identità Elettronica", mezzo di

identificazione elettronica, di livello elevato, notificato ai sensi dell'articolo 9 del Regolamento eIDAS.

Il Richiedente effettua l'autenticazione sul portale del Certificatore o del CIE ID Server con credenziali di livello 3 (LoA4-High). Il sistema recupera le informazioni anagrafiche inserite nel certificato digitale e le associa a quelle relative al certificato di sottoscrizione in oggetto di richiesta.

A seguito della corretta esecuzione della procedura di identificazione sopra descritta sarà possibile, per Bit4id, emettere il certificato digitale qualificato richiesto dal Richiedente, previa sottoscrizione, da parte di quest'ultimo, delle Condizioni Generali di Contratto per la fornitura dei servizi fiduciari qualificati.

I dati di registrazione in questo caso sono conservati esclusivamente in formato elettronico.

3.2.3.5. Procedura di identificazione tramite firma digitale rilasciata da altro QTSP

La seguente procedura di identificazione consente al Richiedente di identificarsi in maniera certa mediante l'utilizzo di certificati qualificati rilasciati da altri prestatori di servizi, in conformità al Regolamento eIDAS.

In questo caso, il Richiedente è stato già previamente identificato da un prestatore di servizi fiduciari qualificato, che ha rilasciato il certificato digitale e utilizzerà quest'ultimo, se ancora in corso di validità, per firmare il modulo di richiesta di emissione del certificato qualificato da parte di Bit4id.

Ricevuta la richiesta di emissione, sottoscritta digitalmente da parte del Richiedente, Bit4id effettuerà adeguati controlli al fine di verificare la validità del certificato utilizzato per la firma riservandosi di rifiutare la richiesta di emissione in caso di esito negativo di questa.

3.2.3.6. Procedura di identificazione tramite identità digitale SPID

Ai sensi dell'art. 64 co. 2-bis del Codice dell'Amministrazione Digitale "*per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID)*".

Il Richiedente, in possesso di credenziali di autenticazione SPID (di livello 2 o superiore), potrà richiedere a Bit4id. previa accettazione delle Condizioni Generali di Contratto, l'emissione di certificati digitali qualificati.

In tali casi, infatti, l'identità del Richiedente è già stata previamente accertata da uno dei Fornitori dell'Identità Digitale SPID (IdP) accreditato dall'Agenzia per l'Italia Digitale, per la gestione dell'identità digitale dei propri utenti.

Il richiedente è chiamato ad effettuare un'autenticazione sul portale del Certificatore attraverso meccanismi del circuito SPID, in tale processo di autenticazione, sono richiesti i seguenti

dati minimi, acquisiti insieme alla transazione dell'autenticazione dal Certificatore:

- Nome;
- Cognome;
- Codice Fiscale;
- Sesso;
- Data di Nascita;
- Luogo di Nascita;

I dati di registrazione sono conservati esclusivamente in formato elettronico.

3.2.3.7. Rafforzamento dell'identificazione - Adeguamento ai requisiti eIDAS 2

In coerenza con le disposizioni dell'articolo 24 del Regolamento (UE) 2024/1183 (c.d. eIDAS 2) in materia di verifica dell'identità ai fini del rilascio di certificati qualificati, Bit4id assicura che i processi di identificazione impiegati per l'emissione dei certificati raggiungano un livello di sicurezza e affidabilità coerente con il livello di garanzia "elevato" (High) adottato nell'ambito del percorso di adeguamento regolamentare (in sostituzione di approcci basati sul solo livello "significativo/substantial").

Qualora l'identificazione del Richiedente avvenga inizialmente tramite un mezzo di identificazione elettronica che, di per sé, presenti livello di garanzia "significativo" (ad esempio SPID livello 2), tale modalità viene considerata un fattore di ingresso e non l'unico elemento di certezza dell'identità ai fini del requisito "High".

In tali casi, al fine di rafforzare la certezza dell'identità del Richiedente e garantire il livello di garanzia elevato richiesto, Bit4id utilizza Namirial Onboarding, piattaforma di digital onboarding e identificazione remota progettata da Namirial S.p.A. (società capogruppo) e certificata ETSI TS 119 461, integrata nei flussi Bit4id come componente di supporto al processo di identificazione.

In particolare, mediante il processo denominato *ID Self*, la piattaforma esegue una verifica aggiuntiva basata su acquisizione tramite web application del documento d'identità (fronte e retro) e del volto del Richiedente, abilitando controlli di corrispondenza e "binding" tra titolare e documento, nonché meccanismi di verifica biometrica e di vivacità ("liveness") previsti dai flussi ETSI.

L'integrazione di Namirial Onboarding consente dunque di elevare la robustezza del processo di identificazione anche quando il mezzo iniziale (es. SPID L2) non risulti, da solo, sufficiente a soddisfare l'obiettivo di livello "High", mantenendo coerenza con gli standard tecnici di riferimento applicabili ai processi di identity proofing in ambito servizi fiduciari.

3.2.4. *Verifica dell'identità di una persona giuridica*

Nel caso in cui il soggetto da identificare sia una persona giuridica, il Richiedente dovrà sottoporsi alle procedure di identificazione previste nel precedente capo 3.2.3. fornendo, in aggiunta, anche i dati relativi alla persona giuridica (visura, certificato camerale o documento equipollente).

A tal fine, il Richiedente dovrà, quindi, presentare la documentazione necessaria ad attestare il possesso dei poteri di rappresentanza (certificato camerale o visura storica/ordinaria da cui risulti la carica dichiarata) e/o di delega da persona munita di tale potere.

3.2.5. *Misure anticontraffazione*

Al fine di prevenire il verificarsi di ogni possibile furto di identità (mediante impersonificazione *totale* o *parziale*) Bit4id ha implementato rigide misure per l'adeguata verifica dell'identità dei Richiedenti attuate durante le procedure di identificazione condotte ai sensi del presente Manuale (v. par. 3.2.2.1. e ss.).

In particolare, la verifica dell'identità dei Richiedenti è attuata mediante:

a) adeguata formazione degli operatori deputati allo svolgimento delle attività di identificazione dei Richiedenti (con particolare riferimento alla verifica della genuinità dei documenti di identità presentati in occasione delle operazioni di riconoscimento);
b) utilizzo di piattaforme e portali di fonti autoritative per il riscontro dei dati contenuti all'interno dei documenti di identità e delle tessere sanitarie utilizzate dai Richiedenti nella fase di identificazione. A titolo esemplificativo e non esaustivo:
    1. verifica dell'esattezza del codice fiscale (e/o della Partita Iva in caso di persona giuridica) dei Richiedenti attraverso l'interrogazione del servizio on-line messo a disposizione dall'Agenzia delle Entrate;
    2. verifica dei dati contenuti all'interno dei documenti di identità presentati dai Richiedenti attraverso l'utilizzo della piattaforma *SCIPAFI* ("*Sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo, con specifico riferimento al furto di identità*") gestita da Consap S.p.a. e di titolarità del Ministero dell'Economia e delle Finanze.

Bit4id si riserva il diritto di adottare ulteriori e più adeguate misure di verifica dell'identità dei Richiedenti con l'esclusivo fine di prevenire il cd. *furto di identità* inteso nelle seguenti duplici accezioni:

- **Impersonificazione totale**: occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità di un altro soggetto;

- **Impersonificazione parziale**: occultamento parziale della propria identità mediante l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi ad un altro soggetto.

3.2.6. Informazioni non verificate

Bit4id non include nei certificati nessuna informazione relativa al Richiedente e/o Titolare che non sia stata correttamente verificata.

3.2.7. Autorizzazione di un Ufficio di Registrazione e dei suoi Operatori

Per la costituzione di un nuovo Ufficio di Registrazione (RA), Bit4id effettua le necessarie verifiche per confermare l'esistenza dell'entità o dell'organizzazione in questione. A tal fine, Bit4id potrà utilizzare i documenti presentati o le proprie fonti di informazione.
Allo stesso modo, Bit4id verifica e convalida l'identità degli Operatori di Registrazione delle RA, per i quali, queste ultime, inviano a Bit4id la documentazione di identificazione, unitamente alla loro autorizzazione ad agire come tale. Bit4id garantisce che gli Operatori di Registrazione delle RA ricevano una formazione adeguata al corretto svolgimento delle loro attività, formazione che verrà confermata attraverso una corrispondente valutazione. Tale formazione e valutazione possono essere eseguite anche dalla RA precedentemente autorizzata da Bit4id.
Per la prestazione dei servizi oggetto del presente Manuale, Bit4id garantisce che gli operatori delle RA accedano al sistema tramite un'autenticazione sicura con certificati digitali.

3.3. Identificazione e autenticazione per le richieste di rinnovo

3.3.1. Rinnovo periodico dei certificati

Il rinnovo dei certificati può essere eseguito su certificati emessi da Bit4id.
Per procedere al rinnovo del certificato, il Titolare è tenuto a verificare che le informazioni in esso riportate siano ancora valide e non abbiano subito variazioni.
A tal fine, il processo prevede l'utilizzo del certificato ancora in corso di validità per la sottoscrizione del modulo di rinnovo, mediante il quale il Titolare autocertifica, ai sensi del D.P.R. 445/2000, la permanenza della validità dei propri dati anagrafici. Tale modalità presuppone, inoltre, che il certificato non sia scaduto, ossia che non risulti superata la data indicata nel campo "valido al".
Se le informazioni del Richiedente o del Titolare identificato nel certificato hanno subito variazioni, le nuove informazioni verranno correttamente registrate e sarà effettuata un'identificazione completa, conformemente alle disposizioni della sezione 3.2.3.

3.3.2. Richieste di rinnovo dopo la revoca

Nel caso in cui sia richiesto un rinnovo del certificato dopo la sua revoca è necessario, per il Richiedente, ripetere la procedura di validazione dell'identità di cui al par. 3.2.3.

Prima di generare un certificato per un Titolare il cui certificato precedente sia stato revocato, l'operatore o il personale autorizzato da una R.A. di Bit4id verificherà che le informazioni utilizzate per validare l'identità e le ulteriori informazioni del Richiedente e/o del Titolare siano valide, in quel caso si applicheranno le disposizioni della sezione precedente.

Dopo la revoca del certificato non sarà possibile procedere alla sua riattivazione ma sarà possibile unicamente procedere alla ri-emissione di un nuovo certificato (intesa quale nuova emissione).

Se le informazioni del Richiedente (o del Titolare) identificato nel certificato hanno subito variazioni, le nuove informazioni verranno correttamente registrate e sarà effettuata un'identificazione completa, conformemente alle disposizioni della sezione 3.

3.4. Identificazione e autenticazione per le richieste di revoca

Bit4id o il personale autorizzato dalla RA, ha il compito di gestire le richieste relative alla revoca di un certificato.

L'identificazione dei Richiedenti e/o dei Titolari nel processo di revoca dei certificati può essere effettuata:

- dal Richiedente e/o il Titolare:
  - tramite l'uso del codice di revoca ERC attraverso il sito Web di Bit4id https://www.bit4idtsp.com/lcm/ disponibile 7 giorni su 7 e 24 ore su 24;
- dalle RA: queste devono identificare il Titolare prima di approvare una richiesta di revoca in base ai mezzi che ritengono necessari.

In tutte le ipotesi in cui sussistano dei dubbi sull'identità del Richiedente il certificato entrerà in stato di sospensione.

La revoca non può essere richiesta per i certificati di tipo One-Shot.

4. REQUISITI OPERATIVI RELATIVI AL CICLO DI VITA DEI CERTIFICATI

4.1. Domanda di emissione del certificato

4.1.1. Legittimazione della richiesta

Il Richiedente è tenuto ad accettare e sottoscrivere la documentazione contrattuale predisposta da Bit4id.

4.1.2. Procedure e responsabilità

Bit4id riceve le richieste di certificati: tali richieste vengono inoltrate tramite un modulo, in formato cartaceo o digitale, tramite appositi servizi Web predisposti da Bit4id.

La domanda deve essere accompagnata da una documentazione di supporto relativa all'identità e da altre informazioni sulla persona fisica identificata nel certificato, in conformità alle disposizioni della sezione 3. Inoltre, è necessario allegare un indirizzo fisico o altri dati che consentano di contattare la persona fisica/giuridica identificata nel certificato.

4.2. Elaborazione della richiesta

4.2.1. Svolgimento delle funzioni di identificazione ed autenticazione

Ricevuta una richiesta di emissione di un certificato qualificato, Bit4id verifica che quest'ultima sia completa, accurata e debitamente autorizzata, prima di elaborarla.

In caso di esito positivo, Bit4id analizza le informazioni fornite, verificandone la compatibilità con gli aspetti descritti nella sezione 3.

Nel caso di un certificato qualificato, la documentazione comprovante l'approvazione della richiesta deve essere conservata e debitamente registrata e con garanzie di sicurezza e integrità per un periodo di 20 anni dalla data di scadenza del certificato, anche in caso di perdita anticipata della validità del certificato dovuta alla sua revoca.

4.2.2. Approvazione o rifiuto della richiesta

Nel caso in cui la verifica dei dati forniti abbia esito positivo, Bit4id approverà la richiesta di certificato e procederà alla sua emissione e consegna.

Se dalla verifica effettuata emerge che le informazioni fornite sono errate, o nel caso in cui tali informazioni vengano giudicate non affidabili, inesatte, incomplete o incoerenti, Bit4id rigetterà la

richiesta o interromperà la sua approvazione fino a quando non avrà effettuato i controlli che riterrà necessari.
Se, a seguito dell'ulteriore verifica, dovesse risultare che le informazioni fornite non sono corrette, Bit4id rifiuterà definitivamente la richiesta.
Bit4id notificherà al Richiedente l'approvazione o il rifiuto della richiesta.
Le procedure che permettono di verificare la correttezza delle informazioni contenute nei certificati e i processi di approvazione delle domande, in determinati casi, sono automatizzate.

4.2.3. Termine per l'elaborazione della richiesta

Bit4id elabora e lavora le richieste di certificati in ordine di arrivo entro il tempo necessario per gli adempimenti di carattere tecnico.
Le richieste rimangono attive fino alla loro approvazione o rifiuto.

4.3. Emissione del certificato

4.3.1. Processo e modalità di emissione

A seguito dell'approvazione della richiesta, il certificato viene generato in modo sicuro e reso disponibile al Titolare per l'accettazione.
Le procedure stabilite in questa sezione si applicano anche in caso di rinnovo dei certificati, poiché quest'ultimo implica, comunque, l'emissione di un nuovo certificato.
Durante il processo di emissione Bit4id:

- garantisce la riservatezza e l'integrità dei dati di registrazione forniti;
- utilizza sistemi e prodotti affidabili che siano protetti da qualsiasi alterazione possibile e che garantiscono la sicurezza, dal punto di vista tecnico, dei processi in cui vengono adoperati;
- produce una coppia di chiavi, tramite una procedura sicura di generazione;
- implementa un processo di generazione di certificati che collega in modo sicuro il certificato alle informazioni di registrazione, inclusa la chiave pubblica certificata;
- assicura che il certificato sia rilasciato da sistemi protetti da ogni possibile contraffazione e che garantiscono la riservatezza delle chiavi durante il processo di generazione di queste ultime;
- indica la data e l'ora in cui è stato emesso un certificato;
- garantisce il controllo esclusivo delle chiavi da parte dell'utente, di modo che terzi non possano detrarle o utilizzarle in alcun modo.

L'emissione del Certificato (di firma o di sigillo) con le modalità indicate potrà avvenire secondo le seguenti due differenti modalità:

1. Emissione del certificato su Smartcard/Token;
2. Emissione del certificato su dispositivo HSM (di firma remota).

Nei paragrafi che seguono (4.3.1.1. e 4.3.1.2) è descritto il flusso di emissione del certificato con le diverse modalità sopra indicate.

4.3.1.1. Emissione del certificato su Smartcard/Token

La modalità di emissione del certificato ai sensi del presente paragrafo prevede che l'emissione avvenga su un dispositivo sicuro per la generazione della firma. Bit4id mette a disposizione diverse tipologie di dispositivi QSCD per l'emissione dei certificati, che garantiscono i medesimi standard di sicurezza, mentre differiscono unicamente per le interfacce offerte: Smartcard, Token USB e DNA Key (con doppia interfaccia USB e *Bluetooth Low Energy*).

La generazione della coppia di chiavi crittografiche avviene, a cura della R.A. di riferimento, direttamente sul dispositivo sicuro di firma prescelto, tramite l'utilizzo di appositi programmi per elaboratore, forniti da Bit4id, che garantiscono adeguate misure di sicurezza.

In seguito, la RA invia a Bit4id la richiesta di certificazione, in formato PKCS#10, della chiave pubblica firmata digitalmente affinché quest'ultima, verificata la validità della firma e la provenienza della richiesta da soggetto a ciò autorizzato, genera il certificato qualificato, successivamente importato all'interno del dispositivo tramite canale sicuro.

L'emissione del certificato, secondo le modalità descritte nel presente paragrafo è prevista solo nell'ipotesi di identificazione *de visu* del Richiedente (v. 3.2.3.1 *infra*).

4.3.1.2. Emissione del certificato dispositivo HSM (firma remota)

La modalità di emissione del certificato ai sensi del presente paragrafo – emissione del certificato su dispositivo di firma remota - non prevede la consegna di un dispositivo fisico al titolare del certificato ma prevede, infatti che l'emissione avvenga su dispositivo HSM della CA.

In questo caso, la generazione della coppia di chiavi crittografiche avviene direttamente sull'HSM, a cura della RA, che invia a Bit4id la richiesta di certificazione, in formato PKCS#10 della chiave pubblica firmata digitalmente affinché quest'ultima, verificata la validità della firma e la provenienza della richiesta da soggetto a ciò autorizzato, genera il certificato qualificato, successivamente memorizzato.

Per la richiesta di apposizione della firma digitale con procedura automatica, l'utente utilizza un'applicazione *client* di firma fornita dal Certificatore o dalla propria organizzazione che eroga servizi applicativi ad utenti interni o esterni (es. impresa, istituto bancario, ente pubblico, ecc.). Le specifiche modalità per l'esecuzione della firma dipendono, quindi, dalla particolare applicazione usata dagli utenti.

La soluzione fornita dal Certificatore, basata su HSM, è composta da due componenti:

- la componente "*SignCloud*", responsabile della firma a basso livello degli *hash* dei documenti;

- il server "*SignBox*", ossia la componente capace di apporre le firme ad un alto livello di astrazione. Si integra con i sistemi dell'organizzazione ed esegue l'imbustamento nei vari formati supportati, comunicando con la componente *SignCloud* per la firma degli *hash* calcolati.

L'organizzazione si limita, dunque, ad effettuare l'integrazione tra i suoi sistemi e la componente SignBox, che stabilisce connessioni sicure sempre protette e, in conformità all'art. 42 comma 6 del DPCM 22 febbraio 2013, non consente al Certificatore di conoscere gli atti o fatti rappresentati nel documento informatico oggetto del processo di sottoscrizione.
La richiesta di firma proveniente dall'applicazione client è autenticata con username, password e PIN, e il certificato di firma automatica contiene le opportune limitazioni d'uso.

4.3.1.2.1. Componenti del servizio SSAS (firma remota)

L'emissione del certificato collega in modo sicuro la chiave pubblica certificata alle informazioni di registrazione validate. Per la firma remota, l'associazione tra certificato e chiave privata residente in HSM è mantenuta e protetta dai sistemi del QTSP, senza consegna della chiave privata al Titolare. L'uso della chiave privata è consentito esclusivamente previa attivazione tramite SAM certificato, che applica i controlli di autenticazione e autorizzazione. La combinazione SAM e HSM realizza il requisito di sole control.
L'operazione di firma remota è eseguita solo dopo attivazione tramite SAM, che valida l'identità/autenticazione del Titolare e la sua autorizzazione all'uso della chiave privata. L'HSM certificato esegue l'operazione crittografica in ambiente protetto e non esporta la chiave privata. Gli eventi di attivazione e l'esito dell'operazione sono registrati per finalità di audit e tracciabilità.

4.3.2. Emissione del certificato di TSU

La richiesta di certificato viene eseguita manualmente da un operatore di sistema che opera per conto di Bit4id ed è coinvolto nel processo di conduzione tecnica dei sistemi.

- L'operatore provvede alla generazione di una coppia di chiavi all'interno della partizione dell'HSM dedicata al servizio di marcatura temporale e, contestualmente, alla creazione della richiesta di certificato (CSR) in formato PKCS#10. Successivamente procede all'emissione del certificato di TSU tramite la TSA.

- Il certificato emesso viene quindi associato alla chiave precedentemente generata e installato sull'HSM, completando così la configurazione del servizio di marcatura temporale.

In conformità a quanto previsto dall'art. 49, comma 3, del DPCM 22 febbraio 2013, una volta emesso il certificato di marcatura temporale, le chiavi di marcatura temporale sono gestite in

conformità alle procedure interne di sicurezza di Bit4id, che garantiscono la corretta conservazione, rotazione e tracciabilità delle stesse, indipendentemente dal periodo di validità del certificato di TSU, che viene sostituito dopo non più di tre mesi di utilizzazione.

4.3.3. Notifica di emissione del certificato

Bit4id notifica l'emissione del certificato al Richiedente agli indirizzi da quest'ultimo forniti.

4.4. Consegna e accettazione del certificato

4.4.1. Responsabilità della R.A.

Il personale autorizzato dalla R.A. di Bit4id è tenuto a:

- verificare correttamente l'identità della persona fisica/giuridica identificata nel certificato, in conformità con le disposizioni delle sezioni 3;
- notificare l'emissione del certificato al Titolare, rendendo noto a quest'ultimo, almeno le seguenti informazioni:
  a) le informazioni di base sull'uso del certificato, il Manuale Operativo applicabile, i dati relativi alla CA, così come i suoi obblighi, facoltà e responsabilità;
  b) le informazioni sul certificato;
  c) evidenza della ricezione e accettazione da parte del Titolare dei dati associati all'uso del certificato;
  d) gli obblighi e responsabilità del Titolare;
  e) il metodo con cui viene garantito il controllo esclusivo, da parte del Titolare, della propria chiave privata o dei dati di attivazione della stessa secondo quanto stabilito nella sezione 6;
  f) la data dell'atto di consegna e accettazione del certificato.
- ottenere la firma del Richiedente così come identificato nel certificato.

Le R.A. sono responsabili dell'esecuzione di tali processi, sono tenute a conservare i documenti originali (fogli di consegna e accettazione), per le ipotesi in cui Bit4id abbia bisogno di accedervi e ad inviare una copia in formato digitale all'Organismo di vigilanza.

Tutti i documenti sopra indicati saranno conservati e archiviati, in formato elettronico, da Bit4id con garanzie di sicurezza e integrità per un periodo di almeno 20 anni decorrenti dalla data di scadenza del certificato di firma (ex art. 28 co. 4-bis D.Lgs. 7 marzo 2005 n. 82 e s.m.i.), anche al fine di fornire prova della certificazione in eventuali procedimenti dell'Autorità Giudiziaria e, comunque, non oltre il periodo stabilito dalla legge.

4.4.2. Processo di accettazione del certificato

L'accettazione del certificato da parte della persona fisica o della persona giuridica identificata nel certificato viene effettuata firmando il modulo di consegna e accettazione.

4.4.3. Notifica dell'emissione a terzi

Bit4id non notificherà alcuna emissione del certificato a favore di terzi diversi dal titolare.

4.5. Uso della coppia di chiavi e del certificato

4.5.1. Utilizzo da parte del Richiedente e/o Titolare

Il Titolare del certificato è tenuto a:

- leggere ed accettare integralmente il contenuto del presente documento prima di richiedere il certificato;
- fornire alla CA informazioni esatte, complete e veritiere in fase di richiesta del certificato;
- esprimere il suo consenso preventivamente all'emissione e alla consegna di un certificato;
- utilizzare la propria chiave privata e il proprio certificato unicamente per gli scopi previsti dal presente documento;
- adottare misure di sicurezza atte a prevenire l'uso non autorizzato della propria chiave privata;
- assicurare la confidenzialità dei codici riservati ricevuti dalla CA;
- richiedere tempestivamente alla CA la revoca del certificato nel caso di sospetta compromissione della propria chiave privata;
- nel caso di accertata compromissione della propria chiave privata, richiedere tempestivamente alla CA la revoca del certificato;
- prima di cominciare ad utilizzare la chiave privata, controllare attentamente che il corrispondente certificato ottenuto da Bit4id abbia il profilo previsto e contenga informazioni corrette, incluse le eventuali limitazioni d'uso;
- fino alla data di scadenza o di eventuale revoca del proprio certificato, informare prontamente la CA o la RA nel caso in cui: il proprio dispositivo di firma sia andato perso, sia stato sottratto o si sia danneggiato; abbia perso il controllo esclusivo della propria chiave privata, per esempio a causa della compromissione dei dati di attivazione (PIN o password) della propria chiave privata di firma; alcune informazioni contenute nel certificato siano inesatte o non più valide;

- nel caso di compromissione della propria chiave privata (per esempio, a causa dello smarrimento del PIN o della sua rivelazione a terzi non autorizzata), cessare immediatamente l'utilizzo della stessa ed assicurarsi che non venga più utilizzata: in tale situazione la CA revoca immediatamente il certificato.

A seguito della richiesta del certificato il Titolare assume consapevolmente le seguenti responsabilità affinché:

- tutte le informazioni fornite contenute nel certificato siano corrette;
- il certificato sia utilizzato esclusivamente per usi legali e autorizzati, in conformità con il presente Manuale Operativo;
- nessuna persona non autorizzata abbia accesso alla chiave privata del certificato, assumendosi, inoltre, l'esclusiva responsabilità per i danni causati dalla mancata protezione della chiave privata;
- non cedere o concedere in uso in nessuna circostanza la chiave privata (trattandosi di un elemento strettamente personale) a terzi.

4.5.2. Utilizzo da parte delle Relying Parties

4.5.2.1. Obblighi delle Relying Parties

Tutti coloro che fanno affidamento sulle informazioni contenute nei certificati (R.P., termine abbreviato per indicare le Relying Parties), in ossequio a quanto disciplinato dal requisito OVR-6.3.5-03 delle norme ETSI EN 319 411-1/411-2 per i certificati di firma e sigillo hanno l'obbligo di:

- Verificare che il certificato non sia scaduto;
- verificare lo stato di validità del certificato, vale a dire la sua eventuale revoca utilizzando le informazioni correnti sullo stato di revoca. La convalida deve essere effettuata tenendo in considerazione lo stato del certificato alla data-ora rilevante per la RP, secondo il particolare contesto (es. data-ora corrente, data-ora di apposizione della firma nel caso in cui essa possa essere dimostrabile attraverso una marca temporale apposta al documento);
- tenere conto di eventuali limitazioni all'uso del certificato;
- prendere qualsiasi precauzione così come prescritto negli accordi o altrove.

Per la marca temporale, in ossequio a quanto disciplinato dal requisito OVE-6.6-01 della norma ETSI EN 319 421 hanno l'obbligo di:

- verificare che la marca temporale sia stata correttamente firmata e che la chiave privata utilizzata per firmare la marca temporale non sia stata compromessa fino al momento della verifica;
- verificare lo stato di validità del certificato, vale a dire la sua eventuale revoca utilizzando le informazioni correnti sullo stato di revoca. La convalida deve essere effettuata tenendo

in considerazione lo stato del certificato alla data-ora rilevante per la RP, secondo il particolare contesto (es. data-ora corrente, data-ora di apposizione della firma nel caso in cui essa possa essere dimostrabile attraverso una marca temporale apposta al documento);
- tenere conto di eventuali limitazioni all'uso del certificato;
- prendere qualsiasi precauzione così come prescritto negli accordi o altrove.

All'interno dell'Allegato "A" al presente Manuale è presente il link, insieme al relativo manuale, dell'applicativo messo a disposizione da Bit4id al fine di consentire alle Relying Parties la verifica dei certificati.
Le Relying Parties possono, inoltre, utilizzare gli indicatori e le disposizioni di cui al presente manuale per determinare l'idoneità e l'affidabilità dei certificati nel quadro del Regolamento (UE) n. 910/2014.

4.5.2.2. Responsabilità civile delle Relying Parties

Tutti coloro che fanno affidamento sulle informazioni contenute nei certificati sono responsabili quanto a:
- disporre di informazioni sufficienti per prendere decisioni in merito all'affidabilità di un certificato;
- accettare la veridicità delle informazioni contenute nel certificato;
- rispettare gli obblighi gravanti su di sé come Relying Parties, secondo quanto disposto nel precedente paragrafo.

4.5.3. Limiti d'uso e di valore

Bit4id, in conformità alla Determinazione n. 147/2019 di AgID recante "Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate" garantisce i limiti di uso di cui al Par. 3.1.6. ed informa i Richiedenti circa le seguenti ulteriori limitazioni di uso, specificate nei certificati mediante l'attributo *userNotice* dell'estensione *CertificatePolicies* o tramite *Policy* OID dedicati:

a) I certificati digitali qualificati emessi in seguito ad identificazione del Richiedente con le modalità di cui al Par. 3.2.2.6 – "Procedura di identificazione tramite identità SPID" contengono l'OID 1.3.76.16.5 il seguente limite di uso:
    1) IT: "*Il certificato emesso tramite il Sistema Pubblico di Identità Digitale (SPID) non è utilizzabile per richiedere un'altra Identità Digitale (SPID)*";
    EN: "*Certificate issued through Sistema Pubblico di Identità Digitale (SPID) is not usable to require another SPID digital identity*";

b) I certificati digitali qualificati della tipologia "*OneShot*" di cui al Par. 1.4.1.2. contengono almeno uno dei seguenti limiti di uso:

1) IT: "*Il presente certificato è rilasciato per un utilizzo singolo ed è valido esclusivamente nell'ambito dello specifico flusso applicativo per il quale è stato generato.*".
   EN: *"This certificate is issued for single use and is valid exclusively within the specific application workflow for which it has been generated.*".
2) IT: "*L'utilizzo del certificato è limitato esclusivamente alla sottoscrizione dei documenti cui la firma è apposta e, comunque, limitatamente ai rapporti tra il sottoscrittore e (inserire soggetto)*";
   EN: "*The use of the certificate is limited exclusively to the signature of the underlying document and, in any case, limited to the relationships between the subscriber and (insert subject name)*".

c) I certificati digitali qualificati della tipologia "*automatica*" contengono il seguente limite di uso (user Notice):

1) IT: "*Il presente certificato è valido solo per firme apposte con procedura automatica*."
2) EN: "*The certificate may only be used for unattended/automatic digital signature*."

Fatti salvi i casi di responsabilità della CA normativamente previsti (v. art. 30 co. 1 del CAD) il Titolare è tenuto alla verifica dei limiti di uso e di valore inseriti nel certificato nonché alla loro scrupolosa osservanza.
Specifici limiti d'uso potranno essere concordati per meglio descrivere e/o delimitare l'ambito di applicazione nel dominio della specifica RA.
La mancata osservanza, da parte del Titolare, dei limiti di uso del certificato non determina e non potrà determinare il sorgere di qualsivoglia responsabilità in capo alla CA (per ulteriori informazioni sui diritti e gli obblighi del Titolare e della CA si rimanda al Capitolo 9 del presente Manuale).

4.6. Rinnovo di chiavi e certificati

4.6.1. Cause di rinnovo di chiavi e certificati

I certificati di firma o di sigillo elettronico non ancora scaduti e non revocati possono essere rinnovati attraverso una procedura specifica.
Questa consiste nella generazione di una nuova coppia di chiavi (da parte del Richiedente attraverso appositi strumenti messi a disposizione da Bit4id) ed emissione di un nuovo certificato con:

- periodo di validità uguale al periodo di validità del certificato in scadenza
- con gli stessi dati identificativi del Titolare.

Il rinnovo non richiede una nuova identificazione del Titolare e pertanto può essere condotto in autonomia anche da quest'ultimo attraverso l'utilizzo di appositi software messi a disposizione da Bit4id.

4.6.2. Procedura di rinnovo

Il Richiedente può richiedere un rinnovo del certificato nel caso in cui i dati identificativi non siano cambiati o, comunque, nel caso in cui il ciclo di vita del certificato è prossimo alla scadenza.
Il titolare firma la richiesta di rinnovo con il certificato in suo possesso ancora in corso di validità. Non possono essere, infatti, rinnovati certificati precedentemente sospesi o revocati.
Qualora, nel Certificato qualificato, dovessero essere presenti anche informazioni relative al ruolo e all'organizzazione cui il Richiedente fa parte, la CA provvederà ad inserirle nel nuovo certificato verificando, al momento del rinnovo.
L'avvenuto rinnovo del certificato sarà notificato a cura della CA al Richiedente mediante posta elettronica all'ultimo indirizzo e-mail comunicato.
Il Richiedente che abbia ricevuto il nuovo certificato non potrà più utilizzare la Chiave privata relativa al vecchio certificato.
Una volta scaduto o revocato, il certificato non può più essere riemesso ma è necessaria una emissione *ex novo* del certificato con le medesime modalità descritte per l'emissione del primo (v. par. 4.1, 4.2 e 4.3).

La procedura di rinnovo non si applica ai certificati di tipo *One-Shot*.

4.7. Key Changeover (re-key dei certificati)

Bit4id non ammette in nessuna circostanza il *rekeying* del certificato.

4.8. Modifica dei certificati

La modifica dei certificati, applicabile nei casi in cui variano le informazioni identificative del Titolare (ad eccezione della modifica della chiave pubblica che si effettua nel caso di rinnovo) sarà gestita come un'emissione ex novo, applicando quanto descritto nella sezione 4.

4.9. Revoca e sospensione di un certificato

La revoca e la sospensione di un certificato comportano la cessazione della sua validità. La revoca comporta la cessazione anticipata e definitiva della validità del certificato. È pertanto una condizione irreversibile che non consente la riattivazione del certificato.
La sospensione comporta l'interruzione momentanea della validità di un certificato e consente la successiva riattivazione oppure la revoca definitiva.

La revoca o sospensione del certificato si materializzano con l'inserimento del numero di serie del certificato all'interno della CRL – *Certificate Revocation List*, vale a dire una lista dei certificati revocati.

Questa viene pubblicata da parte di Bit4id per consentire agli interessati la consultazione necessaria alla determinazione dello stato di validità dei certificati emessi da Bit4id.

Con la stessa finalità, Bit4id rende disponibile la stessa informazione mediante il protocollo OCSP.

Le operazioni di revoca e sospensione non possono essere richieste per i certificati di tipo *One-Shot*.

4.9.1. Ipotesi di revoca di un certificato

Bit4id revoca un certificato quando si presenta una delle seguenti cause (elenco non esaustivo):

1. **circostanze che influenzano le informazioni contenute nel certificato:**
   a) modifica di alcuni dei dati contenuti nel certificato, successivamente all'emissione del certificato corrispondente;
   b) prova della non correttezza dei dati contenuti nella richiesta di certificato;
2. **circostanze che influiscono sulla sicurezza della chiave o del certificato:**
   a) compromissione della chiave privata, dell'infrastruttura o dei sistemi della CA, a condizione che ciò influisca sull'affidabilità dei certificati rilasciati;
   b) violazione dei requisiti previsti nelle procedure di gestione dei certificati, stabiliti nel presente Manuale Operativo;
   c) sospetto o prova di compromissione della sicurezza della chiave o del certificato emesso;
   d) accesso o uso non autorizzato, da parte di terzi, della chiave privata corrispondente alla chiave pubblica contenuta nel certificato;
   e) uso improprio del certificato da parte della persona fisica identificata nel certificato o mancanza di diligenza nella custodia della chiave privata.
3. **circostanze che riguardino il Richiedente e/o il Titolare:**
   a) cessazione del contratto tra la CA e il Richiedente e/o il Titolare;
   b) modifica o risoluzione anticipata del contratto tra la CA e il Richiedente e/o il Titolare;
   c) violazione da parte del Richiedente il certificato dei requisiti prestabiliti per la sua richiesta;
   d) violazione da parte del Richiedente e/o del Titolare degli obblighi contrattuali;
   e) incapacità sopravvenuta del Richiedente e/o Titolare;

f) richiesta esplicita di revoca del certificato da parte del Titolare e/o del suo rappresentante, per qualsiasi motivo, conformemente alle disposizioni della sezione 3.

4. **altre circostanze:**
   a) cessazione del servizio di certificazione da parte dell'Autorità di certificazione Bit4id;
   b) utilizzo del certificato non conforme e pregiudizievole per Bit4id, specie in modo continuativo;
   c) provvedimento dell'Autorità giudiziaria.

In questo caso, un utilizzo è considerato dannoso in base ai seguenti criteri:

- la natura e il numero di reclami ricevuti;
- l'identità dei soggetti che presentano i reclami;
- la legislazione applicabile;
- la risposta fornita dal Richiedente rispetto ai reclami ricevuti.

4.9.2. Chi può richiedere la revoca

Può domandare la revoca del certificato il Titolare, nonché, nei casi in cui sia presente, il Terzo Interessato attraverso l'intervento dell'Operatore di registrazione con le modalità appresso indicate, oltre che da Bit4id laddove venisse ravvisata detta necessità.
Inoltre, la revoca può essere richiesta dall'Autorità Giudiziaria e tali segnalazioni, vista la specifica identità del segnalatore, saranno trattate con maggiore priorità rispetto alle altre.

4.9.3. Procedura di revoca

Il soggetto che richiede la revoca di un certificato può farlo rivolgendosi direttamente a Bit4id ovvero alla R.A. ovvero, in prima persona, attraverso il servizio online disponibile sulla pagina web di Bit4id. La richiesta di revoca dovrà includere le informazioni seguenti:

- data della richiesta di revoca;
- dati identificativi del Richiedente;
- recapiti della persona che chiede la revoca;
- motivazione dettagliata relativa alla richiesta di revoca.

La richiesta può essere presentata dal Titolare o dal terzo interessato (ove presente) direttamente a Bit4id tramite l'invio di una PEC all'indirizzo bit4id-tsp@sicurezzapostale.it, allegando l'apposito modulo "Modulo di richiesta sospensione, riattivazione e revoca dei certificati digitali" debitamente compilato, scaricabile dal sito https://www.bit4id.com/documentazione-qtsp, o presentandosi presso una delle R.A.

La R.A. o la C.A. hanno la facoltà di richiedere documentazione integrativa al modulo, al fine di poter effettuare l'operazione richiesta.
Prima di procedere alla revoca, la richiesta deve essere validata da Bit4id, in accordo con i requisiti stabiliti nel paragrafo 3 di questo Manuale.
Il servizio di revoca è disponibile esclusivamente ai Titolari al sito web di Bit4id all'indirizzo https://www.bit4idtsp.com/lcm/.
In seguito all'elaborazione della richiesta di revoca, il cambio di stato del certificato verrà notificato al Richiedente.
Il servizio di revoca è considerato un servizio critico, incluso nel piano di emergenza e di continuità operativa di Bit4id.

4.9.4. Periodo di grazia della richiesta di revoca

Bit4id esegue la revoca con la massima tempestività e attenzione, garantendo che il tempo necessario per l'elaborazione dell'operazione di revoca o sospensione e il conseguente aggiornamento dello stato del certificato (effettuato tramite pubblicazione di una nuova lista di revoca CRL) sia il più ridotto possibile.

4.9.5. Durata dell'elaborazione della richiesta di revoca

Se effettuata per mezzo di un Operatore, la richiesta di revoca sarà elaborata entro il consueto orario d'ufficio di Bit4id o laddove applicabile dalla R.A. che ha proceduto all'emissione del certificato. Se effettuata online, avrà effetto immediato.
In caso di ricezione da parte di Bit4id di una richiesta di revoca, questa viene processata immediatamente, al più entro le 24 ore lavorative, per ridurre al minimo il tempo dopo il quale la revoca diventa effettiva (che coincide con la pubblicazione del certificato in una nuova CRL).
Il certificato revocato viene inserito nella CRL entro 1 ora dalla revoca e comunque in nessuna circostanza oltre le 24 ore successive all'operazione.
Lo stato del certificato può essere in ogni caso verificato in tempo reale tramite il servizio OCSP.

4.9.6. Verifica delle informazioni relative alla revoca dei certificati

Tutti coloro che devono fare affidamento sulle informazioni contenute nei certificati (c.d. "Relying Parties") hanno l'obbligo, prima di accettare un certificato, di verificare che quest'ultimo non sia scaduto alla data della verifica e che sia valido alla medesima data.
Un metodo per effettuare tale verifica è consultare la Lista di Revoca dei certificati (CRL) più recente emessa da Bit4id.
Le Liste di Revoca dei Certificati sono pubblicate ai seguenti indirizzi (URL):

- http://crl.bit4idtsp.com/qc-oneshot-ecc-256-g1.crl

- http://crl.bit4idtsp.com/qc-ecc-256-g1.crl
- http://crl.bit4idtsp.com/qc-rsa-4096-g1.crl
- http://crl.bit4idtsp.com/tsa-ecc-256-g1.crl
- http://crl.bit4idtsp.com/tsa-rsa-4096-g1.crl

I suddetti indirizzi sono riportati in ciascuno dei certificati emessi da Bit4id, nella sezione "CRL Distribution Point".

La verifica, inoltre, può essere compiuta mediante interrogazione del servizio OCSP erogato da Bit4id al seguente indirizzo: http://ocsp.bit4idtsp.com

4.9.7. Frequenza di emissione della CRL

Bit4id emette una nuova CRL ogni ora con una validità di 24h (ventiquattro ore) e, indipendentemente dalla presenza o meno di nuove richieste di revoca.

4.9.8. Pubblicazione delle CRL

Le CRL vengono pubblicate immediatamente dopo essere state create. La latenza tra l'istante della creazione della CRL e quello della sua pubblicazione in nessuna circostanza supera i 5 minuti.

4.9.9. Disponibilità dei servizi di verifica on-line della revoca

Bit4id rende disponibile, in aggiunta alla pubblicazione delle CRL, un servizio di verifica on-line dello stato dei certificati basato sul protocollo OCSP (RFC 6960) (v. allegato A *infra*)

Il servizio OCSP è accessibile 7x24.

In caso di malfunzionamento dei sistemi di verifica dei certificati, Bit4id si impegna ad assicurare che il servizio rimanga inattivo il minor tempo possibile. In ogni caso il tempo di indisponibilità del servizio di verifica online della revoca non potrà superare le 6 ore.

4.9.10. Altre forme disponibili di pubblicazione della revoca

Non è prevista nessuna ulteriore modalità di pubblicazione della revoca a parte di quelle previste nella sezione 4.9.

4.9.11. Condizioni speciali in caso di compromissione/corruzione della chiave privata

Non previste.

4.9.12. Circostanze per la sospensione

La sospensione del certificato di firma elettronica qualificata è prevista nelle seguenti circostanze:

1. circostanze che influenzano le informazioni contenute nel certificato:

2. sospetta non correttezza dei dati contenuti nella richiesta di certificato;
3. circostanze che influiscono sulla sicurezza della chiave o del certificato;
4. sospetta violazione dei requisiti previsti nelle procedure di gestione dei certificati, stabiliti nel presente Manuale Operativo;
5. sospetto accesso o uso non autorizzato, da parte di terzi, della chiave privata corrispondente alla chiave pubblica contenuta nel certificato;
6. sospetto uso improprio del certificato da parte della persona fisica identificata nel certificato o mancanza di diligenza nella custodia della chiave privata;
7. circostanze che riguardino il Richiedente e/o il Titolare.

La sospensione per i certificati di TSU non è prevista in nessun caso.

4.9.13. Chi può richiedere la sospensione

Può domandare la sospensione del certificato il Richiedente, nonché, ove presente, il Terzo Interessato attraverso l'intervento dell'Operatore di registrazione con le modalità appresso indicate, oltre che da Bit4id laddove venisse ravvisata detta necessità.

4.9.14. Procedura per la sospensione

Ai sensi dell'art. 26 delle Regole Tecniche di cui al DPCM 22 febbraio 2013 la sospensione dei certificati qualificati è effettuata dalla CA mediante l'inserimento del Codice identificativo in una delle liste dei certificati revocati e sospesi (CRL).

Ai sensi del comma 3 dell'art. 26 sopra citato, Bit4id ha fissato la durata massima del periodo di sospensione dei certificati qualificati in 90 (novanta) giorni; al termine del periodo di sospensione, senza che sia intervenuta indicazione contraria da parte del Titolare, Bit4id provvederà alla revoca del certificato.

Per la restante parte, la procedura di sospensione si effettua in maniera equivalente a quanto avviene per la revoca, così come descritto nel paragrafo 4.9.3.

In ogni caso, la sospensione della validità di un certificato digitale, così come la cessazione della stessa, è annotata, ai sensi dell'art. 26 co. 5 delle Regole Tecniche (DPCM 22 febbraio 2013) nel giornale di controllo con indicazione della data e dell'ora di esecuzione dell'operazione (per maggiori informazioni sulla gestione del giornale di controllo v. par. 5.4.2. e ss.).

4.10. Servizi informativi sullo stato del certificato

Lo stato dei certificati qualificati è messo a disposizione attraverso la pubblicazione della CRL mediante protocollo HTTP ed in formato conforme alla 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. L'indirizzo delle CRL è inserito nell'estensione *CRLDistributionPoints*.
L'indirizzo del server OCSP viene inserito nell'estensione *AuthorityInformationAccess*.
I Servizi sono ad accesso pubblico.

4.11. Cessazione del contratto

Il contratto tra la CA e il Titolare si intende cessato alla scadenza o alla revoca del certificato, salvo il caso di eventuali condizioni diverse previste nei contratti stipulati con alcuni clienti.
Il rinnovo del certificato determina la continuità della prestazione contrattuale da parte della CA.

4.12. Key escrow e recupero della chiave privata

4.12.1. Politica e servizi di deposito e recupero delle chiavi

Nell'ambito del servizio di certificazione qui descritto, il "*key escrow*" delle chiavi dei Titolari non è previsto. Non è dunque possibile il recupero della chiave privata del Titolare ("*key recovery*") in nessuna circostanza.
Per quanto riguarda le chiavi di CA e di TSA, il recupero è invece previsto in circostanze di emergenza (es: guasto degli apparati HSM). Il ripristino viene condotto seguendo le procedure previste dall'HSM utilizzato.

4.12.2. Politica e servizi sui contenuti e recupero chiavi di sessione

Nessuna disposizione.

5. MISURE DI SICUREZZA FISICA E OPERATIVA

5.1. Sicurezza fisica

Bit4id ha implementato un sistema di sicurezza relativo al sistema informativo del servizio di certificazione digitale caratterizzato da misure di sicurezza fisica finalizzate alla protezione dell'infrastruttura e dei sistemi di elaborazione utilizzati a supporto dei servizi fiduciari prestati.
In tale contesto, viene assicurato:

- controllo degli accessi fisici;
- protezione contro disastri naturali (es. inondazioni);
- continuità di alimentazione elettrica;
- connettività ad Internet ridondata (doppia linea);
- sistemi antincendio ed antiallagamento;
- protezione antifurto;
- ventilazione e condizionamento ottimali;
- adozione di una politica relativa alla fuoriuscita, non autorizzata, di materiale, informazioni, supporto e ogni ulteriore applicazione relativa a componenti impiegati per i servizi fiduciari e di CA.

Il costante monitoraggio dell'infrastruttura e dei servizi ovvero il tempestivo intervento in caso di necessità è garantito da personale sistemistico qualificato che opera 24h-365 giorni l'anno e assicura assistenza nelle 24 ore che seguono la segnalazione.
Bit4id, attraverso Uanataca, si avvale dei servizi di data center e servizi di comunicazione associati (quali *housing*, connettività alla rete Internet, sicurezza fisica) offerti dalla società ADAM con la quale ha stipulato apposito contratto di servizio.
Detti servizi sono certificati secondo le norme:
- ISO/IEC 27001:2022
- ISO 9001:2015
Il Datacenter è ubicato all'indirizzo: C/ del Artesans, 7 – 08290 Cerdanyola de Vallés, Barcellona (Spagna).

5.1.1. Localizzazione e implementazione delle strutture

La protezione delle infrastrutture che consentono l'erogazione dei servizi di certificazione viene assicurata mediante la creazione di perimetri di sicurezza, chiaramente definiti ed individuabili.
Le installazioni sono ubicate in zone a basso rischio di disastri naturali (bassissimo livello di rischio sismico, rischio vulcanico assente, basso rischio di alluvioni).

La qualità e solidità dei materiali di costruzione delle installazioni garantisce livelli di protezione adeguati contro tentativi di intrusione forzate e permette un rapido accesso per eventuali azioni di emergenza.
La sala dove si realizzano le operazioni di crittografia nel Centro di Elaborazione Dati vanta infrastrutture con elevatissimi requisiti tecnologici, così come varie fonti alternative di elettricità e raffreddamento in caso di emergenza.
Bit4id dispone di strutture che proteggono fisicamente gli ambienti in cui vengono effettuate le operazioni proprie dell'erogazione di servizi fiduciari.

5.1.2. Accesso fisico

I Fornitori hanno realizzato un sistema di sicurezza fisica articolato su tre livelli:

- accesso all'edificio dove si trova il CED;
- accesso alla sala;
- accesso al rack

per la protezione dei servizi fiduciari erogati.
L'accesso fisico ai locali dove avvengono i processi di certificazione è protetto attraverso una combinazione di misure fisiche e procedurali.
Tale accesso, in particolare:

- è limitato al personale espressamente autorizzato, con autenticazione all'accesso, registrazione, ripresa video a circuito chiuso e archiviazione;
- si realizza con lettori di badge ed è gestito da un sistema informatico con tracciamento (e relativa generazione di evidenze e log) di ingresso e uscita.

Inoltre, l'accesso al rack dove sono ubicati i moduli crittografici e il "core" dell'infrastruttura avviene esclusivamente previa autorizzazione da parte della Direzione di Uanataca ovvero del Responsabile della Sicurezza.
Bit4id identifica i fornitori ai fini dell'erogazione dei suddetti servizi assicurando che i controlli per la sicurezza, le definizioni di servizio e i livelli di erogazione inclusi negli
accordi di erogazione di servizi di terze parti, siano attuati, condotti e mantenuti attivi.

5.1.3. Elettricità ed aria condizionata

Le strutture nell'ambito delle quali viene svolto, il servizio di certificazione dispongono di attrezzature per stabilizzare la corrente e di un sistema di alimentazione elettrica supportato da un gruppo elettrogeno.
I locali che accolgono le attrezzature informatiche dispongono di sistemi di controllo della temperatura con aria condizionata.

5.1.4. Esposizione all'acqua

I macchinari si trovano in una zona a basso rischio di inondazione.
Le sale dove si trovano le apparecchiature informatiche dispongono di un sistema di rilevamento dell'umidità.

5.1.5. Prevenzione e protezione antincendio

Le attrezzature e il materiale hanno un sistema automatico di individuazione ed estinzione di incendi.

5.1.6. Dispositivi di archiviazione

Solo il personale autorizzato ha accesso ai dispositivi di archiviazione.
Le informazioni di livello superiore sono custodite in una cassaforte fuori le strutture del Centro Elaborazione Dati.

5.1.7. Smaltimento dei rifiuti

L'eliminazione dei materiali, cartacei e magnetici, si effettua attraverso meccanismi che garantiscono l'impossibilità di recupero delle informazioni.
Nel caso di materiale magnetico, questo viene fisicamente distrutto o riutilizzato dopo aver provveduto alla cancellazione sicura del contenuto.
In caso di documentazione cartacea, la cancellazione delle informazioni avviene attraverso macchine trita-documenti o cestini che vengono successivamente distrutti sotto stretto controllo.

5.1.8. Copia di riserva esterna alle strutture

Per Bit4id, i Fornitori utilizzano un archivio esterno sicuro per la custodia dei documenti, dispositivi magnetici ed elettronici indipendenti dal Centro operativo.

5.2. Controlli sulle procedure e sicurezza operativa

Bit4id garantisce che i suoi sistemi operino in maniera sicura, pertanto ha stabilito e introdotto procedure che stabiliscano in maniera rigorosa la prestazione dei suoi servizi.
Il personale addetto di Bit4id esegue le procedure amministrative e di gestione in accordo con la politica di sicurezza stabilita da Bit4id e da Uanataca, quale fornitore della soluzione PKIaaS.

5.2.1. Ruoli di fiducia

In ottemperanza alle disposizioni dell'articolo 38 comma 1 del 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", Bit4id ha nominato internamente all'organizzazione le seguenti figure:

- **Responsabile della sicurezza**: incaricato di coordinare, controllare e far applicare le misure di sicurezza definite nella politica sulla sicurezza di Bit4id. Questi deve incaricarsi degli aspetti relativi alla sicurezza dell'informazione: logistica, fisica, di rete, organizzativa, etc.;
- **Responsabile delle verifiche e delle ispezioni (auditing)**: responsabile dello svolgimento delle procedure operative. È inoltre responsabile della verifica degli archivi e dei log di audit dei sistemi di CA;
- **Responsabile della conduzione tecnica dei sistemi**: responsabile dell''installazione, della configurazione, della manutenzione e del corretto funzionamento dei sistemi preposti all'erogazione dei servizi fiduciari;
- **Responsabile del servizio di certificazione e validazione temporale**;
- **Responsabile dei servizi tecnici e logistici**;

Inoltre, in ottemperanza alle disposizioni definite al REQ 7-14 dello Standard ETSI EN 319 401, sono state previste le seguenti ulteriori figure:

Amministratore di sistema (System Administrator): soggetto incaricato di gestire e manutenere il sistema informatico dell'organizzazione e di attenersi alle prescrizioni del Garante per la Protezione dei Dati Personali fornite nel relativo provvedimento oltre ai compiti già affidatogli dal Titolare del Trattamento e sempre e comunque nel pieno rispetto dell'art. 32 del GDPR sulla sicurezza del trattamento dei dati personali;

Operatore di sistema (System Operator): responsabile della quotidiana operatività del corretto funzionamento dei sistemi preposti all'erogazione dei servizi fiduciari;

Auditor di sistema (System Auditor): autorizzato a visualizzare archivi e audit log dei sistemi affidabili del TSP, ai fini delle attività di verifica e controllo.

Security Officer: con la responsabilità complessiva per l'amministrazione dell'implementazione delle pratiche di sicurezza del Qualified Trust Service Provider (QTSP).

Operatore di registrazione: responsabile dell'approvazione delle richieste di emissione di un certificato inoltrate dal Richiedente e/o Titolare; responsabile della verifica delle informazioni necessarie e dell'applicazione delle procedure definite da Bit4id per l'emissione di certificati digitali ovvero per l'erogazione di servizi fiduciari;

Le persone che rivestono i ruoli sopra elencati sono soggette a procedure di controllo e di sicurezza specifiche. La suddivisione dei ruoli, inoltre, secondo criteri definiti nel contesto organizzativo di Bit4id, costituisce una misura atta a prevenire la commissione di attività fraudolente.

5.2.2. Numero di persone per attività

Bit4id, con il supporto del partner tecnologico, garantisce almeno due persone per realizzare le attività relative alla generazione, al recupero e al back-up della chiave privata dell'Autorità di Certificazione.

5.2.3. Identificazione e autenticazione per i diversi ruoli

Le persone assegnate ad ogni ruolo sono identificate dall'auditor interno che si assicurerà che ogni persona effettui le operazioni che le sono state assegnate.
Ogni addetto verifica unicamente le attività relative al proprio ruolo, assicurandosi così che nessuno acceda alle risorse che non gli sono state assegnate.
L'accesso alle risorse avviene a seconda dell'attività attraverso nome utente/codice, certificato digitale, badge e/o chiave. con il supporto del partner tecnologico, garantisce almeno due persone per realizzare le attività relative alla generazione, al recupero e al back-up della chiave privata dell'Autorità di Certificazione.

5.2.4. Mansioni che richiedono separazione di compiti

Le seguenti mansioni sono effettuate almeno da due persone:

- i compiti dell'Auditor interno sono incompatibili con quelli relativi all'amministrazione di sistemi e, in generale, con le operazioni correlate all'implementazione dei servizi elettronici fiduciari;
- i compiti relativi all'emissione e revoca di certificati sono incompatibili con quelli concernenti l'amministrazione dei sistemi.

5.2.5. Sistema di gestione PKI

Il sistema di PKI si compone dei seguenti moduli:

- componente/modulo di gestione dell'Autorità di Certificazione;
- componente/modulo di gestione dell'Ufficio di Registrazione;
- componente/modulo di gestione delle richieste;
- componente/modulo di gestione delle chiavi (HSM);
- componente/modulo di database;
- componente/modulo di gestione di CRL;
- componente/modulo di gestione dell'Autorità di Validazione.

5.3. Sicurezza del personale

5.3.1. Qualifica, esperienza ed autorizzazioni richieste

Il personale di Bit4id, analogamente a quello di propri partner tecnologici, altamente qualificato e/o è stato debitamente formato per effettuare le operazioni che gli sono state assegnate.

Il personale con ruolo di fiducia non ha interessi personali che entrino in conflitto con lo svolgimento del ruolo che gli è stato affidato.

Bit4id si assicura che il personale addetto alla registrazione sia affidabile per la realizzazione dei compiti di registrazione. Il responsabile della registrazione riceve informazioni per svolgere le mansioni di convalida delle richieste.

In generale Bit4id solleverà dall'incarico di fiducia un impiegato se a conoscenza dell'esistenza di conflitti di interessi e/o della commissione di un qualsiasi atto illecito avente effetto sullo svolgimento delle sue funzioni.

Bit4id non assegnerà una mansione confidenziale o di gestione a una persona non ritenuta idonea. Per questo motivo, nei limiti della legislazione vigente, un'indagine preliminare verrà effettuata relativamente ai seguenti aspetti:

- studi, incluso i titoli da allegare;
- lavori effettuati precedentemente all'incarico (fino a cinque anni prima);
- referenze professionali.

In ogni caso, le RA, essendo responsabili delle persone da esse autorizzate allo svolgimento delle attività che gli sono normalmente proprie, potranno stabilire procedure ulteriori per l'accertamento dei requisiti di cui sopra, sempre nel rispetto della politica di Bit4id.

5.3.2. Procedure di verifica delle informazioni relative al personale

Bit4id, prima di assumere una persona o consentirgli l'accesso al posto di lavoro, compie accertamenti relativi ai seguenti aspetti:

- referenze sui lavori effettuati negli ultimi anni;
- referenze professionali;
- studi, incluso titoli allegati.

Bit4id ottiene, preliminarmente allo svolgimento di tali accertamenti, il consenso espresso dell'interessato, impegnandosi a trattare e proteggere i dati personali di tali soggetti, nel rispetto della normativa vigente in materia di protezione dei dati personali, di cui al Regolamento Europeo 679/2016 (GDPR) e alla normativa nazionale vigente in materia.

Tutte le verifiche vengono svolte nel rispetto della legislazione vigente.

I motivi che possono indurre a rifiutare il candidato per la copertura di un incarico di fiducia sono i seguenti:

- dichiarazioni false compiute dal candidato nel curriculum vitae;
- referenze professionali molto negative e/o poco affidabili.

5.3.3. Requisiti di formazione

Bit4id forma adeguatamente il personale destinato ad incarichi di fiducia e di gestione, fino al raggiungimento della qualifica da ricoprire, conservando traccia della suddetta formazione.
I programmi di formazione sono rivisti, aggiornati e migliorati periodicamente ed includono almeno i contenuti seguenti:

- principi e meccanismi di sicurezza della gerarchia di certificazione;
- mansioni che deve svolgere la persona;
- politiche e procedimenti di sicurezza di Bit4id;
- utilizzo e interventi su macchinari e applicazioni installate;
- gestione e risoluzione di incidenti e compromissioni della sicurezza;
- continuità aziendale e procedure di emergenza;
- procedure di gestione e sicurezza in relazione al trattamento dei dati a carattere personale.

5.3.4. Requisiti e frequenza dei corsi di aggiornamento

Specialmente quando vengono effettuate modifiche sostanziali alle mansioni relative ai servizi di certificazione, Bit4id provvede ad aggiornare il proprio personale in maniera accurata e soddisfacente. I corsi di formazione vengono erogati

5.3.5. Rotazione delle mansioni

Non applicabile.

5.3.6. Sanzioni per azioni non autorizzate

Bit4id mette in atto procedure disciplinari nelle ipotesi in cui sia necessario stabilire le responsabilità derivanti da azioni non autorizzate, nei limiti ed in conformità alle norme di diritto del lavoro applicabili.
Proporzionalmente alla gravità dell'azione non autorizzata, le azioni disciplinari includono la sospensione, la separazione dei compiti fino alla risoluzione del rapporto contrattuale di lavoro.

5.3.7. Requisiti di assunzione di personale qualificato

Gli impiegati assunti per svolgere incarichi di fiducia firmano in anticipo le clausole sulla riservatezza e i requisiti operativi impiegati da Bit4id. Qualsiasi azione che comprometta la

sicurezza delle procedure accettate potrà, previa valutazione, dar luogo alla risoluzione del contratto di lavoro.

Nel caso in cui tutti o una parte dei servizi di certificazione siano svolti da terzi, costoro saranno tenuti al rispetto dei controlli e delle disposizioni prevista in questa o in altre sezioni del Manuale Operativo. Il riparto di responsabilità tra la CA e tali soggetti viene definito da un apposito accordo tra le Parti.

5.3.8. *Somministrazione della documentazione al personale*

Il Prestatore dei servizi di certificazione somministrerà la documentazione necessaria al proprio personale, affinché quest'ultimo possa adempiere alle proprie attività in maniera competente ed efficace.

5.4. *Procedure di controllo per la sicurezza*

5.4.1. *Tipi di eventi registrati*

Bit4id produce documenti e salvaguarda informazioni, almeno in merito agli eventi seguenti, correlati alla sicurezza dell'Autorità di Certificazione:

- avvio e arresto del sistema;
- tentativi di creazione, cancellazione, reimpostazione password o cambio di diritti;
- tentativi di accesso e arresto sessione;
- tentativi di accesso non autorizzato al sistema della CA attraverso la rete;
- tentativi non autorizzati di accesso al sistema di archiviazione;
- cambio della configurazione del sistema;
- log delle applicazioni della CA;
- modifiche della CA e/o delle sue chiavi;
- cambio nella creazione di norme relative ai profili dei certificati;
- generazione di chiavi;
- creazione e revoca di certificati;
- log sulla distruzione dei dispositivi che contengono chiavi e relativi dati di attivazione;
- eventi legati al ciclo di vita del modulo crittografico, quali rilascio e utilizzo dello stesso;
- la generazione di chiavi e di database di gestione delle chiavi;
- registri di accesso fisico;
- manutenzione e cambi di configurazione del sistema;
- cambio del personale;
- rapporti su compromissioni e discrepanze;

- log sulla distruzione di materiale che contenga informazioni su chiavi, dati di attivazione o informazioni personali;
- rapporti completi sui tentativi di intrusione fisica nelle infrastrutture che supportano l'emissione e gestione dei certificati.

Le voci del Registro includono gli elementi seguenti:

- data e ora;
- numero seriale o sequenza di entrata nei registri automatici (log);
- identità del soggetto che effettua l'accesso.
- tipo di accesso.

Tutti gli eventi rilevanti, ivi descritti e tracciati dalla Certification Authority, sono costantemente monitorati tramite sistemi automatici di controllo, progettati per garantire un'elevata tempestività nell'individuazione di potenziali anomalie o incidenti di sicurezza. Tali sistemi generano alert automatici al verificarsi di condizioni che potrebbero indicare un evento di sicurezza, consentendo un'immediata presa in carico da parte delle funzioni competenti. Gli alert generati sono oggetto di analisi puntuale al fine di valutarne l'effettiva rilevanza, distinguendo i casi di reale impatto sulla sicurezza dai falsi positivi o dagli incidenti performativi, così da assicurare una gestione degli incidenti proporzionata, tracciabile e coerente con i requisiti normativi e di sicurezza applicabili.

5.4.2. Frequenza di elaborazione del giornale di controllo

Bit4id effettua il controllo dei log quando si produce un alert del sistema causata da un incidente.
L'elaborazione dei registri di controllo consiste nel riesame degli stessi, finalizzato all'accertamento della non-manipolazione degli stessi, in una breve ispezione di tutti gli accessi registrati e in un'indagine più profonda finalizzata all'analisi di eventi potenzialmente pericolosi.
Le azioni svolte per l'analisi del giornale di controllo sono documentate.
Bit4id dispone di un sistema che permette di garantire:

- che ci sia spazio sufficiente per la memorizzazione dei log;
- che i log non vengano riscritti;
- che il log registri almeno il tipo di evento, data e ora, utente e risultato dell'operazione.

5.4.3. Periodo di conservazione del giornale di controllo

Bit4id conserva le informazioni del giornale di controllo per un periodo di 20 (venti) anni.

5.4.4. Protezione dei registri di verifica

I Log dei sistemi sono protetti da eventuale manipolazione mediante cifratura e apposizione di firma digitale.

L'accesso ai log è riservato esclusivamente al personale autorizzato.

Esiste una procedura interna in cui sono dettagliati i processi di gestione dei dispositivi che contengono dati di log di controllo.

5.4.5. Procedure di backup

Bit4id dispone di una procedura adeguata di backup in modo che, in caso di perdita o distruzione di archivi importanti, le rispettive copie di backup dei logs siano disponibili entro un breve periodo di tempo.

Bit4id ha implementato un sistema di procedura di backup sicuro dei logs di controllo effettuando settimanalmente una copia di tutti i logs in un ambiente esterno. Inoltre une copia è conservata in un centro di custodia esterno.

5.4.6. Sistema di memorizzazione del giornale di controllo

L'informazione relativa al giornale di controllo è memorizzata in modo automatico attraverso l'uso di utility sviluppate ad hoc da Bit4id.

Esclusivamente il personale designato potrà richiedere agli amministratori di sistema il giornale di controllo, che viene firmato e cifrato automaticamente dalle utility suddette.

5.4.7. Notifica in caso di evento sospetto

Nessuna disposizione.

5.4.8. Analisi di vulnerabilità

Le analisi di potenziali vulnerabilità dell'infrastruttura di Bit4id sono soggette alle procedure di controllo implementate dalla stessa.

L'analisi di vulnerabilità deve essere effettuata, esaminata e rivista per effettuare una valutazione degli sviluppi necessari alla risoluzione delle stesse. Tali analisi sono eseguite periodicamente in accordo con la procedura interna, che recepisce le indicazioni e le tempistiche definite dagli standard di riferimento. I dati di verifica dei sistemi sono conservati allo scopo di essere utilizzati per eventuali indagini relative a incidenti e per localizzare le vulnerabilità.

5.5. Archiviazione delle informazioni

Bit4id assicura che tutte le informazioni relative ai certificati siano archiviate per un periodo di tempo adeguato e conforme alle norme vigenti.

5.5.1. Tipologie di documenti archiviati

Si provvede ad archiviare, da parte di Bit4id (o delle R.A) i seguenti documenti coinvolti nel ciclo di vita del certificato:

- Documento di riconoscimento esibito dal Richiedente per l'emissione del certificato
- Tessera sanitaria (o documento equivalente) esibito in fase di richiesta del certificato
- Contratto di fornitura del servizio firmato.
- Richieste di sospensione, riattivazione e revoca presentate tramite modulo fornito dal Certificatore.
- In caso di sigillo elettronico, documento attestante l'esistenza della Legal Entity e la rappresentanza legale della stessa.
- Ogni altra ulteriore documentazione che il Certificatore ritenga necessario acquisire per l'emissione/gestione del Certificato (es. appartenenza ad una organizzazione per Ruolo).

Bit4id e/o le R.A., a seconda dei casi, saranno responsabili della corretta archiviazione del materiale sopra indicato.

La Certification Authority, inoltre, conserva tutte le informazioni afferenti al certificato che ne costituiscono il giornale di controllo, ossia:

- tutti i dati relativi ai certificati;
- richieste di emissione e revoca dei certificati;
- tipologia di documento presentato al momento della richiesta di certificato;
- identità della R.A. che accetta la richiesta di certificato;
- tutti i certificati emessi o pubblicati;
- CRL emesse;
- log inerenti lo stato dei certificati;
- storico delle chiavi generate;
- comunicazioni tra gli elementi della PKI;
- politiche e pratiche di certificazione;
- informazioni sulle richieste di certificazione;
- informazioni sul ciclo di vita del certificato.

5.5.2. Periodo di archiviazione dei registri

Bit4id archivia i registri sopra elencati per almeno 20 anni, o per il periodo stabilito dalla legislazione vigente.
In particolare, i registri dei certificati revocati saranno accessibili per la consultazione per almeno 20 anni o per il periodo stabilito dalla legislazione in vigore al momento della revoca.

5.5.3. Protezione degli archivi

Bit4id protegge gli archivi in modo tale che solo le persone autorizzate possano accedervi. L'archivio è protetto dalla visualizzazione, la modifica, la cancellazione o qualsiasi altra manipolazione grazie all'implementazione di un sistema affidabile.
Bit4id garantisce la corretta protezione degli archivi grazie al personale qualificato che si occupa del trattamento e dell'archiviazione in strutture esterne sicure.

5.5.4. Procedure di back-up

Bit4id dispone di un centro di archiviazione esterno per garantire la disponibilità delle copie dei documenti elettronici. I documenti cartacei sono archiviati in luoghi sicuri con accesso limitato solo al personale autorizzato.
Bit4id esegue ogni giorno backup incrementali di tutti i dati elettronici e ogni settimana svolge backup completi in caso di recupero dei dati.
Inoltre, Bit4id (o, ove previsto dagli accordi, gli Uffici di Registrazione) conservano una copia dei documenti cartacei in un luogo sicuro e separato dalle strutture dell'Autorità di certificazione.

5.5.5. Requisiti della marcatura temporale

I registri sono datati in base ad una fonte affidabile via NTP.
Non è necessario che queste informazioni siano firmate digitalmente.

5.5.6. Localizzazione del sistema di archiviazione

Bit4id dispone di un sistema centralizzato per raccogliere informazioni sull'attività del team coinvolto nel servizio di gestione dei certificati.

5.5.7. Procedure per ottenere e verificare le informazioni di archiviazione

Bit4id dispone di una procedura che descrive il processo per verificare che le informazioni archiviate siano corrette e accessibili. Bit4id fornisce le informazioni e i mezzi per la verifica all'auditor.

5.6. Rinnovo delle chiavi

Almeno 5 anni prima della scadenza della validità della chiave privata della CA e della scadenza dell'ultimo certificato emesso, verrà effettuata da parte di Bit4id la generazione di una nuova coppia di chiavi di CA.

Il certificato *self-signed* corrispondente a suddetta coppia di chiavi viene trasmesso all'Organismo Nazionale di Supervisione dei Prestatori di Servizi Fiduciari (AgID).

Dopo l'inserimento del nuovo certificato di CA nell'elenco di fiducia (TSL) pubblicato dal precedentemente menzionato Organismo di Supervisione, Bit4id inizia a firmare i nuovi certificati e le corrispondenti CRL con la nuova chiave di CA.

La vecchia CA e la sua chiave privata saranno utilizzati solo per la firma di CRL.

Il relativo periodo di validità del certificato è quindi determinato in base:

- allo stato tecnologico;
- allo stato dell'arte delle conoscenze crittografiche;
- all'utilizzo previsto per lo stesso certificato;

Ogni sostituzione della chiave privata della CA determinerà una modifica al presente manuale e relativa comunicazione al competente Organismo di Vigilanza (AgID).

5.7. Compromissione delle chiavi e disaster recovery

5.7.1. Procedure di gestione degli incidenti e delle compromissioni

Bit4id, ha sviluppato politiche di sicurezza e continuità che consentono di gestire e recuperare i sistemi in caso di incidenti e compromissione delle operazioni, garantendo l'erogazione dei servizi critici per la revoca e la pubblicazione dello stato dei certificati.

5.7.2. Corruzione di risorse, applicazioni o dati

In caso di corruzione di risorse, applicazioni o dati, saranno attivate le procedure di gestione appropriate in base alle politiche di sicurezza e di gestione degli incidenti di Bit4id, che includono escalation, ricerca e risposta alla criticità. Se necessario, verrà avviata la procedura di compromissione della chiave o di Disaster Recovery di Bit4id.

5.7.3. Compromissione della chiave privata della CA

In caso di sospetto o accertamento della compromissione da parte di Bit4id, verranno attivate le procedure di compromissione delle chiavi in base alle politiche di sicurezza, alla gestione degli incidenti e alla continuità operativa, che consente il recupero dei sistemi critici, se necessario in un centro dati alternativo.

5.7.4. Continuità operativa dopo una criticità

Bit4id adotta tutte le procedure necessarie a garantire la continuità del servizio anche a seguito di situazioni di elevata criticità tramite l'utilizzo di sistemi di riserva.

Il piano si applica al centro di DR designato da Bit4id, il quale prevede una ridondanza di sistemi sufficiente a soddisfare i requisiti di disponibilità dei sistemi previsti e il ripristino dei servizi di elaborazione sul sito di Disaster Recovery.

Bit4id ripristinerà i servizi critici (revoca e pubblicazione delle informazioni sullo stato dei certificati) in accordo con il piano di criticità e continuità operativa esistente (conforme allo standard ISO/IEC 27001), garantendo così il funzionamento previsto dei servizi entro i termini previsti dal suddetto piano di continuità.

Bit4id dispone di un centro di DR, laddove se ne renda necessario la disponibilità per l'implementazione dei sistemi di certificazione descritti nel piano di continuità operativa, situato presso il data center della stessa Bit4id S.r.l in Napoli alla via Diocleziano n. 107.

5.8. Cessazione del servizio

Bit4id assicura ai Richiedenti e/o Titolari ed alle Relying Parties che le eventuali interruzioni, a seguito della cessazione temporanea dei servizi di certificazione svolti dalla CA, siano minime. In questo modo, Bit4id garantisce una manutenzione continua dei registri per il tempo stabilito nella sezione 5 del presente Manuale Operativo.

Tuttavia, Bit4id eseguirà tutte le azioni necessarie per trasferire a terzi o ad un notaio gli obblighi di manutenzione dei registri sopra indicati, per un periodo adeguato, in base alle prescrizioni del presente Manuale Operativo e alle disposizioni normative relative alla prestazione dei servizi fiduciari.

Prima di cessare l'erogazione dei Servizi di Certificazione, Bit4id ha sviluppato un piano di cessazione dell'attività, con le seguenti disposizioni:

- fornirà i fondi necessari per dar seguito alle attività di cessazione;
- informerà tutti i Titolari/Richiedenti, le terze parti e le altre CA con cui hanno stipulato accordi o altri tipi di relazioni della cessazione con almeno 60 giorni di anticipo rispetto alla data pianificata di cessazione del servizio;
- revocherà qualsiasi autorizzazione concessa ad Autorità subordinate per poter agire per conto della CA nella procedura di emissione del certificato;
- trasferirà gli obblighi relativi alla manutenzione delle informazioni dei registri e dei log per il periodo di tempo indicato ai Titolari e agli utenti;
- distruggerà o disabiliterà le chiavi private della CA;

- manterrà i certificati attivi e il sistema di verifica e revoca fino alla scadenza di tutti i certificati emessi;
- eseguirà le attività necessarie per trasferire gli obblighi di manutenzione delle informazioni di registro e degli archivi di registro degli eventi per i rispettivi periodi di tempo indicati al contraente e alle terze parti che utilizzano i certificati;
- comunicherà all'Organismo di vigilanza competente, con almeno 60 (sessanta) giorni di anticipo, la cessazione dell'attività e la destinazione dei certificati specificando se sarà trasferita la gestione e a chi o se il trasferimento non sarà più valido;
- comunicherà all'Organismo di vigilanza competente l'avvio di qualsiasi procedura concorsuale nei confronti di Bit4id, nonché qualsiasi altra circostanza rilevante che possa impedire il proseguimento dell'attività.

6. MISURE DI SICUREZZA TECNICA

Bit4id utilizza sistemi e tecniche affidabili atte a garantire la sicurezza tecnica dei processi implementati. Tutte le misure di sicurezza tecnica impiegate da Bit4id sono conformi ai seguenti standard di riferimento:

- ETSI EN 319 411-1;
- ETSI EN 319 411-2;
- ETSI EN 319 421;
- ETSI EN 319 422.

6.1. Generazione e installazione della coppia di chiavi

6.1.1. Generazione della coppia di chiavi

6.1.1.1. Chiavi della CA

La coppia di chiavi delle CA è generata seguendo una procedura di "*cerimonia di chiavi*" che avviene in un ambiente protetto, all'interno di un perimetro di elevata sicurezza specificatamente destinato a tale scopo.

Le attività svolte durante la "cerimonia" di generazione delle chiavi di certificazione sono registrate, datate e firmate da tutte le persone coinvolte.

Inoltre, l'esecuzione di tali attività avviene in presenza dell'auditor interno ed è documentata in un apposito verbale redatto dal responsabile della sicurezza.

I verbali sono conservati per scopi di controllo e monitoraggio, per un periodo appropriato definito da Bit4id.

Per la generazione delle chiavi sono stati utilizzati dispositivi HSM conformi Common Criteria EAL4+.

Bit4id S.r.l. QTSP Qualified Certificates CA RSA 4096 G1	**4.096 bits**	**20 anni**
- Certificati di entità finale	3.072 bits	Fino a 6 anni
Bit4id S.r.l. QTSP Qualified Certificates CA ECC 256 G1	**ECC (secp256)**	**20 anni**
- Certificati di entità finale	ECC (secp256)	Fino a 6 anni
Bit4id S.r.l. QTSP Qualified Time-Stamp CA RSA 4096 G1	**4.096**	**20 anni**
Certificati di Time Stamping Unit	3.072	Fino a 11 anni

Bit4id S.r.l. QTSP Qualified Time-Stamp CA ECC 256 G1	**ECC (secp256)**	**20 anni**
Certificati di Time Stamping Unit	ECC (secp256)	Fino a 11 anni

Nel caso di emissione di un certificato digitale di sottoscrizione "One-Shot", tramite la CA **Bit4id S.r.l. QTSP Qualified One-Shot Certificates CA ECC 256 G1,** la durata del relativo certificato (di entità finale) è differente da quella indicata nella tabella di cui sopra (v. 1.4.1.2. infra).

6.1.1.2. Chiavi dei Titolari

Le chiavi dei Titolari sono generate tramite dispositivi hardware sicuri (QSCD – *Qualified Signature Creation Device*), in maniera conforme a quanto indicato nel "*security target*" del dispositivo stesso e attraverso le librerie software fornite dal produttore del dispositivo.

Gli algoritmi e le suite crittografiche utilizzate sono conformi alle specifiche ETSI TS 119 312.

In particolare, le chiavi vengono generate utilizzando l'algoritmo a chiave pubblica RSA, con una lunghezza minima di 3072 bit o chiavi ECDSA equiparabili (lunghezza minima 256 bit), in ottemperanza a quanto previsto dall'art. 24, paragrafo 2, lettera e) del Regolamento eIDAS.

6.1.1.3. Chiavi di TSU

Le chiavi di TSU sono generate in un ambiente fisicamente protetto, in conformità con le procedure interne di Bit4id relative ai sistemi di marcatura temporale.

L'esecuzione di tali attività avviene in presenza dell'auditor interno ed è documentata in un apposito verbale.

Il dispositivo utilizzato per la generazione e custodia delle chiavi di TSU è certificato in conformità ai Common Criteria EAL 4+.

6.1.2. Consegna della chiave privata al Titolare

Nel caso di certificati relativi a chiavi che risiedono su smartcard o token (dispositivo qualificato per la creazione della firma), la chiave privata viene generata e archiviata in modo protetto all'interno del suddetto dispositivo qualificato.

I codici segreti relativi all'utilizzo del dispositivo (PIN e PUK) sono comunicati all'utente attraverso canali sicuri oppure impostati autonomamente dall'utente in una sessione autenticata fornita da Bit4id.

Nel caso di certificati relativi a chiavi che risiedono su un HSM, la chiave privata del Titolare viene generata all'interno di una sezione privata dell'HSM destinata al Titolare.

I mezzi e i dati di attivazione della firma remota (gestiti dal SAM) sono forniti e gestiti con procedure e canali sicuri, in modo che siano nella disponibilità esclusiva del Titolare. I sistemi SSAS non

memorizzano in chiaro segreti del Titolare e applicano misure per prevenirne intercettazione o deduzione.
L'accesso alla chiave privata avviene mediante interfacce applicative esposte dal dispositivo ed esclusivamente mediante una procedura di autenticazione sicura.
La chiave privata non viene inviata al Titolare, pertanto non lascia mai l'ambiente di sicurezza che garantisce il controllo esclusivo della chiave privata da parte del Titolare.

6.1.3. Distribuzione della chiave pubblica della CA

Le chiavi pubbliche di Bit4id sono comunicate a terze parti che utilizzano i certificati, assicurando l'integrità della chiave e autenticandone l'origine, attraverso la pubblicazione sul sito web ufficiale https://www.bit4id.com/documentazione-qtsp e attraverso la pubblicazione sulla Trust-service Status List (TSL) effettuata dall'Organismo di Supervisione Nazionale (AgID).

6.1.4. Dimensioni delle chiavi

La CA utilizza chiavi RSA con lunghezza pari a 4096 bit oppure su crittografia a curve ellittiche (Elliptic Curve Cryptography – ECC) con lunghezza pari a 256 bit;
La lunghezza delle chiavi dei Certificati degli utenti finali è di 3.072 bit per i certificati emessi dalle CA a 4096 bit o 256 bit per i certificati a curve ellittiche. La lunghezza delle chiavi dei certificati di TSU è di 3.072 bit o curve ellittiche.

6.1.5. Generazione dei parametri della chiave pubblica

La chiave pubblica delle CA radice, subordinate e dei certificati dei Titolari e di TSU è codificata in conformità con lo standard RFC 5280.

6.1.6. Controllo di qualità dei parametri della chiave pubblica

- Lunghezza del Modulo = 4096 bits/ECC (secp256);
- Funzioni crittografiche di riepilogo: SHA256.

6.1.7. Generazione delle chiavi in applicazioni informatiche o in beni strumentali

Tutte le chiavi si generano con strumenti e procedure, in conformità con quanto indicato nella sezione 6.

6.1.8. Scopo delle chiavi

Le chiavi per i certificati emessi dalle CA sono utilizzate esclusivamente per la firma di certificati e CRL. Le chiavi per i certificati degli utenti finali (firme e sigilli qualificati) sono utilizzate esclusivamente per il "Non ripudio" (*content committment*).

6.2. Protezione delle chiavi private e sicurezza moduli

6.2.1. Standard e sicurezza dei moduli crittografici

In relazione ai moduli che gestiscono le chiavi di Bit4id, dei contraenti dei certificati di firma elettronica e le chiavi di TSU, è garantito il livello richiesto dagli standard indicati nel paragrafo precedente 6.1. (e sotto paragrafi).

In particolare, le chiavi private della CA sono generate ed utilizzate all'interno di apparati HSM dotati di certificazione Common Criteria (ISO 15408) livello EAL4+ superiore.

La chiave privata del Titolare usata per i certificati (di firma o sigillo elettronico) risiede all'interno di un dispositivo crittografico hardware certificato Common Criteria livello EAL4+ o superiore, appropriato per l'uso previsto delle chiavi, in accordo alla Normativa vigente.

6.2.2. Controllo da parte di più di una persona (n di m) sulla chiave privata

È richiesto un controllo composto da più persone per l'attivazione della chiave privata della CA e della TSA.

Nel caso della chiave privata della CA e della TSA di Bit4id, è richiesta la presenza simultanea di almeno 3 delle 6 persone che hanno partecipato alla corrispondente cerimonia di chiavi. I dispositivi crittografici sono protetti fisicamente come stabilito in questo documento.

6.2.3. Ripristino della chiave privata

Nel caso di ripristino della chiave privata della CA o della TSA di Bit4id su HSM è richiesta la presenza simultanea di almeno 3 delle 6 persone che hanno partecipato alla corrispondente cerimonia delle chiavi e, in aggiunta, un operatore con una carta OCS.

6.2.4. Backup della chiave privata

Bit4id effettua una copia di backup delle chiavi private della CA e di TSA che rende possibile il recupero in caso di criticità, perdita o danneggiamento.

Sia la generazione che il recupero della copia richiedono la partecipazione di almeno tre persone.

Questi file di backup in un luogo sicuro, differente da quello in cui si trova la copia operativa.

6.2.5. Archivio della chiave privata

Le chiavi private delle CA vengono archiviate in modo sicuro nei server e nei sistemi della Bit4id.

Bit4id dispone di tutti i requisiti e le necessarie autorizzazioni affinché la gestione delle chiavi private archiviate avvenga nel rispetto dei più elevati standard di sicurezza, facendo in modo che le informazioni siano conservate in archivi ignifughi sicuri e fisicamente isolati dal resto delle infrastrutture e all'interno del centro di custodia.

6.2.6. Trasferimento della chiave privata tra moduli crittografici

Le chiavi private vengono generate direttamente nei moduli crittografici di produzione di Bit4id.
Le operazioni di backup e di ripristino delle chiavi di CA e di TSA vengono condotte secondo quanto specificato nella sezione 6.2 del presente documento.

6.2.7. Memorizzazione della chiave privata sul modulo crittografico

Le chiavi private della CA vengono generate nei moduli crittografici HSM, che garantiscono la sicurezza, la confidenzialità e l'impossibilità di esportazione delle chiavi secondo le modalità descritte nella sezione 6 del presente documento.

6.2.8. Modalità di attivazione della chiave privata

La chiave privata di Bit4id viene attivata eseguendo la corrispondente procedura di avvio sicuro del modulo crittografico (così come indicato dal produttore e in accorso al traguardo di sicurezza del dispositivo), da parte delle persone indicate nella sezione 6.

6.2.9. Modalità di distruzione della chiave privata

Prima della distruzione delle chiavi di CA e di TSA, i relativi certificati vengono revocati. I dispositivi che contengono parte delle chiavi private di Bit4id verranno distrutti o riavviati a basso livello. Per l'eliminazione verranno seguite le fasi descritte nel manuale dell'amministratore del dispositivo crittografico.
Infine, le copie di backup saranno distrutte in modo sicuro. Tali operazioni vengono condotte esclusivamente in circostanze che le rendano necessarie, come ad esempio in caso di cessazione del servizio.

6.2.10. Modalità di disattivazione della chiave privata

Non prevista.

6.2.11. Classificazione dei moduli crittografici

Vedere il paragrafo 6.1.

6.3. Altri aspetti della gestione della coppia di chiavi

6.3.1. Archiviazione della chiave pubblica

Secondo quanto stabilito nel paragrafo 5 del presente Manuale.

6.3.2. Periodi di utilizzo delle chiavi pubbliche e private

I periodi di utilizzo delle chiavi sono quelli determinati dalla durata del certificato, dopodiché non possono continuare ad essere utilizzate.

6.4. Dati di attivazione

6.4.1. Generazione dei dati di attivazione

I dati di attivazione dei dispositivi che proteggono le chiavi private di CA e di TSA di Bit4id sono generati in conformità con quanto stabilito nella sezione 6 e con la cerimonia delle chiavi. La creazione e la distribuzione dei suddetti dispositivi è registrata.
Allo stesso modo, Bit4id genera i dati di attivazione in modo sicuro.

6.4.2. Protezione dei dati di attivazione

I dati di attivazione dei dispositivi che proteggono le chiavi private di CA e di TSA sono protetti con PIN, la cui conoscenza è ristretta esclusivamente ai titolari delle carte *dell'Administrative Card Set* e *Operative Card Set* dei moduli crittografici utilizzati, così come indicato nel documento di cerimonia della chiave. I dati di attivazione delle chiavi private relative a certificati di firma qualificata sono protetti in fase di emissione in modo tale che il titolare sia l'unico a conoscerle. I titolari sono responsabili della gestione e della protezione in sicurezza dei dati di attivazione privati, prevenendo la loro rivelazione a terzi non autorizzati.

6.5. Controlli di sicurezza informatica

Bit4id utilizza sistemi affidabili per offrire i servizi di certificazione.
Bit4id effettua controlli e verifiche informatiche al fine di stabilire una gestione delle risorse informatiche in conformità con il livello di sicurezza richiesto per la gestione dei sistemi di certificazione digitale e nello specifico a quanto richiesto dagli standard tecnici ETSI EN 319 411-1 e ETSI EN 319 411-2 per la firma e i sigilli elettronici qualificati ed ETSI EN 319 421 per il servizio di marcatura temporale.
Per quanto riguarda la sicurezza delle informazioni, Bit4id si avvale dei controlli dello schema di certificazione sui sistemi di gestione delle informazioni conformi ISO 27001.
Le attrezzature utilizzate sono inizialmente configurate secondo i profili di sicurezza appropriati, per quanto concerne gli aspetti di:

- Configurazione di sicurezza del sistema operativo.
- Configurazione di sicurezza delle applicazioni.
- Dimensionamento corretto del sistema.

- Configurazione degli utenti e dei permessi.
- Configurazione dei registri di log.
- Piano di backup e ripristino.
- Configurazione dell'antivirus.
- Requisiti del traffico di rete.

6.5.1. Requisiti tecnici specifici per la sicurezza informatica

Ogni server impiegato da Bit4id include le seguenti funzionalità:

- Controllo dell'accesso ai servizi e gestione dei privilegi.
- Imposizione della separazione delle attività per la gestione dei privilegi.
- Identificazione e autenticazione dei ruoli associati alle identità.
- Verifica degli eventi relativi alla sicurezza.

6.5.2. Valutazione del livello di sicurezza informatica

Le applicazioni delle CA e di registro utilizzate da Bit4id sono sottoposte a verifiche di sicurezza (Vunerability Assessment) con cadenza almeno trimestrale. I Penetration Test sono effettuati con cadenza almeno annuale.

6.6. Controlli tecnici del ciclo di vita

6.6.1. Controlli di sviluppo dei sistemi

Le applicazioni e i sistemi sono sviluppati, implementati e gestiti secondo gli standard di sviluppo e le procedure interne di *change management* e le applicazioni dispongono di metodi per verificare l'integrità e l'autenticità, nonché per correggere la versione da utilizzare.
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 ETSI EN 319 411-2, e sono ulteriormente definiti nelle procedure di qualità ISO 9001 e nelle policy di sicurezza ISO 27001.

6.6.2. Controlli di gestione della sicurezza

Bit4id sviluppa le attività necessarie per la formazione e la consapevolezza dei dipendenti in materia di sicurezza. I materiali utilizzati per la formazione e i documenti che descrivono i processi sono aggiornati dopo esser stati approvati da un gruppo che si occupa della gestione della sicurezza. Nell'esecuzione di questa funzione viene disposto un piano di formazione annuale.
Bit4id richiede, tramite apposito contratto, a qualsiasi fornitore esterno coinvolto nella prestazione di servizi qualificati fiduciari le misure di sicurezza equivalenti. Descrizioni dettagliate dei controlli di sicurezza di rete eseguiti sono disponibili come documenti interni.

6.7. Controlli di sicurezza della rete

L'accesso ai dispositivi che fanno parte dell'infrastruttura PKI è protetto da firewall che implementano una suddivisione dell'architettura in perimetri di rete ben definiti.
Le comunicazioni tra i differenti elementi dell'architettura avvengono utilizzando protocolli di rete che implementano crittografia (utilizzando i protocolli TSL/SSL) e mediante l'uso di autenticazione a doppio fattore da parte del personale esplicitamente autorizzato. Periodicamente vengono inoltre condotti (da parte di personale qualificato e in grado di garantire un sufficiente livello di indipendenza rispetto all'operatività dei servizi di certificazione) dei Vulnerability Assessment con la finalità di individuare eventuali vulnerabilità.

6.8. Controlli ingegneristici dei moduli crittografici

I moduli crittografici vengono sottoposti ai controlli ingegneristici previsti dagli standard indicati nel presente paragrafo.
Gli algoritmi impiegati per la generazione delle chiavi sono comunemente accettati per l'uso della chiave a cui sono destinati.
Tutte le operazioni crittografiche di Bit4id sono realizzate in moduli con certificazioni Common Criteria EAL 4+.

6.9. Riferimento temporale

Bit4id utilizza un sistema di sincronizzazione dei sistemi tramite NTP, che accede a due servizi indipendenti:

1. la prima sincronizzazione avviene tramite un servizio basato su antenne e ricevitori GPS che permette un livello di accuratezza STRATUM 1 (con due sistemi in alta disponibilità);
2. la seconda dispone di una sincronizzazione complementare, tramite NTP, con il Real Instituto y Observatorio de la Armada (ROA). Si garantisce in questo modo differenza non superiore al secondo rispetto alla scala di tempo UTC.

6.10. Cambiamento di stato di un Dispositivo Sicuro di Creazione di Firma o Sigillo Elettronico (QSCD)

Bit4id garantisce l'applicazione delle norme per valutare la sicurezza dei prodotti delle tecnologie dell'informazione applicabili alla certificazione dei dispositivi per la creazione di una firma o di un sigillo elettronico qualificato a norma dell'art. 30, co. 3, lett. a) e art. 39 co. 2 del Regolamento (UE) n. 910/2014.

Le norme cui si fa riferimento sono indicate all'art. 1 co. 1 e nel relativo Allegato alla Decisione di Esecuzione (UE) n. 650/2016 della Commissione del 25 aprile 2016.

In particolare, in caso di modifiche dello stato di certificazione dei dispositivi qualificati di creazione di firma o sigillo elettronico (QSCD), Bit4id procederà come descritto di seguito:

1. Bit4id dispone di una lista di vari QSCD certificati, così come di una stretta relazione con i fornitori di questi dispositivi, al fine di garantire alternative alla possibile perdita di certificazione dei dispositivi QSCD;
2. in caso di cessazione del periodo di validità o perdita della certificazione, Bit4id non utilizzerà detti QSCD per l'emissione di nuovi certificati digitali, né in nuove emissioni.
3. Procederà immediatamente ad utilizzare QSCD con una certificazione valida.
4. Nel caso in cui un dispositivo QSCD dimostri di non esserlo mai stato, per falsificazione o qualsiasi altro tipo di frode, Bit4id procederà immediatamente a comunicarlo ai suoi clienti e all'organismo regolatore, a revocare i certificati digitali emessi in questi dispositivi e a rimpiazzarli emettendoli in QSCD validi;
5. In ogni caso in cui si manifesti ovvero vi sia chiara evidenza di una compromissione dei dispositivi QSCD, Bit4id provvederà immediatamente alla revoca di tutti i certificati le cui coppie di chiavi siano state generate mediante il suddetto dispositivo, dandone espressa comunicazione ai titolari e alle eventuali terze parti interessate. Procederà inoltre alla sostituzione del dispositivo interessato con un QSCD valido.

7. PROFILO DEI CERTIFICATI, CRL, OCSP

7.1. Profilo dei certificati

I certificati emessi secondo questo Manuale sono conformi alla specifica pubblica RFC 3739, basata sullo standard ITU-T X.509 v3, nonché alle norme europee ETSI EN 319 412 (n. 1, 2, 3, 4 e 5) e ETSI EN 319 422.

Le regole di valorizzazione degli attributi del DN rispettano le norme ETSI EN in relazione ai profili dei certificati per persone fisiche/giuridiche nonché le specifiche contenute nella RFC 5280 e si conformano alle Raccomandazioni di cui alla Determinazione n. 147/2019 emessa dall'AgID.

La documentazione relativa al profilo dei certificati emessi in conformità alla norma europea ETSI EN 319 412 può essere richiesta in qualsiasi momento a Bit4id.

7.1.1. Numero di versione ed estensioni del certificato

La versione del certificato è v3, basata sullo standard ITU-T X.509.

Le estensioni caratterizzanti i certificati emessi secondo questo Manuale sono indicate, nel dettaglio, all'interno della documentazione relativa a ciascun profilo di certificato, disponibile sul sito web di Bit4id (https://www.bit4id.com/documentazione-qtsp).

7.1.2. Identificatori degli algoritmi

Tutti i certificati emessi secondo questo Manuale sono firmati con algoritmi standard, identificati identificati dai relativi OID.

7.1.3. Forme dei nomi

Il campo *Subject* del certificato contiene un *Distinguished Name* (DN) conforme allo standard ITU-T X.500 e alla norma ETSI EN 319 412.

Il DN è composto da attributi definiti nella specifica pubblica RFC 5280.

7.1.4. OID (Object Identifier)

Come previsto nel par. 1.2.1., ciascun profilo di certificato, emesso secondo questo Manuale, è identificato da uno specifico OID (*Object Identifier*).

7.2. Profilo delle CRL

Le CRL emesse da Bit4id sono conformi alla specifica pubblica RFC 5280.

7.2.1. Numero di versione

Nel campo Versione della CLR è indicato il valore 2, come richiesto nella specifica di cui al par. precedente.

7.3. Profilo OCSP

Il servizio OCSP erogato da Bit4id è conforme alla specifica pubblica RFC 6960.

8. AUDIT DI CONFORMITÀ

Bit4id, in qualità di prestatore di Servizi Fiduciari, è soggetta a verifiche di conformità.

8.1. Frequenza degli audit

Con frequenza annuale, un Organismo di Valutazione accreditato (Conformity Assessment Body, CAB) provvede a verificare la conformità dei servizi CA di Bit4id al presente Manuale, al Regolamento (UE) n. 910/2014 e agli standard ETSI applicabili.

Sempre su base annuale, relativamente ai servizi di certificazione digitale, Bit4id dispone e svolge un'attività di auditing interno.

Le verifiche di conformità interne, inoltre, possono aver luogo in qualsiasi momento, qualora si sospetti il verificarsi di una qualsiasi violazione di misure di sicurezza.

8.2. Identità e qualificazione degli auditor

Gli audit di conformità, nel rispetto di quanto dettato dalla norma ETSI EN 319 403, sono svolti esclusivamente da personale altamente qualificato, specializzato nella conduzione di audit relativi a servizi fiduciari, e competente in materia, dipendente da un Organismo di Valutazione (CAB) accreditato in conformità al Regolamento (CE) n. 765/2008.

8.3. Relazione tra la CA e gli auditor

Tra l'Organismo di Valutazione (CAB) e Bit4id non intercorre alcun rapporto che possa compromettere la genuinità delle verifiche di conformità ovvero determinare un conflitto d'interessi idoneo a distorcere le attività di auditing realizzate dal primo nei confronti di Bit4id.

8.4. Elementi soggetti a verifica

Le attività di auditing riguardano, più nel dettaglio, i seguenti aspetti:

a. la conformità dei servizi di certificazione digitale resi da Bit4id al presente Manuale nonché alla ulteriore documentazione applicabile al servizio di CA (per es. procedure operative interne);
b. l'implementazione delle previste misure di sicurezza fisica, tecnica ed operativa nonché quelle relative alla sicurezza del personale;
c. la conformità del presente Manuale e degli altri documenti applicabili al servizio di CA alla normativa vigente;
d. la predisposizione di un sistema informativo e di gestione che garantisca la qualità del servizio fornito;

e. il corretto svolgimento, da parte della CA, delle attività che concernono i servizi di certificazione digitale (es.: identificazione ed autenticazione dei soggetti che richiedono i certificati; gestione della relativa documentazione; gestione delle chiavi).

In sintesi, potranno costituire oggetto delle verifiche di conformità i seguenti elementi:

a. procedure operative della CA e delle RA;
b. sistemi informatici della CA;
c. misure atte alla protezione del centro di elaborazione dati;
d. documentazione inerente ai servizi di CA.

Oggetto di verifica, in accordo alla norma ETSI EN 19 401 (REQ-7.13-03), è anche l'accessibilità dei servizi fiduciari da parte di persone con disabilità.

Considerando il contesto dell'Organizzazione ed il fatto che i servizi fiduciari emessi da Bit4id sono destinati principalmente a personale sanitario e amministrativo, il requisito di accessibilità dei servizi non è considerato strettamente necessario per l'erogazione degli stessi ai soggetti interessati.

8.5. *Azioni successive alle non-conformità*

Ricevuto il report, la Direzione Aziendale provvede ad esaminare, con la collaborazione dell'OdV, le eventuali non-conformità riscontrate durante gli audit.

A seconda della natura e della severità della non-conformità evidenziata, la Direzione Aziendale definisce il piano di azioni conseguenti e dispone l'adozione delle misure correttive necessarie, anche tenendo conto delle procedure interne relative alla gestione delle non-conformità.

Nelle ipotesi in cui le misure definite si rivelino non adeguate a correggere le carenze riscontrate ovvero nei casi in cui tali carenze rappresentino una minaccia a pregiudizio della sicurezza ed integrità dei servizi di certificazione digitale, la Direzione aziendale, potrà provvedere a:

- cessare temporaneamente, e in via transitoria, le operazioni in corso;
- revocare la chiave di CA e rigenerare l'infrastruttura;
- cessare il servizio di CA;
- adottare ogni ulteriore misura necessaria.

8.6. *Comunicazione dei risultati*

L'Organismo di Valutazione (CAB) comunica il risultato dell'attività di auditing alla Direzione Aziendale di Bit4id.

Il report prodotto dal CAB, inoltre, viene trasmesso all'Organismo nazionale di Supervisione (AgID).

9. CONDIZIONI ECONOMICHE E LEGALI

9.1. Tariffe

9.1.1. Tariffe per l'emissione o rinnovo del certificato

I servizi di certificazione di Bit4id sono forniti indistintamente nei confronti di persone fisiche e persone giuridiche che intendono utilizzare i certificati digitali qualificati di Bit4id nell'ambito della propria organizzazione o nell'ambito dei rapporti con soggetti terzi/utenti finali.
Bit4id, inoltre, può affidare – in conformità al presente Manuale Operativo (v. par. 1.3.2. *infra*) – agli Uffici di Registrazione le attività di identificazione e registrazione dei Richiedenti.
Bit4id può, altresì, avvalersi di una rete di distribuzione consistente in canali retail ed on-line, tra cui si citano:

- marketplace on-line;
- canali di vendita on-line della capogruppo Namirial SpA;
- canali di vendita indiretti di Namirial SpA (commercialisti, avvocati, etc.);
- altre reti distributive retail.

In questi casi, le tariffe per l'emissione dei certificati sono disponibili direttamente presso gli Uffici di Registrazione, o presso i canali di vendita sopra indicati.
Le tariffe sono disponibili, per i servizi erogati direttamente dalla Certification Authority, presso il sito https://www.bit4id.com/ e/o presso le Registration Authority. La CA può stipulare accordi commerciali con le RA e/o i Richiedenti prevedendo tariffe specifiche.
Tuttavia Bit4id si riserva la facoltà di modificare le tariffe per i servizi di certificazione erogati senza previa notifica agli utenti e di rinegoziare le condizioni economiche con i singoli clienti in ragione del volume richiesto.

9.1.2. Tariffa per l'accesso ai certificati

L'accesso al pubblico registro dei certificati pubblicati è libero e gratuito: per tale motivo Bit4id non ha stabilito alcuna tariffa economica per l'accesso alla lista di tali certificati.

9.1.3. Tariffa per l'accesso alle informazioni di stato dei certificati

Bit4id non ha stabilito alcuna tariffa economica per l'accesso ai servizi informativi (CRL, OCSP) sullo stato dei certificati. Tale accesso è libero e gratuito.

9.1.4. Tariffa per altri servizi

Nessuna condizione.

9.1.5. Politica per il rimborso – Recesso

Ai sensi e per gli effetti degli artt. 49 e ss. del D.lgs. 6 settembre 2005 n. 206 e s.m.i. (Codice del Consumo) il Richiedente - consumatore ha diritto di recedere dal contratto, anche senza indicarne le ragioni, entro il termine di 14 (quattordici) giorni decorrenti dalla data della sua conclusione e di ottenere il relativo rimborso.

Il diritto di recesso può essere esercitato unicamente da Richiedenti che, nella stipulazione del contratto, hanno agito per scopi estranei all'attività imprenditoriale (e, dunque, da coloro che sono qualificabili come consumatori ai sensi dell'art. 3 co. 1 lett. a) del Codice del Consumo).

Per poter esercitare il diritto di recesso il Richiedente - consumatore è tenuto ad informare Bit4id, della sua decisione di recedere dal contratto tramite una dichiarazione esplicita, ai recapiti di seguito forniti:

Bit4id s.r.l.
Via Diocleziano, 107
80125 – Napoli

Per ulteriori contatti è possibile consultare la sezione 1.3.1 del presente Manuale.

La comunicazione del recesso potrà avvenire tramite:

1) Posta raccomandata con avviso di ricevimento all'indirizzo indicato;
2) messaggio e-mail all'indirizzo di posta elettronica reperibile nelle condizioni generali di servizio.

Ulteriori condizioni per il rimborso/recesso potranno essere applicate a seconda della modalità/canale di vendita utilizzato dal Titolare, opportunamente messe a conoscenza di quest'ultimo da Bit4id e/o direttamente da parte del proprietario del canale di vendita.

9.2. Capacità finanziaria

In relazione alla gestione dei servizi di CA e al piano di cessazione delle attività, Bit4id garantisce di possedere e poter disporre di sufficienti risorse finanziarie necessarie a garantire l'operatività dei propri servizi, ad assicurare l'adempimento dei propri obblighi e ad affrontare i rischi e le responsabilità eventualmente derivanti dall'erogazione del servizio di certificazione.

9.2.1. Copertura assicurativa

In conformità con la normativa richiamata nel paragrafo precedente e per lo svolgimento e l'esecuzione di tutte le attività legate ai servizi di cui al presente Manuale Operativo, Bit4id ha stipulato polizza assicurativa a copertura di tutti i rischi, con compagnia di primaria importanza in campo assicurativo.

La predetta polizza assicurativa garantisce la copertura per lo svolgimento di tutte le attività di "*servizi di certificazione digitale e/o elettronica, come fornitore di servizi di certificazione che emette certificati qualificati, nonché la sua attività come autorità di registrazione [...]*" ed è posta a copertura di tutti i rischi derivanti dall'erogazione dei servizi di certificazione, i cui dettagli sono disponibili al link https://static.namirial.com/docs/it/responsabilita-civile-professionale-e-cyber.pdf.

9.2.2. Altri asset

Nessuna condizione.

9.2.3. Copertura assicurativa per gli utenti finali

Si rinvia al precedente paragrafo 9.2.1.

9.3. Tutela delle informazioni trattate

9.3.1. Informazioni confidenziali

Bit4id si impegna a trattare e a gestire, qualificandole come confidenziali, tutte le seguenti informazioni:

- richieste di emissione certificati, approvate o negate, nonché tutti i dati personali ottenuti per l'emissione e il mantenimento dei certificati, ad eccezione delle informazioni che devono essere inserite nei certificati o che per altre ragioni, ai sensi del paragrafo seguente, sono da considerarsi non confidenziali;
- chiavi private dei Titolari qualora siano generate e/o memorizzate dalla CA;
- log dei sistemi di elaborazione della CA;
- contratti con le RA;
- documenti di controllo, interni ed esterni, creati e/o gestiti dalla CA e dai suoi auditor;
- business continuity e piani di emergenza;
- piani di sicurezza;
- ogni altra informazione identificata come "Confidenziale".

Tutte le informazioni confidenziali sono trattate da Bit4id nel rispetto delle norme applicabili, in particolare del D.lgs. 196/03 e s.m.i. e del Regolamento (UE) 2016/679.

La CA assicura che le informazioni confidenziali siano adeguatamente protette fisicamente e/o logicamente dagli accessi non autorizzati nonché dal rischio di perdita a seguito di disastri (si veda a tal riguardo la sezione apposita).

9.3.2. Informazioni non confidenziali

Non sono considerate confidenziali le seguenti informazioni:

- certificati emessi o in corso di emissione;
- periodo di validità del certificato, nonché la data di emissione del certificato e la data di scadenza;
- numero di serie del certificato;
- differenti stati del certificato (ad esempio: in attesa di generazione e/o consegna, valido, revocato, sospeso o scaduto), la data di inizio di ciascuno di essi e il motivo che ha determinato il cambiamento di stato;
- liste dei certificati sospesi o revocati (CRL), nonché le altre informazioni sullo stato di revoca;
- informazioni contenute all'interno del certificato;
- informazioni sui Titolari ottenibili dalla consultazione delle fonti pubbliche;
- informazioni che il Titolare stesso ha chiesto alla CA di rendere pubbliche;
- qualsiasi altra informazione che non rientri nell'ambito di applicazione nel paragrafo precedente.

9.3.3. Ipotesi di divulgazione delle informazioni

Bit4id non divulga le informazioni confidenziali di cui al paragrafo 9.3.1., salvo che tale circostanza non gli sia imposta da un obbligo giuridico/normativo di divulgazione dello Stato.
I dati personali del Titolare potranno essere comunicati alle forze di polizia, all'autorità giudiziaria, agli organismi di informazione e sicurezza o ad altri soggetti pubblici, ai sensi del D.lgs. 196/2003 e s.m.i. o del Reg. (UE) 679/2016, nel caso in cui ciò sia richiesto per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.
Le circostanze che legittimano la divulgazione, da parte di Bit4id, delle informazioni confidenziali e, in particolare, dei dati personali dei soggetti richiedenti e/o titolari, verranno debitamente indicate nell'informativa sul trattamento dei dati personali predisposta e rilasciata dalla CA.

9.4. Trattamento e protezione dei dati personali

9.4.1. Informativa sulla Privacy

Il Regolamento Europeo (UE) n.679/2016 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (GDPR) ha introdotto requisiti normativi innovativi per la protezione dei dati personali, con ricadute organizzative, operative e tecnologiche che riguardano i principali processi di gestione dei Dati all'interno delle strutture organizzative aziendali.
Il predetto Regolamento impone ai Titolari e Responsabili del trattamento un obbligo generale di adozione di misure tecnico-organizzative adeguate al rischio associato al trattamento dei dati (cfr. art. 32 del GDPR).

In conformità alle disposizioni di cui al GDPR in materia di tutela dei dati personali, Bit4id ha predisposto l'Informativa ai sensi dell'art. 13 del GDPR, disponibile alla consultazione, nella sua ultima versione al seguente indirizzo: https://www.bit4id.com/documentazione-qtsp
In ogni caso, è possibile esercitare i diritti in materia di protezione dei dati personali in ogni momento e gratuitamente rivolgendosi al Responsabile della Protezione dei Dati, che è contattabile inviando una richiesta all'indirizzo dpo@bit4id.com, oppure indirizzando la comunicazione via posta a:

Bit4id S.r.l.
Via Diocleziano n. 107
(80125) - Napoli
CA: Responsabile della Protezione dei Dati

Nel contattare Bit4id, è necessario che l'Interessato includa nome, e-mail/indirizzo postale e/o numero/i di telefono per essere sicuro che la sua richiesta possa essere gestita correttamente.

9.4.2. Emissione dei Certificati di CNS

Con riferimento al Trattamento dei dati personali trattati nell'ambito del ciclo di vita dei certificati di CNS, Bit4id opera in regime di contitolarità, ai sensi dell'art. 26 del GDPR, con l'Ente Emettitore.

9.5. Diritti di proprietà intellettuale

9.5.1. Proprietà dei certificati

Bit4id gode di tutti i diritti di proprietà intellettuale e sfruttamento economico, riconosciuti dalla legge, su tutti i certificati emessi in esecuzione dei rapporti contrattuali con i Richiedenti e applicazione del presente Manuale Operativo.

9.5.2. Proprietà del Manuale Operativo – Servizi di Certificazione digitale

Il presente Manuale Operativo è di proprietà di Bit4id S.r.l.; la traduzione, l'adattamento totale o parziale, la riproduzione con qualsiasi mezzo (comprese le fotocopie) nonché la memorizzazione elettronica sono riservate.

9.5.3. Proprietà dei marchi

Il nome "Bit4id" è un marchio registrato di proprietà esclusiva della Bit4id S.r.l. cui spettano tutti i diritti di proprietà intellettuale e di utilizzazione economica ai sensi della normativa attualmente vigente.
I Richiedenti garantiscono che l'utilizzo delle informazioni relative alla richiesta del certificato non interferiscono né danneggino i diritti di una qualsiasi terza parte, di qualunque giurisdizione, in

merito a marchi, marchi di identificazione di servizio, nomi commerciali, denominazioni societarie e ogni altro diritto di proprietà intellettuale.

I Titolari e i Richiedenti del certificato saranno tenuti a manlevare e indennizzare Bit4id contro qualunque perdita o danno derivanti dall'utilizzo del certificato e delle informazioni in esso contenute per scopi illegali, nell'ambito dei quali sono ricompresi, a titolo esemplificativo e non esaustivo, interferenze illecite su vantaggi contrattuali o potenziali vantaggi aziendali, concorrenza sleale, azioni volte a ledere la reputazione di altra persona, pubblicità ingannevole, e ingenerare confusione su persone fisiche o giuridiche.

9.6. Obblighi, Garanzie e responsabilità

9.6.1. Garanzie offerte da Bit4id

Fermo il rispetto degli obblighi di garanzia di cui al paragrafo 9.2, Bit4id si impegna a:

- erogare il servizio di certificazione in conformità alle disposizioni del Manuale Operativo;
- fornire un efficiente servizio di revoca dei certificati;
- fornire un servizio informativo efficiente ed affidabile sullo stato dei certificati;
- fornire informazioni chiare e complete sui requisiti e le condizioni del servizio;
- rendere disponibile una copia di questo Manuale a chiunque ne faccia richiesta;
- trattare i dati personali conformemente alle norme vigenti.

Inoltre:

a) provvede con certezza alla identificazione della persona che fa richiesta della certificazione. Con l'emissione del certificato, Bit4id attesta e garantisce che i dati identificativi, contenuti nel certificato erano, alla data di emissione del certificato, esatti e veritieri;
b) informa i Richiedenti, prima della sottoscrizione dell'accordo tra quest'ultimo e la CA, in modo completo e trasparente, delle condizioni che regolano la procedura di certificazione;
c) utilizza sistemi di sicurezza affidabili, finalizzati, non solo a garantire che soltanto le persone autorizzate possano compiere inserimenti e modifiche ma anche che l'autenticità delle informazioni sia verificabile;
d) garantisce il corretto funzionamento e la continuità del sistema;
e) si conforma alla normativa di cui al Regolamento (UE) n. 679/2016 e pubblica l'informativa ai sensi dell'art. 13 del citato Regolamento;
f) garantisce che i dati raccolti non vengano utilizzati o elaborati per fini diversi senza l'espresso consenso della persona alla quale si riferiscono.

9.6.2. Esclusione di garanzie

Bit4id non è responsabile e non si assume ulteriori obblighi eccetto quanto espressamente previsto dalla normativa vigente in materia ovvero rispetto a quanto indicato nel presente Manuale o nelle Condizioni Generali di Fornitura relative ai servizi di certificazione digitale.

9.6.3. Limitazioni di responsabilità

Bit4id è responsabile verso i Titolari, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dal Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 e successive modifiche ed integrazioni, dalla normativa italiana di settore, ove applicabile, (D.Lgs. 7 marzo 2005, n. 82 - Codice dell'Amministrazione Digitale e s.m.i., D.P.C.M. 22 febbraio 2013 e s.m.i., e ulteriori disposizioni normative e regolamentari pertinenti per materia), dal D.Lgs. n. 196/2003 nonché di quelle previste dal Regolamento UE 2016/679.

Salva l'applicazione della normativa su richiamata, le uniche ipotesi di responsabilità in capo a Bit4id sono circoscritte, esclusivamente, a quelle dettati dal presente Manuale e dal Contratto di fornitura relativo ai servizi di certificazione.

In nessun altro caso, per nessun titolo e/o ragione, Bit4id potrà essere ritenuta responsabile nei confronti del Richiedente e/o Titolare, ovvero verso altri soggetti, direttamente o indirettamente, connessi o collegati a questi ultimi, per danni, diretti o indiretti, perdite di dati, violazione di diritti di terzi, ritardi, malfunzionamenti, interruzioni, totali o parziali, che si dovessero verificare a fronte dell'erogazione del Servizio, ove connessi, direttamente o indirettamente, o derivanti da:

- cause di forza maggiore, caso fortuito, eventi catastrofici (a titolo esemplificativo ma non esaustivo: incendi, esplosioni, scioperi, sommosse, ecc.);
- manomissioni o interventi sul Servizio o sulle apparecchiature effettuati dal Titolare e/o dal Richiedente e/o da parte di terzi non autorizzati da Bit4id.

In particolare, ai sensi dell'art. 13 della normativa eIDAS richiamata dalla normativa ETSI EN 319 401 punto 7.1.1., Bit4id sarà responsabile unicamente per quei danni causati con dolo o negligenza nei confronti di qualsiasi persona fisica o giuridica in seguito al mancato adempimento degli obblighi di cui al Regolamento cit.

Va precisato, tuttavia, che ai sensi dell'art. 13 co. 2 è consentito alla CA di provare l'assenza della presunzione di responsabilità a suo carico se dimostra che il danno si è verificato senza suo dolo o negligenza.

9.6.4. Erogazione del Servizio e Assistenza

Funzionalità del Servizio	Livello di disponibilità	Modalità
Accesso all'archivio dei certificati	24x7	Fino a 6 anni
Sospensione/Revoca/Riattivazione	24x7	- Servizio di assistenza dalle ore 9 alle ore 18 (lun.-ven), esclusi i festivi. - Presso gli Uffici di registrazione secondo gli orari da essi indicati.
Rilascio	Orario di ufficio	Presso gli Uffici di registrazione secondo gli orari da essi indicati.

Con riferimento alle modalità di contatto del Centro Assistenza di Bit4id è possibile inoltrare tutte le richieste al seguente indirizzo di posta elettronica: assistenza-tsp@bit4id.com

9.6.5. Indennizzi a favore di Bit4id

Fermo quanto previsto dalle Condizioni Generali di Contratto relative ai servizi di certificazione, il Titolare si obbliga a risarcire i danni e le perdite, eventualmente sofferte da Bit4id, nelle ipotesi seguenti:

a) falsa dichiarazione nella richiesta del certificato (es. Falsità dei dati del Richiedente);
b) omissioni relativamente ad atti o fatti essenziali, sia nel caso di negligenza che in caso di omissione intenzionale;
c) custodia fallace dei dati di attivazione (es. PIN) della propria chiave privata;
d) utilizzo di nomi in violazione dei diritti di proprietà intellettuale di altri soggetti.

9.6.6. Indennizzi ai contraenti

Fermo quanto previsto dalle Condizioni Generali di Contratto relative ai servizi di certificazione, Bit4id dispone di un'apposita assicurazione a copertura dei rischi dell'attività associata all'erogazione dei servizi di certificazione (si veda il par. 9.2.1).

In caso di danno derivante dalle attività oggetto del Contratto, il Contraente dovrà, a pena di decadenza:

- farne denuncia a Bit4id entro 24 ore dal suo verificarsi, ovvero da quando ne abbia avuta conoscenza (facendo seguire conferma per lettera raccomandata A.R. oppure Posta Elettronica Certificata entro le 24 ore successive);
- entro sei mesi dall'inoltro della denuncia di cui al punto precedente, quantificare l'eventuale danno subìto e formulare la relativa richiesta di risarcimento.

9.6.7. Durata e risoluzione del contratto

Le disposizioni di cui al presente documento trovano applicazione dalla data dell'adesione da parte dell'Utente che usufruisca dei servizi fiduciari qualificati messi a disposizione di Bit4id e che si intendono dunque come integralmente accettati e perdurano sino alla scadenza del periodo di validità del certificato emesso dalla CA.

La durata del contratto è comunque subordinata al periodo di validità dei certificati digitali emessi dalla CA: tale circostanza determina, in caso di revoca del certificato, per qualsiasi motivo, l'immediata caducazione di tutti gli effetti del presente contratto.

Analoga conseguenza deriva dalla risoluzione del contratto che determina la revoca del certificato da parte della CA emittente.

9.6.8. Cessione del contratto

Non è consentito al Richiedente la cessione di tutto o parte degli obblighi e dei diritti nascenti dal presente contratto.

9.6.9. Legge applicabile

Il contratto tra la CA e il Richiedente e/o Titolare è soggetto alla Legge Italiana e come tale sarà interpretato ed eseguito. In relazione agli aspetti non espressamente previsti nel contratto, servizi di certificazione erogati da Bit4id sono sottoposti alle norme vigenti.

9.6.10. Foro competente

Per tutte le controversie nascenti dal presente Manuale Operativo, dai Termini e le Condizioni accettati dal Richiedente o da ulteriori eventuali contratti stipulati per la fruizione dei servizi messi a disposizione da Bit4id, compresi quelle inerenti alla loro esistenza, validità, estinzione, interpretazione, esecuzione e risoluzione sarà, competente in via esclusiva il Foro di Napoli, con espressa esclusione di ogni altro Foro concorrente.

9.7. Disposizioni finali

9.7.1. Modifiche al presente accordo

Il presente Manuale e le disposizioni in esso contenute sono suscettibili di essere modificate, integrate, sostituite o eliminate dalla predisponente in qualunque momento senza necessità di preavviso nei confronti dell'Utente, salvo il rispetto degli obblighi normativamente previsti in tema di pubblicità.

9.7.2. Intero accordo

Il presente Manuale è suscettibile di essere integrato o meno da Condizioni Generali o particolari di contratto sottoscritte specificamente dall'Utente, previo accordo con la CA, e costituisce la disciplina che regola l'utilizzo del certificato da parte del Titolare oltre che regolare i rapporti tra Titolare e CA.

La richiesta del certificato implica l'accettazione integrale e incondizionata delle disposizioni contenute all'interno del presente Manuale.

9.7.3. Forza maggiore

Bit4id non potrà essere ritenuta responsabile della mancata esecuzione delle obbligazioni assunte in forza delle disposizioni di cui al presente Manuale qualora tale mancata esecuzione sia dovuta a cause non imputabili alla stessa, quali - a titolo esemplificativo e non esaustivo - caso fortuito, disfunzioni di ordine tecnico assolutamente imprevedibili e poste al di fuori di ogni controllo, interventi dell'autorità, cause di forza maggiore, calamità naturali, scioperi anche aziendali - ivi compresi quelli presso soggetti di cui le parti si avvalgano nell'esecuzione delle attività connesse al servizio qui descritto - ed altre cause imputabili a terzi.

ALLEGATO A - SISTEMA DI VERIFICA DELLA VALIDITA' DEI CERTIFICATI

Indicazione del Sistema di verifica dei certificati

Bit4id, in conformità a quanto previsto dall'art. 14 co.1 del D.P.C.M. del 22 febbraio 2013 e dall'art. 32 del Regolamento eIDAS, fornisce ed indica ai soggetti interessati un applicativo che permette la verifica dei certificati (secondo gli standard CAdES, PAdES e XAdES) e/o delle marche temporali apposte ad un documento informatico.

In particolare, è messo a disposizione gratuitamente il seguente applicativo on-line, raggiungibile all'indirizzo:

https://vol.bit4idtsp.com/it

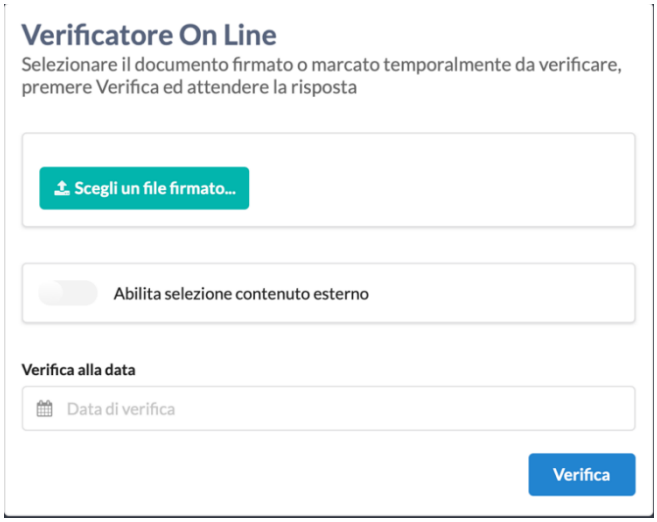
Il predetto software consente, nello specifico, di verificare:

a. l'integrità del documento firmato e i dati del soggetto firmatario (persona fisica o giuridica);
b. l'autenticità e l'affidabilità del certificato utilizzato per la firma del documento;
c. eventuali stati di sospensione o revoca dei certificati utilizzati per la firma.

Modalità operative per l'utilizzo dell'applicativo di verifica

Per poter procedere alla verifica dei certificati secondo le modalità che seguono è necessaria la presenza di una connessione ad internet.

Una volta raggiunta la pagina web dell'applicativo al link innanzi indicato l'utente si troverà di fronte la finestra visibile nell'illustrazione che segue:



- Sarà sufficiente, quindi, selezionare la casella "*Scegli un file firmato*" e scegliere, tra i documenti presenti sul computer locale dell'utente, il file da verificare;

- una volta selezionato il file da caricare, l'utente dovrà indicare la data in cui è stato firmato e/o marcato il documento ed infine cliccare sul tasto "*Verifica*" così da verificarne la validità;
- a questo punto, il software restituirà il risultato della verifica tramite visualizzazione di una schermata nel quale saranno indicati tutti i dati necessari alla verifica.
- L'utente, inoltre, potrà scaricare, tramite l'apposito pulsante "*Report PDF*" il *Rapporto di verifica*, ovvero un documento in formato PDF (visualizzabile tramite il programma gratuito Adobe Reader o similari) nel quale è riportato l'esito della procedura di verifica.

L'applicativo, presente all'indirizzo https://vol.bit4idtsp.com/it, consente all'utente di effettuare una verifica sui certificati di firma digitale o qualificata il cui risultato è pienamente conforme ai requisiti di cui all'art. 14 co. 2 del D.P.C.M. sopra richiamato.