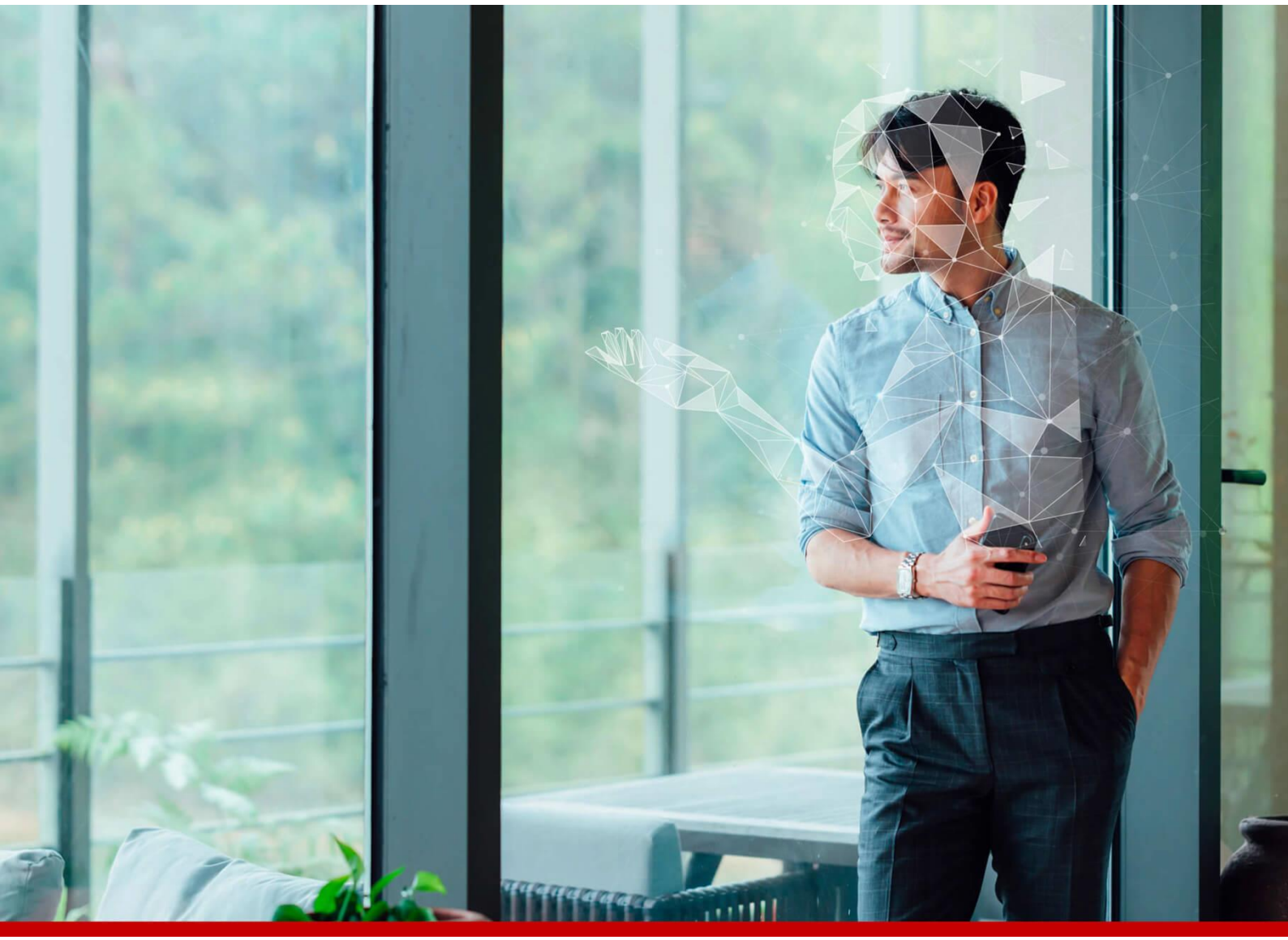


PKI Disclosure Statement

INFORMATIVA PER I CERTIFICATI DI FIRMA ELETTRONICA E SIGILLO ELETTRONICO QUALIFICATI

RELEASE 1.0 – 19/03/2026

INDICE

INFORMAZIONI GENERALI **2**

Controllo documentale 2

Controllo delle versioni 2

1. INFORMATIVA **3**

1.1. Introduzione 3

1.2. Nome del documento e regole di identificazione 3

1.3. Informazioni di contatto 3

1.3.1. Organizzazione 3

1.3.2. Emissione dei certificati 4

1.3.3. Contatto per le procedure di revoca 4

1.4. Tipologia di certificati 4

1.4.1. Verifica dei certificati 6

1.5. Finalità dei certificati 6

1.5.1. Previsioni comuni 6

1.5.2. Certificato qualificato di firma di persona fisica in QSCD 6

1.5.3. Certificato qualificato di firma di sottoscrizione “One-Shot” 7

1.5.4. Certificato qualificato di sigillo di persona giuridica in QSCD 8

1.6. Limiti di utilizzo del certificato 8

1.6.1. Limiti di utilizzo dei Titolari 8

1.6.2. Obblighi dei Richiedenti 9

1.7. Generazione delle chiavi 10

1.8. Richiesta dei certificati 10

1.9. Obblighi del Richiedente 10

1.10. Obblighi dei Titolari 10

1.10.1. Obblighi di custodia 10

1.10.2. Obblighi di uso corretto 11

1.11. Obblighi delle Relying Parties 11

1.11.1. Decisione informata 11

1.11.2. Requisiti di verifica della firma o del sigillo elettronico 11

1.11.3. Attendibilità di un certificato non valido 12

1.11.4. Effetto della verifica 12
1.11.5. Utilizzo corretto e attività proibite 12
1.11.6. Clausola d'indennità 12
1.12. Obblighi di Bit4id S.r.l. 13
1.12.1. Fornitura dei servizi di certificazione digitale 13
1.12.2. In relazione alle verifiche del registro 13
1.12.3. Periodo di conservazione 14
1.13. Garanzia 14
1.13.1. Garanzia di Bit4id S.r.l. per i servizi di certificazione digitale 14
1.14. Esclusioni della garanzia 15
2. ACCORDI APPLICABILI AL MANUALE OPERATIVO 16
2.1. Accordi applicabili 16
2.2. Manuale Operativo (CPS) 16
2.3. Politica sulla privacy 16
2.4. Politica di rimborso 17
2.5. Normativa applicabile e Foro competente 17
2.6. Elenco dei Prestatori di servizi fiduciari 17
2.7. Disposizioni finali, accordo integrale e notifiche 17

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:	PKI_Disclosure_Statement_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. INFORMATIVA

1.1. Introduzione

Il presente documento PKI Disclosure Statement (di seguito anche solo "*Informativa*" o "*Dichiarazione di Trasparenza*"), redatto in conformità con lo standard ETSI EN 319 411-1, costituisce parte integrante dei termini e delle condizioni contrattuali Bit4id S.r.l. (nel seguito "Bit4id") che opera in qualità di Prestatore di Servizi Fiduciari Qualificati relativamente alle operazioni di PKI ivi descritte.

L'informativa, redatta in conformità alla "*PDS structure*" di cui alla lett. A2 dell'Annex A contenuto nello standard ETSI sopra richiamata, contiene le informazioni essenziali da conoscere in relazione ai servizi di certificazione di Bit4id.

Per tutti i termini e le definizioni utilizzate all'interno del presente documento è possibile fare riferimento al Manuale Operativo di Bit4id disponibile al seguente indirizzo https://www.bit4id.com/documentazione-qtsp ovvero alle definizioni fornite dalla normativa applicabile in materia.

1.2. Nome del documento e regole di identificazione

Il presente documento è aggiornato alla versione risultante dal "*Controllo delle Versioni*" o dal "*Controllo Documentale*" di cui alle "*Informazioni Generali*" del presente documento.

Bit4id assicura una costante verifica e un costante aggiornamento del documento che tenga conto di ogni eventuale e successivo aggiornamento normativo.

Bit4id, inoltre, si impegna a rendere noto e disponibile il presente documento ai soggetti interessati tramite pubblicazione sul proprio sito web, laddove è sempre possibile consultare l'ultima versione approvata.

1.3. Informazioni di contatto

1.3.1. Organizzazione

Di seguito sono indicati i dati societari della Bit4id S.r.l. e relativi contatti:

BIT4ID S.R.L.

Sede legale: Via Diocleziano n. 107, 80125 - Napoli

Partita Iva (IT): 04741241212

Phone: +39 081 7625600

E-mail: info@bit4id.com

PEC: bit4id-tsp@sicurezzapostale.it

Sito Web: https://www.bit4id.com

1.3.2. Emissione dei certificati

I certificati descritti in questo documento sono erogati da Bit4id s.r.l., identificata mediante i dati sopra indicati (v.1.3.1. *infra*) e secondo le modalità indicate dal Manuale Operativo del Certificatore.

1.3.3. Contatto per le procedure di revoca

Per le richieste di revoca dei certificati, i Titolari e gli interessati possono rivolgersi a Bit4id tramite comunicazione inviata via PEC all'indirizzo del Certificatore (§1.3.1), secondo le modalità previste dal Manuale Operativo.

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

1.4. Tipologia di certificati

I certificati emessi da Bit4id sono qualificati in ottemperanza agli artt. 28 e 38 nonché all'Allegato I del Regolamento (UE) 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 (di seguito anche solo "Regolamento eIDAS") e sono conformi a quanto disposto dalla normativa tecnica di riferimento ETSI EN 319 411-1/2 nelle sue ultime versioni approvate.

L'*Object Identifier* (OID) che identifica la CA Bit4id è il seguente:

1.3.6.1.4.1.31898.10

La gerarchia OID per i certificati end-entity segue una struttura a 4 (quattro) sottolivelli:

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

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

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. del Manuale Operativo.

Bit4id si impegna, per ogni tipologia di certificato qualificato emesso, a rendere disponibile le CRL (*Certificate Revocation List*) per tutto il periodo di validità dei certificati in accordo con il punto 6.3.10 - 02 della ETSI 319 411-2.

1.4.1. Verifica dei certificati

La verifica dello stato dei certificati si realizza tramite:

- Acceso al servizio OCSP: http://ocsp.bit4idtsp.com/
- Download della CRL:
    - Per i certificati di tipo One Shot: http://crl.bit4idtsp.com/qc-oneshot-ecc-256-g1.crl
    - Per i certificati a curve ellittiche: http://crl.bit4idtsp.com/qc-ecc-256-g1.crl
    - Per i certificati a 3072 bit: http://crl.bit4idtsp.com/qc-rsa-4096-g1.crl

1.5. Finalità dei certificati

1.5.1. Previsioni comuni

I certificati qualificati descritti in questo documento garantiscono l'identità del firmatario e della persona fisica/giuridica indicata nel certificato, consentendo la generazione della "*firma elettronica qualificata*" o del "*sigillo elettronico qualificato*".

I suddetti certificati, emessi in QSCD (su Smartcard/Token o HSM – Firma remota), funzionano con dispositivi qualificati di creazione di firma, in accordo con il Regolamento eIDAS e in conformità a quanto disposto dalla normativa tecnica dell'Istituto Europeo per gli Standard nelle Telecomunicazioni EN 319 411-2 già citata.

1.5.2. Certificato qualificato di firma di persona fisica in QSCD

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

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. del Manuale Operativo) sia in caso di emissione su HSM (v. Par. 4.3.1.2. del Manuale Operativo), sono conformi alla politica di certificazione *QCP-n-qscd* con OID 0.4.0.194112.1.2, anche dichiarata nei certificati.

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

Essi 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 necessaria la sussistenza di ulteriori requisiti.

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

1.5.3. Certificato qualificato di firma 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. del Manuale Operativo.

1.5.4. Certificato qualificato di sigillo di persona giuridica in QSCD

Questi certificati sono contrassegnati 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.
Tali certificati, emessi in "*Qualified Seal Creation Device*" (di seguito anche solo "*QSealCD*" o anche "QSCD"), costituiscono certificati qualificati 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 "*Content commitment*" (non ripudio).

1.6. Limiti di utilizzo del certificato

1.6.1. Limiti di utilizzo dei Titolari

Il Titolare deve utilizzare il servizio di fornitura dei certificati erogato da Bit4id esclusivamente in conformità alle disposizioni del Manuale Operativo pubblicato sul sito web dell'organizzazione al seguente indirizzo https://www.bit4id.com/documentazione-qtsp e, comunque, per gli usi autorizzati nel contratto sottoscritto tra Bit4id e il Titolare.
Per ulteriori informazioni si invita il Titolare a consultare i termini e le condizioni generali di contratto dei servizi di certificazione, disponibile al seguente link: https://www.bit4id.com/documentazione-qtsp.

Parimenti, il Titolare si impegna a utilizzare il servizio di certificazione digitale in accordo con le istruzioni, i manuali e/o le procedure fornite da Bit4id.

Il Titolare deve attenersi a qualsiasi normativa e regolamentazione che possa influire sul suo diritto all'utilizzo degli strumenti crittografici che impiega.

I certificati possono essere utilizzati unicamente per le funzioni e le finalità stabiliti dal Manuale Operativo e dai termini e condizioni generali di contratto accettate dai Titolari al momento della richiesta del certificato, con espressa esclusione di qualsiasi altro utilizzo.

Ne consegue che i certificati non possono essere utilizzati per firmare certificati di chiave pubblica di nessun tipo, né firmare elenchi di revoca di certificati (CRL).

È fatto salvo il rispetto della normativa applicabile per l'utilizzo dei certificati.

Devono, inoltre, tenersi in conto dei limiti indicati nei diversi campi dei profili dei certificati, per il cui dettaglio si rinvia al Manuale Operativo di Bit4id, disponibile al seguente indirizzo: https://www.bit4id.com/documentazione-qtsp.

In caso di utilizzo dei certificati in violazione delle disposizioni contenute all'interno del presente documento o in violazione delle disposizioni sopra richiamate, il Titolare sarà tenuto a manlevare Bit4id da qualsiasi responsabilità dovesse sorgere relativamente all'utilizzo illegittimo dei certificati, in conformità alla normativa vigente.

Bit4id conserverà, per un periodo pari a 20 (venti) anni decorrenti dalla scadenza e/o dalla revoca del certificato, in accordo con la normativa applicabile, le seguenti informazioni sui certificati:

- le informazioni sui soggetti relative alle procedure di identificazione e registrazione;
- le informazioni sul ciclo di vita dei certificati;
- registri di eventi significativi per fini di sicurezza.

Ulteriori informazioni sulla conservazione sono indicate nei paragrafi successivi, nel Manuale Operativo fatta salva la facoltà, per i Titolari, di richiedere chiarimenti o informazioni a Bit4id agli indirizzi contenuti all'interno dell'Informativa sul trattamento dei dati personali.

1.6.2. Obblighi dei Richiedenti

I Richiedenti, ovvero coloro che richiedono l'emissione di un certificato qualificato a Bit4id, sono tenuti a conformarsi alle disposizioni di cui alla presente informativa, al Manuale Operativo, ai Termini e alle Condizioni accettate in fase di conclusione del contratto ed altre eventuali regole stabilite dalla CA, le quali sono messe adeguatamente e pubblicamente a disposizione dei Richiedenti.

1.7. Generazione delle chiavi

Il Richiedente autorizza Bit4id a gestire, in accordo con le politiche di certificazione descritte nel presente documento e nel Manuale Operativo, l'emissione di chiavi pubbliche/private legate al certificato richiesto nelle forme e con le modalità previste dal Manuale Operativo di Bit4id.

1.8. Richiesta dei certificati

Il Richiedente si impegna a soddisfare i requisiti definiti da Bit4id per la richiesta di certificati qualificati. Tale richiesta avviene in accordo con la procedura definita da Bit4id e in conformità con quanto stabilito nel Manuale Operativo e nella restante documentazione contrattuale di Bit4id cui espressamente si rinvia per la relativa disciplina.

1.9. Obblighi del Richiedente

Il Richiedente del certificato è responsabile circa la veridicità e la completezza di tutte le informazioni fornite all'atto della richiesta del certificato.

Il Richiedente deve informare immediatamente Bit4id in merito a:

- qualsiasi inesattezza rilevata nel certificato una volta che sia stato emesso;
- cambiamenti che si verifichino nelle informazioni riportate e/o registrate per l'emissione del certificato;
- perdita, del furto o di qualsiasi altro tipo di perdita di controllo della chiave privata da parte del Titolare.

Inoltre, il Richiedente è tenuto a verificare la data indicata all'interno del certificato.

1.10. Obblighi dei Titolari

1.10.1. Obblighi di custodia

Il Titolare si impegna a conservare, con la dovuta premura ed attenzione, eventuali dispositivi e/o codici segreti forniti da Bit4id.

In caso di perdita o di furto della chiave privata del certificato o nel caso in cui il Titolare sospetti che la chiave privata abbia perso affidabilità per qualsiasi motivo, tali circostanze devono essere immediatamente notificate a Bit4id, direttamente o per il tramite della RA di riferimento.

1.10.2. Obblighi di uso corretto

Il Titolare deve utilizzare i certificati digitali forniti da Bit4id esclusivamente per gli usi autorizzati nel Manuale Operativo e in qualsiasi altra istruzione, manuale o procedimento fornito al momento della richiesta di emissione e presente sul sito internet https://www.bit4id.com/documentazione-qtsp.
Il Titolare deve attenersi a qualsiasi normativa e regolamentazione che possa influire sul suo diritto all'utilizzo degli strumenti crittografici che impiega.
Il Titolare non può impiegare mezzi di controllo, alterazione o decompilazione dei servizi di certificazione digitale erogati.
Il Titolare, inoltre, si impegna:

a) ad attenersi alle suddette disposizioni circa l'utilizzo del certificato;
b) in caso di eventuale compromissione della chiave privata, a interrompere immediatamente e permanentemente il suo utilizzo e procedere alle opportune notifiche riportate in questo documento.

1.11. Obblighi delle Relying Parties

1.11.1. Decisione informata

Bit4id assicura alle *Relying Parties* (ovvero coloro che fanno affidamento o richiedono la verifica della validità del certificato) l'accesso a tutte le informazioni sufficienti a consentire loro di prendere una decisione informata al momento della verifica di un certificato assicurando, al contempo, la completezza delle informazioni ivi contenute.
Le *Relying Parties* riconoscono che l'uso del registro e degli elenchi di revoca dei Certificati ("CRL") di Bit4id sono disciplinati dal Manuale Operativo di Bit4id e si impegnano ad adempiere ai requisiti tecnici, operativi e di sicurezza descritti nel predetto Manuale.

1.11.2. Requisiti di verifica della firma o del sigillo elettronico

La verifica potrà essere eseguita dal software di verifica messo a disposizione di Bit4id e, in ogni caso, in accordo con il Manuale Operativo con i requisiti seguenti:

- l'utilizzo di un software o di un applicativo appropriato per la verifica, capace di effettuare le operazioni crittografiche necessarie utilizzando algoritmi e lunghezze di chiavi indicate nel certificato;
- verifica dello stato di revoca dei certificati della catena di "*trust*" con l'informazione fornita al Registro di Bit4id (con CRL per esempio) per determinare la validità di tutti i certificati della catena di certificati, dal momento che può unicamente considerarsi verificata

correttamente una firma elettronica se tutti e ognuno dei certificati della catena sono corretti e sono in vigore;

- verifica tecnica della firma di tutti i certificati della catena prima di accertare il certificato utilizzato dal Titolare.

Bit4id mette a disposizione delle *Relying Parties*, un applicativo (raggiungibile al seguente indirizzo: https://vol.bit4idtsp.com/it) che consente la verifica dei certificati qualificati di firma e sigillo elettronico: le caratteristiche e la relativa procedura di utilizzo di tale applicativo vengono descritte nell'Allegato A al Manuale Operativo di Bit4id.

1.11.3. Attendibilità di un certificato non valido

Bit4id non potrà, in nessun caso, essere ritenuta responsabile nel caso in cui le *Relying Parties* considereranno attendibile un certificato non valido; in tale evenienza, infatti, queste ultime si assumeranno tutti i rischi derivanti e derivati da tale comportamento.

1.11.4. Effetto della verifica

In virtù della corretta verifica dei certificati in conformità con questa informativa, le *Relying Parties* possono avere certezza dell'identificazione e, in tal caso, della paternità della chiave pubblica del Titolare entro i limiti d'uso corrispondenti.

1.11.5. Utilizzo corretto e attività proibite

Le *Relying Parties* si impegnano a non utilizzare alcuna informazione relativa ai certificati o di nessun altro tipo che sia stata fornita da Bit4id nella realizzazione di transazioni vietate per legge.

I servizi di certificazione digitale erogati da Bit4id non sono stati progettati né permettono l'utilizzo o la rivendita come apparecchiature di controllo per situazioni pericolose non autorizzate o per usi che richiedano azioni soggette a errore, quali le operazioni di installazioni nucleari, sistemi di navigazione, comunicazione aerea o sistemi di controllo degli armamenti, ove un errore possa causare la morte, danni fisici o danni ambientali gravi.

1.11.6. Clausola d'indennità

Il terzo che verifica la validità del certificato s'impegna a mantenere indenne Bit4id da tutti i danni provenienti da qualunque azione o omissione che si concretizzi nella responsabilità, nel danno, nella perdita o in un costo di qualunque tipo, compresi quelli legali e di assistenza legale nella quale possano incorrere, per la pubblicazione e l'uso del certificato, quando concorra una delle cause seguenti:

- inadempimento degli obblighi da parte del terzo che accerta il certificato;

- autorizzazione imprudente di un certificato a seconda delle circostanze;
- mancato accertamento dello stato di un certificato per determinare che non sia stato sospeso o revocato;
- mancato accertamento della totalità delle misure assicurative prescritte nel Manuale Operativo.

1.12. Obblighi di Bit4id S.r.l.

1.12.1. Fornitura dei servizi di certificazione digitale

Bit4id si impegna a:

a. emettere, consegnare, gestire, sospendere, riattivare, revocare e rinnovare i certificati in accordo con le informazioni fornite dal Richiedente e/o dal Titolare nei casi, nelle modalità e per i motivi descritti nel Manuale Operativo di Bit4id;
b. eseguire i servizi con i mezzi tecnici e materiali adeguati e con personale che rispetti le condizioni di qualifica e d'esperienza stabilite nel Manuale Operativo;
c. rispettare i livelli di qualità del servizio, in conformità con quanto stabilito nel Manuale Operativo per quanto riguarda gli aspetti tecnici, operativi e di sicurezza;
d. notificare al Richiedente e al Titolare, anteriormente alla data di scadenza dei certificati, la possibilità di rinnovarli, così come la sospensione, la proroga della sospensione, la riattivazione o la revoca dei certificati, qualora si manifestino le suddette circostanze;
e. comunicare ai terzi che ne facciano richiesta lo stato dei certificati in accordo con quanto stabilito nel Manuale Operativo per i diversi servizi di verifica dei certificati.

1.12.2. In relazione alle verifiche del registro

Bit4id emetterà i certificati in base ai dati e alle informazioni fornite dai Richiedenti: a tal fine ha adottato una rigida procedura di identificazione dei Richiedenti, in conformità alla normativa vigente, accuratamente descritta nel Manuale Operativo, con la quale effettuerà le opportune verifiche per l'accertamento dell'identità e delle altre informazioni personali e complementari dei Richiedenti.

Tali verifiche potranno includere qualsiasi altro documento e informazione rilevante fornita dal Richiedente e/o dal firmatario.

Nel caso in cui Bit4id riscontri errori nei dati che si devono includere nei certificati, prima di emettere il certificato o sospendere il processo di emissione potrà apportare le modifiche che consideri necessarie solo dopo aver gestito il caso con il Richiedente.

Bit4id si riserva il diritto di non emettere il certificato qualora consideri che la giustificazione documentale sia insufficiente per la corretta identificazione e autenticazione del Richiedente e/o del firmatario.

Gli obblighi precedenti sono sospesi nei casi nei quali il Richiedente agisca come autorità di registrazione e disponga degli elementi tecnici inerenti alla generazione delle chiavi, all'emissione dei certificati e alla registrazione dei dispositivi di firma aziendale.

1.12.3. Periodo di conservazione

Bit4id archivia le registrazioni corrispondenti alle richieste di emissione e di revoca dei certificati per almeno 20 anni, in conformità con la normativa applicabile.

Bit4id conserverà le informazioni dei log per un periodo compreso tra 1 e 20 anni in funzione del tipo di informazione registrata in accordo a quanto previsto dalle politiche di certificazione di cui al Manuale Operativo.

Per ulteriori informazioni sui periodi di conservazione si invita a consultare il Manuale Operativo.

1.13. Garanzia

1.13.1. Garanzia di Bit4id S.r.l. per i servizi di certificazione digitale

Bit4id garantisce al Titolare:

a. che non ci siano errori di fatto nelle informazioni contenute nei certificati rispetto a quelle fornite;
b. che non ci siano errori di fatto nelle informazioni contenute nei certificati dovute a mancanza della dovuta diligenza nella gestione della richiesta del certificato o nella creazione dello stesso;
c. che i certificati rispettino tutti i requisiti materiali stabiliti nel Manuale Operativo;
d. che i servizi di revoca rispettino tutti i requisiti materiali stabiliti nel Manuale Operativo.

Bit4id garantisce ai terzi che fanno affidamento sulla validità dei certificati:

a. che le informazioni contenute o incluse come riferimento nel certificato siano corrette, tranne quando sia indicato il contrario;
b. che nell'approvazione della richiesta di certificato e nell'emissione del certificato siano stati rispettati tutti i requisiti materiali stabiliti nel Manuale Operativo;
c. la disponibilità delle informazioni afferenti allo stato del certificato (CRL/OCSP).

In aggiunta, Bit4id garantisce al Richiedente e al terzo che fa affidamento sulla validità dei certificati:

- che il certificato qualificato per la firma o per il sigillo contenga le informazioni che debba contenere un certificato qualificato, in accordo con quanto stabilito negli artt. 28 e 38 del Regolamento (UE) 910/2014 e in conformità a quanto disposto dalla normativa tecnica identificata con il riferimento ETSI EN 319 411-2;
- che, nel caso in cui si generi la chiave privata del Richiedente o, all'occorrenza, della persona fisica identificata nel certificato, se ne mantenga la confidenzialità durante il processo;
- la responsabilità dell'Autorità di Certificazione, con i limiti previsti.

In nessun caso Bit4id risponderà per caso fortuito o per forza maggiore.

1.14. Esclusioni della garanzia

Bit4id rigetta tutte le altre garanzie diverse alla precedente che non siano legalmente esigibili.

In particolare, Bit4id non risponde dell'uso di software di terze parti.

2. ACCORDI APPLICABILI AL MANUALE OPERATIVO

2.1. Accordi applicabili

Gli accordi applicabili ai certificati sono i seguenti:

- Condizioni generali di contratto per i servizi di certificazione digitale disciplinanti il rapporto tra Bit4id e il Richiedente/Titolare dei certificati disponibile al seguente indirizzo https://www.bit4id.com/documentazione-qtsp;
- Condizioni generali del servizio ed informative incluse in questo documento;
- Manuale Operativo che disciplina la fornitura dei servizi di certificazione (v. par. 2.2. infra);
- eventuali ulteriori Moduli e/o documentazione contrattuale espressamente richiamati dai documenti di cui sopra.

2.2. Manuale Operativo (CPS)

I servizi fiduciari di Bit4id sono regolati tecnicamente e operativamente dal Manuale Operativo per i servizi di certificazione, dagli aggiornamenti successivi così come dalla documentazione complementare.

La documentazione è modificata periodicamente e può essere consultata al sito internet https://www.bit4id.com/documentazione-qtsp.

2.3. Politica sulla privacy

Bit4id, con riferimento al trattamento dei dati personali, si conforma alla normativa vigente in materia, sia nazionale che comunitaria, con particolare riferimento al D.lgs. 196/03, e s.m.i., ed il Regolamento (UE) 2016/679 (di seguito anche solo "GDPR").

Bit4id non può divulgare né può essere obbligata a divulgare informazioni confidenziali a meno di una richiesta specifica proveniente da:

a) dall'interessato, ovvero la persona rispetto alla quale Bit4id ha l'obbligo di mantenere le informazioni confidenziali, o
b) un mandato giudiziario, amministrativo o di qualsiasi altro genere previsto dalla legislazione vigente.

Bit4id, in conformità a quanto disposto dall'art. 13 del GDPR, ha predisposto e reso disponibile una precisa Informativa sul Trattamento dei Dati Personali che descrive i trattamenti effettuati da Bit4id, in qualità di Titolare del Trattamento, relativamente all'erogazione dei servizi fiduciari.

L'Informativa in formato esteso è disponibile sul sito internet all'indirizzo: https://www.bit4id.com/documentazione-qtsp.

2.4. Politica di rimborso

Per la Politica di rimborso è necessario fare riferimento alle Condizioni Generali del Servizio di Bit4id, fornite in fase di richiesta del servizio e pubblicate sul sito https://www.bit4id.com/documentazione-qtsp .

2.5. Normativa applicabile e Foro competente

Le relazioni con Bit4id sono disciplinate esclusivamente dalla normativa italiana.

In caso di disaccordo tra le parti, queste tenteranno la conciliazione amichevole. A tal fine le parti dovranno indirizzare una comunicazione a Bit4id tramite uno dei contatti indicati nel presente documento.

Per il Foro competente si rinvia al Manuale Operativo di Bit4id che qui abbia a intendersi come integralmente richiamato e trascritto.

2.6. Elenco dei Prestatori di servizi fiduciari

Di seguito si riporta il link attraverso il quale è possibile consultare la lista dei prestatori di servizi fiduciari attivi in Italia: https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia.

2.7. Disposizioni finali, accordo integrale e notifiche

Le clausole della presente informativa sono indipendenti tra di loro, ragione per la quale se qualsivoglia clausola è considerata invalida o inapplicabile le restanti clausole del Manuale Operativo continueranno a essere applicabili.

Questo testo esprime la volontà completa e tutti gli accordi tra le parti.

Le notifiche tra le parti avvengono tramite l'invio di mail all'indirizzo indicato dal Titolare nel contratto con Bit4id.