TrustPro	Code	Revision	Title
	QTSP-CP/CPS	08	Certificate Policy Certificate Practice Statement
	Date		Classification
	1O-Apr-2024		Public

Manuale operativo

Data	Rev	Descrizione delle modifiche
1-Mar-201 9	01	Primo rilascio
28-Mar-201 9	02	3.5 – Riformulazione e modifiche minori 5.2.1 - aggiunto RAO ai ruoli attendibili
1-7-May-2019	03	Modificati il supporto, I documenti ed i certificati dell'URL
20-May-2020	04	3.2.3 - Riformulazione 3.2.5 - Riformulazione ed aggiunta dell'identificazione remota mediante l'impiego dei criteri eiDAS di identificazione
4-Jun-2021	05	4.9 – Aggiunto periodo di conservazione per I certificate revocati e OIDs ExpiredCertsOnCRL , ArchiveCutOff
13-Jul-2021	06	4.9 - dettagli sulla pubblicazione della CRL in caso di risoluzione o compromissione della chiave
12-Feb-2022	07	7.1 .7 – Aggiunta informativa sui certificati 0.4.0.1941 1 2.1 .0 (QCP-n), 0.4.0.1941 12.1.1, (QCP-1), 0.4.0.1941 12.1.2 (QCP-n-qscd) , 0.4.0.1941 12.1.3 (QCP-1-qscd)
1 O-Apr-2024	08	3.2.5 - rimodulazione del processo di identificazione remota per chiarire che tutte le identità siano verificate da un agente

1. Introduzione

Questo documento contiene la Dichiarazione sulla Politica Integrata per i Certificati Qualificati e le Pratiche di Certificazione, relativa al servizio di certificazione qualificata dell'Autorità di Certificazione TrustPro QTSP Ltd (di seguito il Provider).
Il Provider fornisce i suoi servizi ai Clienti nell'ambito di un rapporto contrattuale.
Il presente documento descrive il quadro per la fornitura dei suddetti servizi, include le procedure dettagliate e le regole operative varie, e formula raccomandazioni per le Parti Affidanti per la verifica delle firme elettroniche e dei Certificati creati dai servizi.
Questo documento è conforme ai requisiti stabiliti dal Regolamento eIDAS; il servizio fornito secondo queste normative è un servizio fiduciario qualificato dell'UE.
TrustPro QTSP Ltd è registrata come fornitore di servizi fiduciari dal DCCAE - Department of Communications, Climate Action and Environment.

1.1. Panoramica

Questo documento riassume tutte le informazioni che i Clienti dovrebbero conoscere. L'obiettivo è favorire che:

- I Clienti e i futuri Clienti familiarizzino meglio con i dettagli e i requisiti dei servizi forniti dal Provider, e con il contesto pratico dell'erogazione del servizio;
- I Clienti siano in grado di comprendere il funzionamento del Provider, e quindi possano decidere più facilmente se i servizi sono conformi, o quale tipo di servizi soddisfa le loro esigenze e aspettative individuali.

Inoltre, contiene un insieme di regole che specificano l'usabilità di un Certificato per una comunità e/o una classe di applicazioni con requisiti di sicurezza comuni, e informazioni per aiutare gli utenti e gli accettanti di Certificati, gli elenchi di revoca dei Certificati e le risposte online sullo stato dei Certificati, in merito a come vengono gestiti, al livello di sicurezza garantito, nonché alle garanzie tecniche, commerciali, finanziarie e alla responsabilità legale pertinenti e correlate. Il contenuto e il formato del presente documento sono conformi ai requisiti del framework RFC 3647.
I requisiti per l'attività dell'utente finale relativi ai servizi utilizzati possono essere contenuti, oltre che nel presente documento, nelle Condizioni Generali del contratto di servizio stipulato con il provider, nelle Politiche di Certificato applicate dal Provider, e in altri regolamenti o documenti indipendenti dal Provider stesso.

1.2. Nome e identificazione del documento

Emittente	TrustPro QTSP Ltd Certification Authority
Nome del documento	Qualified Certificate Certification Practice Statement - Certificate Policy
Codice	QTSP -CP/C PS
Versione	1.0
Data di efficacia	01-03-2019
OID (Iana PEN)	1.3.6. l.4.1.52969

1.2.1. Effetti

Il presente documento deve essere rivisto almeno una volta all'anno e deve essere garantito il suo adeguamento ai requisiti e ai prerequisiti potenzialmente modificati.

Ambito oggettivo	Questo documento è stato redatto dal provider per scopi informativi, descrivendo il rilascio di certificati per firme digitali.
Ambito temporale	La presente versione di questo documento è efficace dalla data di entrata in vigore fino al recesso. L'efficacia cessa automaticamente alla cessazione dei servizi.
Ambito soggettivo	Gli effetti del presente documento si estendono a tutti I partecipanti di cui alla sezione 1 .3.
Ambito geografico	Il presente Manuale operativo include requisiti specifici per i servizi forniti principalmente a clienti europei, operanti in conformità al diritto europeo. Il Fornitore può estendere l'ambito geografico del servizio; in tal caso, dovrà utilizzare requisiti non meno rigorosi di quelli applicabili alle condizioni europee.

1.3. Partecipanti

Di seguito trovi un elenco dei partecipanti che usufruiscono dei servizi nell'ambito di questo documento:

- TrustPro QTSP Ltd Autorità di Certificazione e Autorità di Registrazione
- Le Autorità di Registrazione Locali che hanno un rapporto contrattuale con TrustPro QTSP Ltd Autorità di Certificazione,
- i Clienti di TrustPro QTSP Ltd Autorità di Certificazione (Sottoscrittori e Soggetti),
- le parti affidanti
- altri partecipanti.

1.3.1. TrustPro QTSP Autorità di Certificazione.

TrustPro QTSP Autorità di Certificazione (CA) è l'entità che rilascia Certificati all'interno del quadro del Trust Service Provider TrustPro QTSP ed esegue i compiti correlati. TrustPro QTSP CA identifica la persona richiedente, gestisce i registri, accetta le modifiche relative ai Certificati e pubblica le politiche relative ai Certificati, alle chiavi pubbliche e le informazioni sullo stato attuale del Certificato (in particolare sulla sua possibile revoca o sospensione).

Provider data

Nome	TrustPro QTSP Certification Authority
Società	TrustPro QTSP Ltd
Sede legale	Guinness Enterprise Centre Taylor' s Lane, Dublin 8 lreland, 008 N9EX

Telefono	+353 1486 1 130
Sito Web	https://www.trustpro.eu
Servizio clienti 24/h	https://support.trustpro.eu

TrustPro QTSP Ltd è un fornitore di servizi fiduciari qualificato ai sensi del Regolamento 910/2014/UE (di seguito: eIDAS), stabilito in Irlanda e opera come unità aziendale indipendente. L'Autorità di Certificazione TrustPro QTSP ha la propria Autorità di Registrazione e può operare anche con una rete di Autorità di Registrazione Locali.

TrustPro QTSP sottolinea l'importanza dell'esperienza del Cliente e della sicurezza. Al fine di mantenere un elevato livello di servizi, il Provider esternalizza i servizi preferibilmente a società con un sistema di gestione della qualità conforme allo standard ISO 9001 e un sistema di gestione della sicurezza delle informazioni conforme allo standard ISO 27001.
Le interfacce dei servizi di certificazione per i Sottoscrittori sono accessibili alle persone con disabilità secondo gli standard W3C.
Il Provider fornisce i seguenti servizi fiduciari definiti dal regolamento eIDAS nell'ambito della presente Dichiarazione sulle Pratiche di Certificazione:

- Certificati qualificati per Firme Elettroniche (art. 28 regolamento eIDAS) e servizi correlati. Policy supportate: QCP-n e QCP-n-qscd
- Certificati qualificati per Sigilli Elettronici (art. 38 regolamento eIDAS) e servizi correlati. Policy supportate: QCP-1 e QCP-1-qscd

1.3.2. Autorità di registrazione e autorità di registrazione locali

L'Autorità di Registrazione opera come parte contrattuale del Prestatore di Servizi Fiduciari. L'Autorità di Registrazione opera direttamente o tramite Autorità Locali di Registrazione formalmente delegate.
Il Prestatore di Servizi Fiduciari è in ogni caso responsabile del corretto funzionamento dell'Autorità di Registrazione. Il Prestatore di Servizi Fiduciari dovrà obbligare contrattualmente l'Autorità Locale di Registrazione a conformarsi ai requisiti pertinenti. L'elenco delle Autorità Locali di Registrazione attive è disponibile sul sito web di TrustPro QTSP.
L'Autorità Locale di Registrazione sarà formalmente istruita dal Prestatore di Servizi Fiduciari ed è soggetta ad audit da parte del Prestatore di Servizi Fiduciari.
Compiti dell'ufficio:

- identificazione e registrazione del Soggetto indicato sui Certificati dell'utente finale
- attività di amministrazione e registrazione relative all'emissione di Certificati e Dispositivi per la Creazione di Firme Elettroniche
- mantenimento del contatto con i Clienti (ricezione di domande, annunci, richieste e reclami, e avvio della loro elaborazione)
- esecuzione delle azioni sui certificati (revoca, sospensione, reinstallazione, rinnovo del certificato, modifica del certificato e rifacimento della chiave).

Il Prestatore mantiene un servizio continuamente disponibile per l'avvio della revoca o sospensione dei certificati - 24 ore al giorno, tutti i giorni della settimana.
L'Autorità di Registrazione e le Autorità Locali di Registrazione possono svolgere attività di registrazione ovunque sia necessario, incluse le sedi dei clienti.
Qualsiasi comunicazione tra l'Autorità Locale di Registrazione, l'Autorità di Registrazione e l'Autorità di Certificazione è autenticata da un certificato di autenticazione del cliente rilasciato

dall'Autorità di Certificazione.

1.3.3. Sottoscrittori

I Sottoscrittori definiscono l'ambito dei Soggetti che utilizzano il servizio e i Sottoscrittori coprono anche le tariffe di servizio relative all'utilizzo di questi servizi. Il Soggetto è quella persona fisica i cui dati sono indicati sul Certificato. Soggetto e Sottoscrittore possono essere la stessa persona.
Nel caso di un Certificato emesso per la firma elettronica, il Soggetto è anche il Firmatario.
I Clienti dei servizi forniti dal Prestatore:

- Sottoscrittore:
  - conclude un contratto di servizio con il Prestatore,
  - definisce l'ambito dei Soggetti,
  - è responsabile del pagamento delle tariffe derivanti dall'utilizzo del servizio.
- Soggetto: il Prestatore che rilascia il Certificato per il Soggetto.
- Firmatario: l'utente del servizio di certificazione di firma elettronica, che può creare una firma elettronica con l'aiuto del Certificato rilasciato.

1.3.4. Parti affidanti

Le parti affidanti non hanno necessariamente un rapporto contrattuale con il prestatore. Il Prestatore mantiene i contatti con le parti affidanti, principalmente attraverso il suo sito web.

1.3.5. Altri partecipanti

L'Organizzazione Rappresentata, il cui nome è indicato in un Certificato rilasciato a una persona fisica.
Il Prestatore di Servizi Fiduciari non ha necessariamente un rapporto contrattuale con l'Organizzazione Rappresentata ma il Prestatore di Servizi Fiduciari non deve rilasciare un Certificato Organizzativo senza l'approvazione di tale Organizzazione. Il Prestatore di Servizi Fiduciari può revocare il Certificato su richiesta dell'Organizzazione Rappresentata.
Se un Certificato è stato rilasciato al Soggetto per essere utilizzato in rappresentanza di un'Organizzazione (Certificato dell'rganizzazione rilasciato a persona fisica) per la firma o per la sua attività, l'Organizzazione Rappresentata è l'Organizzazione indicata anche all'interno del Certificato.
Il Prestatore definisce obblighi reciproci nel rapporto contrattuale con le aziende che forniscono servizi relativi alle attività della CA (Certification Authority).

1.4. Utilizzo del certificato.

L'area di usabilità del certificato è determinata essenzialmente dai valori degli attributi del certificato impostati dal fornitore di servizi fiduciari. La Certificate Policy e la Certification Practice Statement possono contenere anche ulteriori restrizioni.

1.4.1. Utilizzo corretto del certificato

Le chiavi private appartenenti all'utente finale, legate ai Certificati rilasciati dal Prestatore in base al presente Manuale Operativo, possono essere utilizzate solo per la creazione di firme elettroniche o la creazione di sigilli elettronici in conformità con la Certificate Policy. Il certificato consente la verifica che il documento sia stato firmato o vi sia apposto il sigillo dalla persona descritta nel Certificato.
Nel caso di Certificate Policies che richiedono l'utilizzo di un Dispositivo Qualificato per la Creazione di Firma Elettronica, la chiave privata appartenente al Certificato qualificato è protetta

da un Dispositivo Qualificato per la Creazione di Firma Elettronica. I Certificati rilasciati secondo queste politiche sono idonei per la generazione di Firma Elettronica Qualificata.
Nel caso di Certificate Policies che richiedono l'utilizzo di un Dispositivo Qualificato per la Creazione di Sigillo Elettronico, la chiave privata appartenente al Certificato qualificato è protetta da un Dispositivo Qualificato per la Creazione di Sigillo Elettronico. I Certificati rilasciati secondo queste Policies sono idonei per la generazione di Sigillo Elettronico Qualificato

1.4.2. Utilizzo vietato del certificato

Certificato del Fornitore.
Il Certificato radice del fornitore e le chiavi private associate non devono essere utilizzati per il rilascio di Certificati prima della divulgazione del Certificato del fornitore.

Certificati dell'Utente Finale.
È vietato l'utilizzo dei Certificati rilasciati in conformità con le presenti Certificate Policies, e delle chiavi private ad essi associate, per scopi diversi dalla generazione e verifica di firme elettroniche e sigilli elettronici

1.5. Disposizioni di amministrazione

1.5.1 Soggetto responsabile dei documenti

L'organizzazione che si occupa della Certification Practice Statement è TrustPro QTSP Certification Authority, come definito nella sezione.

1.5.2 Contatti

Tutte le domande relative al presente Manuale Operativo possono essere indirizzate a info@trustpro.eu

1.5.3 Soggetto Responsabile dell'Idoneità delle specifiche tecniche dei Certificati di Firma Qualificata

Il fornitore che ha emesso la Certification Practice Statement è responsabile della sua conformità con la Policy dei Certificati di Firma Qualificata ivi richiamata e della fornitura del servizio in base ai regolamenti ivi contenuti.
Le Certification Practice Statements e la fornitura dei servizi sono supervisionate dal Department of Communications, Climate Action and Environment (DCCAE), di seguito Autorità Nazionale.

1.5.4 Procedure di Approvazione CP-CPS

L'approvazione e l'emissione delle versioni nuove o modificate di questo documento sono sotto il controllo del comitato direttivo di TrustPro QTSP. 1.6

1.6. Definizioni a Acronimi

1.6.1. Definizioni

Unità di certificazione	Un'unità operativa del sistema del Prestatore di Servizi Fiduciari che firma i Certificati. A un'Unità di Certificazione appartiene sempre un solo Dato per la Creazione di Certificati (chiave di firma, dati per la creazione della firma). È possibile che un'Autorità di Certificazione operi simultaneamente con diverse Unità di Certificazione.
Firma elettronica avanzata	Una firma elettronica avanzata soddisfa i seguenti requisiti: è connessa unicamente al firmatario; è idonea a identificare il firmatario; è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.
Richiedente	La persona fisica che agisce durante la richiesta del Certificato in questione.
Certificato	Il certificato di firma elettronica, il certificato di sigillo elettronico e il certificato di autenticazione del sito web, e tutte quelle verifiche elettroniche rilasciate nell'ambito del Servizio Fiduciario dal fornitore di servizi, che include i dati di verifica relativi al certificato e le informazioni relative all'utilizzo del certificato, e che, come documento elettronico, è protetto in modo affidabile contro le tecnologie di contraffazione disponibili al momento del rilascio e durante il suo periodo di validità.
Richiesta di certificato	I dati e le dichiarazioni forniti dal Richiedente al Prestatore di Servizi Fiduciari per il rilascio del Certificato, in cui il Richiedente riafferma l'autenticità dei dati da indicare sul Certificato.
Certificato automatico	Un Certificato in cui il nome del dispositivo IT (applicazione, sistema) utilizzato dal Soggetto per impiegare il Certificato deve essere registrato tra i dati del Soggetto
Certificato per la firma elettronica	Si intende un'attestazione elettronica che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona. Nel caso dei Certificati rilasciati dal Prestatore di Servizi Fiduciari, dalla Certificate policy relativa ai Certificati si può chiaramente desumere se il dato Certificato sia pseudonimo o meno. Il riferimento Certificate policy è nel Certificato.
Certificate Policy	La Policy del Servizio Fiduciario che riguarda il Certificato emesso nell'ambito del Servizio Fiduciario.

Archivio dei certificati	Un archivio di certificati ne contiene molti. Un'Autorità di Certificazione ha un archivio di Certificati in cui sono conservati i certificati emessi, ma anche il sistema contenente i Certificati disponibili nell'applicazione (sistema di gestione dei certificati) sul computer del Soggetto e della Parte Affidante è chiamato archivio dei Certificati.
Autorità di certificazione	Un Prestatore di Servizi Fiduciari, il quale identifica il richiedente nell'ambito del servizio di certificazione, emette Certificati, tiene un registro, riceve le modifiche ai dati relativi al Certificato e pubblica i regolamenti pertinenti al Certificato, i Dati di Verifica del Certificato e le informazioni sullo stato attuale (specialmente su possibile revoca o sospensione) del Certificato.
Cliente	Il termine collettivo per il Sottoscrittore e ogni relativa denominazione del Soggetto.
Compromissione	Una chiave crittografica è compromessa quando quando persone non autorizzate potrebbero avervi avuto accesso.
Chiave crittografica	Una serie di segnali digitali individuali che controllano la trasformazione crittografica, la cui conoscenza è necessaria per la crittografia, la decrittazione, la creazione e la verifica della firma elettronica.
Data center	Una struttura progettata per l'ubicazione e il funzionamento di sistemi informatici e componenti associati. Questi componenti includono tipicamente sistemi di telecomunicazione e connessioni di comunicazione, alimentazione elettrica ridondante, archiviazione dati, condizionamento dell'aria, protezione antincendio e sistemi di sicurezza.
Documento elettronico	Significa qualsiasi contenuto memorizzato in formato elettronico, in particolare testo o registrazione sonora, visiva o audiovisiva.
Firma elettronica	Dati in forma elettronica acclusi oppure connessi logicamente ad altri dati in forma elettronica e usati dal firmatario per firmare
Dati di creazione della firma elettronica	Significa dati unici utilizzati dal firmatario per creare una firma elettronica. Tipicamente, è la chiave privata crittografica, precedentemente nota come dati per la creazione della firma.
Dispositivo di creazione della firma elettronica	Si riferisce a software o hardware configurato utilizzato per creare una firma elettronica. Precedentemente noto come dispositivo per la creazione di firma.
Marca temporale elettronica	Significa dati in forma elettronica che legano altri dati in forma elettronica a un determinato momento, stabilendo la prova che questi ultimi dati esistevano in quel momento.

Situazione operativa straordinaria	Una situazione straordinaria che causa disturbo nel corso dell'operazione del Prestatore di Servizi Fiduciari, quando la continuazione della normale operatività del Prestatore di Servizi Fiduciari non è possibile temporaneamente o permanentemente.
Hash	Una stringa di bit di lunghezza fissa che dipende dal documento elettronico da cui è derivata, con una probabilità molto piccola che due documenti diversi abbiano lo stesso hash, ed è praticamente impossibile preparare un documento con lo stesso hash.
Hardware Security Module (HSM)	Uno strumento hardware sicuro che genera, memorizza e protegge le chiavi crittografiche e fornisce un ambiente sicuro per l'implementazione delle funzioni crittografiche.
Unità di Certificazione Intermedia	Una Unità di Certificazione il cui Certificato è stato emesso da un'altra Unità di Certificazione.
Gestione delle chiavi	La produzione di chiavi crittografiche, la loro consegna agli utenti o la loro implementazione algoritmica, nonché la registrazione, l'archiviazione, la revoca, la sospensione e la cessazione delle chiavi strettamente legate al metodo di sicurezza utilizzato.
Autorità di registrazione locale	Organizzazione locale formalmente delegata dall'Autorità di Registrazione per l'identificazione del Soggetto Sottoscrittore e la verifica dell'autenticità dei dati inviati.
Amministratore dell'organizzazione	Quella persona fisica che è idonea ad agire durante la richiesta, il ripristino e la revoca o la sospensione dei Certificati rilasciati all'Organizzazione e a concedere il rilascio di Certificati di firma elettronica personali relativi all'organizzazione e la revoca o la sospensione di tale Certificato. L'amministratore dell'Organizzazione può essere nominato da una persona idonea a rappresentare l'organizzazione. La designazione di un Amministratore dell'Organizzazione non è obbligatoria per ogni Organizzazione; se non designato, la persona idonea a rappresentare l'Organizzazione svolge i compiti sopra menzionati
Certificato dell'Organizzazione	Un Certificato il cui Soggetto è l'Organizzazione, o che indica che la il soggetto-persona fisica appartiene a un'Organizzazione. In questo caso il nome dell'Organizzazione è indicato nel campo "O" del Certificato.

Chiave privata	Nell'infrastruttura a chiave pubblica, l'elemento di una coppia di chiavi crittografiche asimmetriche appartenenti ad un attore, che il Soggetto deve mantenere strettamente segreto. Nel caso delle firme elettroniche il Firmatario genera la firma con l'ausilio della chiave privata. Durante l'emissione dei Certificati, l'Autorità di Certificazione utilizza le chiavi private dell'Unità di Certificazione per apporre una firma o un sigillo elettronico sul Certificato per proteggerlo
Chiave pubblica	Nell'infrastruttura a chiave pubblica, l'elemento di una coppia di chiavi crittografiche asimmetriche appartenente a un attore, che dovrebbe essere reso pubblico. La divulgazione avviene tipicamente sotto forma di Certificato, che collega il nome dell'attore alla sua chiave pubblica. Nel caso di una firma elettronica, la chiave pubblica del soggetto creatore della firma è necessaria per verificarne l'autenticità. L'autenticità dei Certificati può essere verificata con la chiave pubblica dell'Unità di Certificazione.
Public Key lnfrastructure, PKI	Un'infrastruttura basata sulla crittografia asimmetrica, che include gli algoritmi crittografici, le chiavi, i certificati, gli standard e la legislazione correlati, il sistema istituzionale sottostante, una varietà di fornitori e dispositivi.
Certiificato qualificato per firma elettronica	Un Certificato per firme elettroniche rilasciato da un Prestatore di Servizi Fiduciari Qualificato e che soddisfa i requisiti stabiliti nell'Allegato I dell'eIDAS.
Firma elettronica qualificata	Una firma elettronica avanzata che è creata da un dispositivo qualificato per la creazione di firme elettroniche e che è basata su un certificato qualificato per le firme elettroniche.
Dispositivo per la creazione di firme elettroniche qualificate	Si intende un dispositivo per la creazione di firma elettronica che soddisfa i requisiti stabiliti nell'Allegato II dell'eIDAS.
Marcatura temporale elettronica qualificata	Una marcatura temporale elettronica che soddisfa i requisiti stabiliti dall'Articolo 42 del regolamento eIDAS
Servizio fiduciario qualificato	Un servizio fiduciario che soddisfa i requisiti applicabili stabiliti nel regolamento eIDAS
Fornitore di servizi fiduciari qualificato	Un Prestatore di Servizi Fiduciari che fornisce uno o più Servizi Fiduciari Qualificati e a cui viene concesso lo status di “qualificato” dall'organismo di vigilanza.
Autorità di registrazione	Organizzazione che verifica l'autenticità dei dati del titolare del Certificato e accerta che la richiesta di Certificato sia autentica e sia stata presentata da una persona autorizzata.

Richiesta di registrazione	I dati e le dichiarazioni forniti in anticipo dal Cliente al Prestatore di Servizi Fiduciari per la preparazione della Richiesta di Certificato e del contratto di fornitura, in cui il Cliente autorizza il Prestatore di Servizi Fiduciari alla gestione dei dati.
Parte affidante	Destinatario del documento informatico, che agisce avvalendosi della firma elettronica basata su un dato certificato.
Organizzazione rappresentata	Sure, here is the translation: Se il Certificato è rilasciato al Soggetto allo scopo di utilizzarlo per le proprie attività o per firmare per conto dell'Organizzazione, allora l'Organizzazione Rappresentata è l'Organizzazione in questione, che è anche specificata nel Certificato.
Revoca	La revoca è la cessazione della validità del Certificato prima della fine del periodo di validità indicato sul Certificato. La revoca del Certificato è permanente, il Certificato revocato non può più essere ripristinato.
Sospensione	La validità del certificato può essere sospesa prima della scadenza della validità del Certificato. La sospensione può essere eliminata, aggirata o revocata.
Registrazioni di stati di revoca dei certificati	Le registrazioni dei Certificati revocati, che includono il fatto della sospensione o revoca e il momento della sospensione o revoca, mantenute dall'Autorità di Certificazione.
Root certificate	Conosciuto anche come certificato di primo livello. Certificato autofirmato, emesso da una specifica Unità di Certificazione per sé stessa, firmato con la propria chiave privata, in modo che possa essere verificato con i Dati di Verifica della Firma indicati sul certificato.
Servizio di firma basato su server	Un servizio in cui la chiave privata del firmatario può essere trovata su un server opportunamente protetto in un modulo crittografico sicuro che può essere utilizzato dal firmatario dopo una fase di autenticazione adeguatamente protetta.
Contratto di servizi	Il contratto tra il Prestatore di Servizi Fiduciari e il cliente del Servizio Fiduciario, che include le condizioni per la fornitura del Servizio Fiduciario e per l'utilizzo dei servizi.
Firmatario	Una persona fisica che crea una firma elettronica. Una persona con un'identità o un attributo verificato dal Prestatore di Servizi Fiduciari con il certificato della firma elettronica.
Soggetto	Una persona fisica la cui identità o attributo è verificato dal Prestatore di Servizi Fiduciari tramite il Certificato, in particolare nel caso di un certificato di firma elettronica, è il firmatario.

Abbonato	Una persona o organizzazione che firma l'accordo di servizio con il Prestatore di Servizi Fiduciari al fine di utilizzare alcuni dei suoi servizi.
Servizio fiduciario	Significa un servizio elettronico fornito normalmente a titolo oneroso che consiste in: la creazione, verifica e convalida di firme elettroniche, sigilli elettronici o marcature temporali elettroniche, servizi di recapito certificato elettronico e certificati relativi a tali servizi; o la creazione, verifica e convalida di certificati di autenticazione di siti web; o la conservazione di firme elettroniche, sigilli o certificati relativi a tali servizi.
Policy del servizio fiduciario	Un insieme di regole in cui un Prestatore di Servizi Fiduciari, una parte contraente o un'altra persona stabilisce le condizioni per l'utilizzo del Servizio Fiduciario per una comunità di parti contraenti e/o una classe di applicazioni con requisiti di sicurezza comuni.
Trust Service Practice Statement	La dichiarazione del Prestatore di Servizi Fiduciari delle procedure dettagliate o altri requisiti operativi utilizzati in relazione alla fornitura di un particolare servizio fiduciario.
Fornitore di servizi fiduciari	Una persona fisica o giuridica che fornisce uno o più Servizi Fiduciari, sia come Servizio Fiduciario qualificato che non qualificato.
Organismo di Supervisione dei Servizi Fiduciari.	L'Autorità Nazionale, l'autorità di vigilanza che monitora i Servizi Fiduciari.
Validazione	È il processo teso a verificare e confermare che una firma o un sigillo elettronico è valido.
Catena di validazione	Il documento elettronico o il suo hash, e la serie di informazioni assegnate l'una all'altra (specialmente quei certificati, informazioni relative ai certificati, dati utilizzati per la creazione della firma o del sigillo, lo stato attuale del certificato, informazioni sul ritiro, così come informazioni sui dati di validità del fornitore dell'emittente del certificato e le sue informazioni di revoca o sospensione), con l'aiuto dei quali si può stabilire che la firma elettronica avanzata o qualificata, il sigillo o la marcatura temporale apposta sul documento elettronico era valida al momento dell'apposizione della firma, del sigillo o della marcatura temporale.
Dati di convalida	I dati utilizzati per convalidare una firma elettronica o un sigillo elettronico.

1.6.2. Acronimi

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
eIDAS	Electronic, identification, Authentication and Signature
HSM	Hardware Security Module
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object lDentifier
PKI	Public Key infrastructure
QCP	Qualified Certificate Policy
RA	Registration Authority
SCD	Secure Creation Device
TSP	Trust Service Provider

2. Responsabilità per la pubblicazione e l'archiviazione

Il Fornitore rende disponibili le condizioni contrattuali e le politiche in formato elettronico sul proprio sito web.
I nuovi documenti da introdurre vengono pubblicati sul sito web 30 giorni prima di entrare in vigore.
Qualsiasi modifica nella fornitura dei servizi fiduciari qualificati descritti in questo documento sarà notificata all'Autorità Nazionale, così come l'intenzione di cessare i servizi forniti.
I documenti in vigore sono disponibili sul sito, oltre a tutte le versioni precedenti di tutti i documenti.
Il Fornitore informa i propri Clienti in merito alla modifica delle Condizioni Generali.
Tutti i documenti pubblicati sono originali e firmati dal Fornitore con Firma Elettronica Qualificata.

2.1. Archivi

Il Fornitore pubblica su questa pagina web il presente documento, altri documenti di policy, termini e condizioni su cui si basa la sua operatività, certificati CA, certificati che i proprietari hanno scelto di pubblicare, e altre informazioni relative al centro fiduciario:

https://docs.trustpro.eu

L'Autorità di Certificazione garantisce che la disponibilità del suo sistema di pubblicazione dei propri Certificati di servizio, dell'archivio dei Certificati e delle informazioni sullo stato di revoca o sospensione, su base annuale, sarà disponibile almeno il 99,953% all'anno, mentre i tempi di inattività del servizio non potranno superare le 3 ore in ogni singolo caso.

2.2. Pubblicazione di informazioni sulla certificazione

Il Fornitore rende disponibili sulla sua pagina web i suoi Certificati CA. I certificati dei soggetti non sono pubblicati.

2.2.1. Certificati del fornitore dei servizi

L'Autorità di Certificazione rende pubblici il certificato radice e le unità di servizio online per lo stato dei certificati che gestisce nella Certification Practice Statement. Le informazioni relative alla modifica del loro stato sono disponibili sul sito web dell'Autorità di Certificazione.

2.2.2. I Certificati degli utenti finali.

L'Autorità di Certificazione divulga le informazioni relative allo stato dei certificati dell'utente finale emessi:

- sugli elenchi di revoca,
- nell'ambito del servizio di risposta online sullo stato dei certificati.

La revoca o la sospensione del certificato dell'utente finale è divulgata dal Fornitore ed il consenso del Soggetto non è richiesto per essa.
L'Autorità di Certificazione divulga, se il Soggetto presta il proprio consenso, i certificati dell'utente finale, conservati nel proprio Archivio dei Certificati, dopo l'emissione senza ritardo.

2.3. Frequenza della Pubblicazione.

2.3.1. Frequenza della Pubblicazione dei Termini e Condizioni

La divulgazione di questo documento e delle relative nuove versioni è conforme ai termini descritti nella Sezione 9.
Il Fornitore divulga altre normative, condizioni contrattuali e le loro nuove versioni, se necessario.
Il Fornitore pubblica informazioni straordinarie senza indugio in conformità con i requisiti legali e,

in assenza di questi, quando necessario.

2.3.2. Frequenza della pubblicazione dei certificati

Il Fornitore, per quanto riguarda la divulgazione di alcuni Certificati, segue le seguenti pratiche:

- i Certificati delle unità di Root certificates da esso operate sono resi noti prima dell'inizio del servizio

2.3.3. Frequenza di pubblicazione delle modifiche dello stato di revoca

Le informazioni sullo stato relative ai Certificati dell'utente finale emessi dal Fornitore ed ai Certificati del fornitore sono disponibili immediatamente nell'ambito del servizio di stato dei certificati online.
Le informazioni relative allo stato dei Certificati sono pubblicate nell'archivio dei Certificati negli elenchi di revoca dei certificati. Le pratiche relative all'emissione degli elenchi di revoca dei certificati sono descritte nella Sezione 4.10.

2.3.4. Controlli di accesso agli archivi.

L'accesso in lettura alle informazioni pubbliche dei Certificati e alle informazioni sullo stato divulgate dall'Autorità di Certificazione è fornito a chiunque, secondo le specificità della pubblicazione. Le informazioni divulgate dall'Autorità di Certificazione potranno essere modificate o eliminate solo dall'Autorità di Certificazione stessa. L'Autorità di Certificazione dovrà impedire modifiche non autorizzate alle informazioni.

3. Identificazione e Autenticazione

Questa sezione descrive le pratiche di identificazione e autenticazione del soggetto e del sottoscrittore utilizzate dal Fornitore.
Le attività di identificazione vengono eseguite in stretta conformità con le procedure qui definite - dall'Autorità di Registrazione del Fornitore o dalle Autorità di Registrazione Locali in rapporto contrattuale con il Fornitore.

3.1. Assegnazione del nome

Il soggetto è identificato nel certificate mediante il nome distintivo (DN), nel campo “Soggetto”, in conformità con lo standard X.500 (ISO/IEC 9594).

L’attributo DN è conforme con lo standard ETSI EN standards and RFC 5280 di seguito indicato.

- ETSI EN 319 411-1 [2]: Firme elettroniche e Infrastrutture (ESI); Policy e requisiti di sicurezza per i Fornitori di Servizi Fiduciari che emettono certificati; Parte 1 : Requisiti generali
- ETSI EN 319 411-2 [3]: Firme elettroniche e Infrastrutture (ESI); Policy e requisiti di sicurezza per i Fornitori di Servizi Fiduciari che emettono certificati.; Parte 2: Requisiti per i fornitori di servizi fiduciari che emettono certificati qualificati nell'UE.
- ETSI EN 319 412-1 [4]: Firme elettroniche e Infrastrutture (ESI); Profili dei certificati; Parte 1: Panoramica e strutture dati comuni.
- ETSI EN 319 412-2 [5]: Firme elettroniche e Infrastrutture (ESI); Profili dei certificati; Parte 2: Profilo dei certificati rilasciati a persone fisiche.
- ETSI EN 319 412-3 [6]: Firme elettroniche e Infrastrutture (ESI); Profili dei certificati; Parte 2: Profilo dei certificati rilasciati a persone fisiche..
- ETSI EN 319 412-5 [7]: Firme elettroniche e Infrastrutture (ESI); Profili dei certificati; Parte 5: Dichiarazioni di controllo qualità.

3.1.1. Necessità che i nomi abbiano un significato

Gli attributi del certificato che assegna un nome distintivo (DN) identificano in modo univoco il soggetto a cui viene rilasciato il certificato.
Se il soggetto del certificato è una persona fisica, il campo Soggetto contiene almeno:

- Nome del paese (OID: 2.5.4.6)
- Nome di battesimo (OID: 2.5.4.42)
- Cognome (OID: 2.5.4.4)
- Nome comune (OID: 2.5.4.3)
- Numero di serie (OID: 2.5.4.5)
- Qualificatore DN (OID 2.5.4.46)

  Se il soggetto del certificato è una persona giuridica, il campo “Soggetto” deve contenere almeno:
- Nome del paese (OID: 2.5.4.6)
- Nome dell’ente (OID: 2.5.4.10)
- Identificativo dell’ente (OID: 2.5.4.97)
- Nome comune (OID: 2.5.4
- Qualificatore DN (OID 2.5.4.46)

  Il valore del campo Qualificatore DN è un unico code di identificazione generato da TrustPro QTSP CA e conservato nel database CA

3.1.2. Anonimato o pseudonimato dei soggetti

Il Fornitore valuterà caso per caso la richiesta di utilizzo di uno Pseudonimo in sostituzione dei dati reali. Se la richiesta verrà accettata verrà utilizzato il campo Pseudonimo (OID 2.5.4.65) mentre saranno omessi i dati Nome, Cognome e Seria/Number

3.1.3. Regole per l'Interpretazione delle Varie Forme di Nome

Il Fornitore adotta lo standard X500.

3.1.4. Unicità del nome

Il Soggetto ha un nome univoco nell'Archivio dei Certificati del Fornitore. Per garantirne l'unicità, viene utilizzata una combinazione di codice paese del Soggetto, tipo di documento di identità e numero di documento di identità.
Questa combinazione è conforme all'identificatore semantico di persona fisica e persona giuridica come previsto nello standard ETSI EN 319 412-1 [4].

3.1.5. Procedure dirette a risolvere controversie relative ai nomi

Il Fornitore garantisce il diritto del cliente ad usare il nome indicato. Il Fornitore ha il diritto di revocare il Certificato in questione per l'uso illegale del nome o dei dati.

3.1.6. Riconoscimento, autenticazione e ruolo dei marchi

Nei campi del Certificato dell'utente finale richiesti dal Sottoscrittore possono comparire marchi commerciali. Il Fornitore si assicura del loro uso legittimo e, in caso di reclamo, ha il diritto di revocare il Certificato.
Se il Cliente richiede un Certificato e chiede l'indicazione di un brand o di un marchio registrato, il Cliente deve fornire prova della legittimità del suo uso, che il Fornitore verifica prima dell'emissione del Certificato.
Il Fornitore utilizza il marchio TrustPro QTSP Ltd durante la prestazione del servizio. Il marchio è di proprietà di TrustPro QTSP Ltd LP; per l'uso del marchio, il consenso è dato dal titolare.

3.2. Convalida iniziale dell’identità

L'Autorità di Registrazione può utilizzare qualsiasi canale di comunicazione, nei limiti previsti dalla legge, per la verifica dell'identità del Soggetto che richiede il Certificato e per il controllo dell'autenticità dei dati forniti.
L'Autorità di Registrazione o il Fornitore possono rifiutare il rilascio del Certificato richiesto a loro esclusiva discrezione, senza alcuna giustificazione.

3.2.1. Metodo per dimostrare il possesso della chiave privata

Il Fornitore stabilisce che il richiedente possieda o controlli la chiave privata corrispondente alla chiave pubblica da certificare, verificando che la richiesta di certificato contenga una richiesta firmata con la chiave privata corrispondente alla chiave pubblica da certificare. La richiesta firmata sarà in formato PKCS# 10 (RFC 2314).

3.2.2. Convalida dell’identità di un’organizzazione

L‘identità di una persona giuridica è convalidata usando i registri locali appositamente creati e I documenti emessi dalle organizzazioni o gli enti che tengono tali registri.

3.2.3. Convalida dell'identità personale

L'identità della persona fisica sarà verificata:

- Se il soggetto del certificato emesso è una persona fisica,
- Se la persona fisica agisce per conto di un'organizzazione.

Quando si emette un Certificato qualificato, l'identità della persona fisica deve essere verificata secondo il paragrafo 1 dell'Articolo 24 del regolamento eIDAS mediante presenza fisica o con un metodo che offra una sicurezza equivalente. Vale a dire:

- Identificazione in presenza: la persona fisica deve presentarsi di persona al rappresentante dell'Autorità di Registrazione o al delegato dell'Autorità di Registrazione Locale;
- Identificazione a distanza utilizzando un sistema con garanzia equivalente alla presenza fisica;
- Identificazione tramite certificato elettronico qualificato: l'identità della persona fisica è attestata da una firma elettronica qualificata con un certificato qualificato appartenente alla persona fisica;

Ogni metodo è eseguito da un'Autorità di Registrazione ed è dettagliato nei paragrafi seguenti.
L'Autorità di Registrazione può delegare formalmente l'identificazione a un'Autorità di Registrazione Locale. In questo caso, nel Modulo di Richiesta del Certificato deve essere presente un riferimento all'identità del funzionario dell'Autorità di Registrazione Locale.

3.2.4. Identificazione in presenza

L'identità della persona fisica è accertata in presenza.

- La persona fisica dovrà presentarsi di persona al rappresentante dell'Autorità di Registrazione, al delegato o al Sottoscrittore per eseguire l'identificazione personale;
- L'identità della persona fisica viene verificata durante l'identificazione personale sulla base di un'idonea prova d'identità ufficiale;
- I documenti d'identità accettati sono definiti in ogni paese dalle normative locali;
- La persona fisica dovrà verificare l'accuratezza dei dati per la registrazione e la verifica dell'identità;
- Il rappresentante o il delegato dell'Autorità di Registrazione verifica se sono avvenute alterazioni o contraffazioni ai documenti d'identità presentati.

L'Autorità di Registrazione verifica l'identità dei cittadini stranieri con l'ausilio del loro passaporto o di altri documenti di identificazione personale; in tal caso può effettuare la riconciliazione dei dati con gli appositi registri del paese, se tali registri sono disponibili.
Il Fornitore può accettare anche altri documenti e prove, se si assicura che il livello di sicurezza sia lo stesso di quello sopra indicato. L'ottenimento di tali prove e la loro presentazione al Fornitore sono responsabilità del Cliente.
Il Fornitore accetta solo documenti e prove validi non più vecchi di 3 mesi.
Il Fornitore non emette il Certificato se ritiene che – in base alle proprie regole interne – non possa verificare con la corrispondente fiducia il certificato, il documento o i dati dell'organizzazione straniera.

3.2.5. Identificazione remota

L'Autorità di Registrazione è autorizzata a utilizzare il sistema di identificazione remota fornito dal Fornitore e confermato da un organismo di Valutazione della Conformità.
L'identificazione remota può essere eseguita con uno dei seguenti metodi:

a) Un sistema di identificazione video a distanza come da art. 24.1.d eIDAS. L'identificazione video a distanza di TrustPro è un'applicazione (https://remoteid.trustpro.eu) che raccoglie una serie di prove di identità del soggetto – inclusa una registrazione video –, convalida tali prove e sottopone all'Autorità di Registrazione o al funzionario dell'Autorità di Registrazione Locale solo le identità convalidate con successo. Tutte le identità sono verificate dall'Autorità di Registrazione o dal funzionario dell'Autorità di Registrazione Locale. Se l'identità non è correttamente verificata dal funzionario, il certificato viene revocato.
b) Un sistema di identificazione elettronica notificato ai sensi dell'art. 8 eIDAS [1] utilizzando un livello di garanzia sostanziale e/o elevato per i mezzi di identificazione.

3.2.6. Identificazione del certificato elettronico.

L'identità della persona fisica è attestata da una firma elettronica qualificata con un certificato qualificato appartenente alla persona fisica.

- Il Soggetto presenta la Richiesta di Certificato in formato elettronico con una firma elettronica qualificata basata su un certificato qualificato non pseudonimo.
- La Richiesta di Certificato firmata elettronicamente deve contenere i dati necessari per l'identificazione della persona fisica.
- L'autenticità e la riservatezza della Richiesta di Certificato devono essere verificate sull'intera catena di certificazione.
- Il Fornitore può accettare solo le firme elettroniche basate su un certificato qualificato rilasciato da un Prestatore di Servizi Fiduciari che sia elencato nella Trusted List di uno degli stati membri dell'UE ed era valido al momento della creazione della firma.

Il Fornitore può utilizzare i dati riconciliati durante una precedente procedura di identificazione, se il Soggetto richiede un nuovo Certificato al posto di uno scaduto o revocato, o se richiede un nuovo Certificato oltre a quello esistente durante il periodo di validità dell'accordo di servizio. L'autenticità della Richiesta di Certificato, l'accuratezza dei dati da inserire nel Certificato e l'identità della persona che presenta la richiesta devono essere anch'esse verificate.

3.2.7. Informazioni non verificate

Alcune informazioni relative al Soggetto o al Sottoscrittore, come l'indirizzo o il numero di telefono, potrebbero non essere verificate dal Fornitore. Il Fornitore non è responsabile dell'accuratezza di tali informazioni.

3.2.8. Validazione dell'Autorità

L'identità della persona fisica che rappresenta la persona giuridica viene verificata secondo i requisiti della Sezione 3.2.3 prima di rilasciare un Certificato per la persona giuridica.
Il potere di rappresentanza della persona fisica deve essere verificato. Le persone autorizzate ad agire per conto di un'Organizzazione sono:

- una persona autorizzata a rappresentare l'Organizzazione in questione,
- una persona che è stata incaricata a tale scopo da una persona autorizzata a rappresentare l'Organizzazione,
- un amministratore dell'Organizzazione nominato da una persona autorizzata a rappresentare l'Organizzazione.

L'amministratore dell'organizzazione può essere nominato durante la richiesta del Certificato, o in qualsiasi momento successivo con l'ausilio del modulo corrispondente. Le informazioni identificative della/e persona/e designata/e devono essere fornite sul modulo, tramite le quali

egli/ella potrà essere identificato/a in successive controversie. Il modulo deve essere firmato elettronicamente dal rappresentante dell'Organizzazione, il che viene verificato dall'addetto alla registrazione del Fornitore al momento della ricezione. La nomina di un amministratore dell'organizzazione non è obbligatoria, e possono essere nominati anche più amministratori dell'organizzazione. Se non c'è un amministratore dell'organizzazione nominato, allora la persona autorizzata a rappresentare l'Organizzazione può svolgere questo compito.

3.3. Convalida dell'identificazione nel caso di rinnovo della richiesta di certificato

Il rinnovo del Certificato è il processo in cui il Fornitore rilascia, ad un soggetto, un certificato con informazioni di identificazione del Soggetto invariate, ma per un nuovo periodo di validità. Il rinnovo del Certificato può essere richiesto solo durante il periodo di validità dell'accordo di servizio.

3.3.1. Identificazione con Certificato Valido

Per il rinnovo di un Certificato basato su un certificato valido, il Provider offre le seguenti opzioni

- Richiesta inviata elettronicamente con una firma elettronica basata sul Certificato da rinnovare;
- Modulo elettronico con una firma elettronica del Soggetto basata sul Certificato non pseudonimo con un livello di sicurezza non inferiore a quello del Certificato da rinnovare (vedere sezione 1.2.3.).

Non è necessaria alcuna ulteriore verifica dell'identità del richiedente o dell'autenticità della domanda.

Il certificato deve essere valido. I certificati non validi non possono essere rinnovati.

3.4. Convalida dell'identificazione per le richieste di modifica del Certificato

Non applicabile, in quanto la modifica del certificato non è consentita.

3.5. Identificazione e Autenticazione per le richieste di Revoca e Sospensione

Il Provider riceve ed elabora le richieste relative alla revoca o sospensione dei Certificati, e gli avvisi (ad esempio relativi al compromesso della chiave privata o all'uso improprio del Certificato) riguardanti la revoca dei Certificati.

Il Provider accetta le richieste solo da parti autorizzate prima di elaborare le richieste di revoca o sospensione.

L'identità delle persone che presentano la richiesta e l'autenticità delle domande vengono verificate. Gli aspetti di identificazione e autenticazione di tali richieste sono descritti nella sezione 4.8.3.

4. Requisiti Operativi del Ciclo di Vita del Certificato

Tutte le operazioni del ciclo di vita del certificato sono gestite tramite un'Autorità di Registrazione fidata e sono vincolate a un Accordo di Servizio valido con il Sottoscrittore.
L'accordo di servizio è in formato elettronico e può essere parte di – o essere referenziato da – l'Applicazione e Accettazione del Certificato. L'Applicazione del Certificato è firmata dal Sottoscrittore con firma elettronica avanzata.
L'Applicazione del Certificato viene consegnata al Sottoscrittore insieme al Certificato nel processo di iscrizione.
L'accordo di servizio deve contenere i tipi di Certificato disponibili per Soggetti specifici all'interno dei confini dell'Accordo.
Le operazioni del ciclo di vita del Certificato gestite dal Provider sono:

- Nuovo certificato
- Rinnovo del certificato
- Revoca del certificato

Lo stato di un Certificato può essere valido o revocato.
Il Provider fornisce la manutenzione del Certificato solo durante la validità del relativo accordo di servizio.

4.1. Richiesta di un Certificato

Per ogni nuovo Certificato, è richiesta la presentazione di un'Applicazione del Certificato. Il Soggetto deve specificare i dati da indicare nel Certificato e specificare il tipo di Certificato richiesto, e deve autorizzare il Provider alla gestione dei propri dati personali.
Il Provider informa il Sottoscrittore sui termini e le condizioni d'uso del Certificato prima della conclusione del contratto.
Se il Soggetto non è lo stesso del Sottoscrittore, le suddette informazioni vengono fornite anche al Soggetto via email.
Il Provider pubblica i documenti contenenti queste informazioni in modo comprensibile, resi disponibili in un formato scaricabile elettronicamente.
Nell'Applicazione del Certificato, il Soggetto deve includere almeno i seguenti dati:

- Dati del Soggetto da indicare nel Certificato (vedi sezione 3.1 per i dettagli);Informazioni di identificazione personale del Soggetto - in caso di un'Organizzazione, del rappresentante dell'Organizzazione (almeno data e luogo di nascita per la persona fisica, nome completo per la persona giuridica);
- Il contatto del Soggetto - in caso di un'Organizzazione, del rappresentante dell'Organizzazione - (indirizzo, numero di telefono, indirizzo e-mail);
- In caso di richiesta di Certificato dell'Organizzazione, i dati ufficiali dell'Organizzazione;
- Dati del Sottoscrittore se Soggetto e Sottoscrittore non sono la stessa persona;

Insieme all'Applicazione del Certificato, il rappresentante o delegato dell'Autorità di Registrazione richiede e verifica almeno i seguenti documenti, certificazioni, procure e dichiarazioni:

- Documenti necessari per identificare il Soggetto - in caso di un'Organizzazione, il rappresentante dell'Organizzazione, in conformità alla Sezione 3.2.3;
- In caso di richiesta di Certificato Organizzativo, i documenti per l'identificazione dell'Organizzazione, in conformità alla Sezione 3.2.2;
- Se il Soggetto rappresenta un'Organizzazione, la certificazione o procura rilasciata dall'Organizzazione che il Soggetto è autorizzato a rappresentare l'Organizzazione, in conformità alla sezione 3.2.5;
- Se il Soggetto è una persona fisica che richiede l'indicazione di appartenenza a

un'Organizzazione, la prova del consenso dell'Organizzazione, identificata in conformità alla sezione 3.2.2;

- Se il Certificato richiesto contiene un marchio o un nome di marca, una certificazione sui diritti di utilizzo del Soggetto, in conformità alla sezione 3.1.6.

L'Applicazione del Certificato e l'Accordo di Servizio (o un riferimento a un Accordo di Servizio standard) sono documenti elettronici firmati dal Soggetto e dal Sottoscrittore (se il sottoscrittore e il soggetto sono persone diverse). La firma è:

- Una firma elettronica avanzata autenticata da un fattore di autenticazione dinamico o
- Una firma elettronica avanzata contenente informazioni biometriche della firma del soggetto come velocità, pressione e inclinazione della penna, raccolte da un'applicazione autorizzata dal Provider.
- Una firma qualificata del Sottoscrittore se il sottoscrittore esegue l'identificazione in presenza del Soggetto.

4.1.1. Chi può presentare una domanda di Certificato

La domanda di Certificato può essere presentata solo da persone fisiche, che richiedono un Certificato per sé stesse o per l'organizzazione che rappresentano.
Il Sottoscrittore e il Soggetto, in caso di Organizzazione, il rappresentante dell'Organizzazione, devono fornire le loro informazioni di contatto durante la domanda di Registrazione.

4.1.2. Processo e responsabilità di Iscrizione.

Durante il processo di domanda, il rappresentante o delegato dell'Autorità di Registrazione verifica l'identità della persona che presenta la Domanda di Certificato (vedere sezione 3.2.3).
Se il Soggetto è un'Organizzazione e il nome di un'Organizzazione è indicato nel Certificato, l'Autorità di Registrazione identifica l'Organizzazione (vedere sezione: 3.2.2) e si assicura che il Soggetto sia autorizzato a rappresentare l'Organizzazione (vedere sezione: 3.2.5) e a richiedere un Certificato relativo all'Organizzazione (vedere sezione: 3.2.2).
Il Sottoscrittore determina quale Soggetto è autorizzato a richiedere un Certificato in base alla Politica del Certificato.
Il Soggetto - in caso di Organizzazione, il suo rappresentante - deve fornire tutte le informazioni necessarie per lo svolgimento dei processi di identificazione.
Se il certificato è richiesto con la politica QCP-n-qscd, l'Autorità di Registrazione si assicura che la chiave privata sia generata all'interno di un QSCD sotto il solo controllo del Soggetto.
Se il certificato è richiesto con la politica QCP-l-qscd, l'Autorità di Registrazione si assicura che la chiave privata sia generata all'interno di un QSCD sotto il solo controllo del Soggetto.
Se il certificato è richiesto con la politica QCP-n, l'Autorità di Registrazione si assicura che la chiave privata sia generata sotto il controllo del Soggetto.
Se il certificato è richiesto con la politica QCP-l, l'Autorità di Registrazione si assicura che la chiave privata sia generata sotto il controllo del Soggetto.
Il Provider può effettuare la conciliazione dei dati con registri pubblici (come il registro dei dati personali e degli indirizzi o il registro delle imprese). In caso di disponibilità di un database, il Provider esegue la conciliazione dei dati elettronicamente.
Il Provider registra tutte le informazioni necessarie sull'identità del Soggetto e dell'Organizzazione per la fornitura del servizio e per mantenere il contatto.
Il Provider registra l'accordo di servizio firmato dal Sottoscrittore, che deve contenere la dichiarazione del Sottoscrittore di essere a conoscenza dei propri obblighi e di impegnarsi a rispettarli.

Il Provider registra la Domanda di Certificato che deve contenere quanto segue:

- Una conferma che i dati forniti nella Domanda di Certificato sono accurati;
- Un consenso al fatto che il Provider registri ed elabori i dati forniti nella domanda;
- Una dichiarazione che nel Certificato richiesto non è indicato alcun nome di marca o marchio, oppure, se è indicato, che il richiedente è autorizzato a utilizzarlo.
- Un riferimento all'accordo di servizio utilizzato (o all'accordo di servizio firmato).

Il Provider conserva i suddetti documenti per il periodo di tempo richiesto dalla legge.

Il Provider archivia il documento di Domanda di Certificato e ogni attestazione che l'Organizzazione Rappresentata, il Soggetto o il Sottoscrittore hanno consegnato.

Se l'identità del Soggetto - in caso di Organizzazione, del suo rappresentante - o, in caso di Certificato Organizzativo, l'identità dell'Organizzazione o, in caso di Certificato Organizzativo emesso a una persona fisica, l'appartenenza del Soggetto all'Organizzazione Rappresentata non può essere verificata senza dubbio o se uno qualsiasi dei dati indicati nel modulo di domanda di Certificato è errato, il Provider può, in base ai suoi regolamenti interni, dare al Cliente l'opportunità di correggere i dati mancanti o errati e di consegnare le attestazioni mancanti entro 3 mesi dalla presentazione della Domanda di Certificato.

4.2. Elaborazione della Domanda di Certificato

4.2.1. Esecuzione delle Funzioni di Identificazione e Autenticazione

L'Autorità di Registrazione identifica il Soggetto in conformità alla Sezione 3.2 e verifica l'autenticità della richiesta.

L'Autorità di Registrazione invia al provider l'Applicazione del Certificato e le prove di identificazione.

In caso di richiesta di Certificato organizzativo, anche l'Organizzazione verrà identificata e la verifica dei privilegi avverrà in conformità alla sezione 3.2. Il Provider registra tutte le informazioni utilizzate dal Soggetto o, in caso di Certificato Organizzativo, dall'Organizzazione per certificare la propria identità, inclusi il numero di registrazione della documentazione utilizzata per la certificazione e le eventuali limitazioni relative alla sua validità.

4.2.2. Autenticazione dell'identità con due fattori di autenticazione

Il Provider genera e associa a ciascun dato del Soggetto convalidato due fattori di autenticazione (uno dinamico). Una nuova richiesta di certificato può essere presentata insieme ai due fattori di autenticazione. Un nuovo certificato viene emesso se:

- La verifica di entrambi i fattori di autenticazione ha successo;
- Le prove di identità non sono scadute;
- La richiesta rientra nei limiti dell'accordo di servizio.

4.2.3. Approvazione o Rifiuto delle Domande di Certificato

Per evitare conflitti di interesse, il Provider garantisce la propria indipendenza personale e operativa dal Sottoscrittore. Non costituisce una violazione dei conflitti di interesse se il Provider emette Certificati per i suoi associati.

L'Autorità di Registrazione verifica l'autenticità di tutte le informazioni fornite nell'Applicazione del Certificato da indicare sul Certificato prima di emettere il Certificato.

Se il Soggetto richiede un Certificato contenente un indirizzo e-mail, l'Autorità di Registrazione

verifica l'indirizzo e-mail da indicare nel Certificato.
Il Provider accetta o rifiuta di evadere l'Applicazione del Certificato dopo averla elaborata.
Se l'identità della persona fisica o dell'organizzazione da identificare, o, in caso di Certificato personale, l'appartenenza del Soggetto all'Organizzazione Rappresentata non può essere verificata senza dubbio o se uno qualsiasi dei dati indicati nel modulo di Domanda di Certificato non è corretto, e il Cliente non l'ha corretto su richiesta del Provider, allora il Provider rifiuta la domanda.
In caso di rifiuto dell'Applicazione del Certificato, il Provider informa il Soggetto e il Sottoscrittore, ma il Provider non è tenuto a giustificare la sua decisione.

4.2.4. Tempo di Elaborazione delle Domande di Certificato

Il Provider si impegna a elaborare la Domanda di Certificato entro 5 giorni lavorativi se tutti i dati e i documenti necessari sono disponibili.

4.3. Emissione del Certificato

L'Autorità di Certificazione utilizza HSM ad alta sicurezza per la firma dei certificati utilizzando una chiave RSA a 4096 bit. Ciò garantisce una protezione sostanziale contro la falsificazione.
Il Certificato emesso contiene solo i dati che sono stati indicati nell'Applicazione del Certificato e che sono stati verificati dal Provider (o dall'Autorità di Registrazione) durante il processo di valutazione.
Se l'Autorità di Certificazione fornisce al Soggetto il Dispositivo di Creazione della Firma Elettronica (nell'ambito del servizio di fornitura del dispositivo), come parte del processo, il Certificato emesso viene installato sul Dispositivo di Creazione della Firma Elettronica. La consegna del Dispositivo di Creazione della Firma Elettronica contenente la chiave privata avviene in un ambiente controllato in conformità con le norme di sicurezza definite nella sezione 6.1.2.Se la consegna del Dispositivo di Creazione della Firma Elettronica contenente il Certificato e la chiave privata del Soggetto al Soggetto non avviene subito dopo l'identificazione personale relativa alla domanda di Certificato, allora il Soggetto (in caso di persona non fisica, il suo rappresentante) può ritirare il proprio dispositivo dopo l'identificazione personale, durante la quale deve identificarsi con un documento di identità. La parte che trasferisce verifica che il ritratto del Soggetto corrisponda a quello sulla sua carta d'identità e che la firma del Soggetto corrisponda a quella che appare sulla carta d'identità.
Insieme alla consegna del Dispositivo di Creazione della Firma Elettronica, il Soggetto riceve i codici di attivazione necessari per l'attivazione, generati in conformità alla sezione 6.4. Questi codici vengono consegnati in una busta chiusa ed è obbligatorio per il Soggetto aprirla e verificare se i codici sono leggibili.

4.3.1. Azioni della CA durante l'emissione del Certificato

L'emissione del Certificato avviene secondo processi strettamente regolamentati e controllati, i cui dettagli sono definiti dai regolamenti e requisiti interni del Provider.

4.3.2. Notifica al Sottoscrittore dell'emissione del Certificato

L'Autorità di Certificazione informa il Soggetto e il Sottoscrittore dell'emissione del Certificato e abilita il Soggetto a ricevere il Certificato.
Un codice di revoca univoco è associato al certificato e trasmesso al Soggetto e al Sottoscrittore.

4.4. Accettazione del Certificato

4.4.1. Condotta che costituisce Accettazione del Certificato

Il Soggetto - in caso di un certificato emesso a un'Organizzazione, il rappresentante del Soggetto - deve verificare l'accuratezza dei dati indicati nel Certificato durante il ritiro del Certificato.
Se l'Autorità di Certificazione fornisce al Soggetto un Dispositivo di Creazione di Firma Elettronica Qualificata locale, dopo la ricezione del Dispositivo di Creazione di Firma Elettronica Qualificata contenente la chiave privata, il Certificato del Soggetto e il codice necessario per l'attivazione, il Soggetto può testare il proprio dispositivo. L'uso del dispositivo implica l'accettazione del certificato.
Se l'Autorità di Certificazione o un'Autorità di Registrazione fornisce al Soggetto un Dispositivo di Creazione di Firma Elettronica Qualificata remoto, l'attivazione del dispositivo remoto da parte del soggetto implica l'accettazione del certificato.

4.4.2. Pubblicazione del Certificato da parte della CA

Se l'accordo di servizio consente la divulgazione del certificato e il soggetto lo richiede, dopo la ricezione del Certificato il Provider divulga il Certificato nel suo archivio di Certificati.

4.4.3. Notifica dell'Emissione del Certificato da parte della CA ad altre Entità

Se il Certificato è stato emesso affinché il Soggetto possa creare una firma elettronica per conto di un'Organizzazione, il contatto dell'Organizzazione Rappresentata viene notificato dal Provider dell'emissione del Certificato senza indugio.

4.5. Utilizzo della Coppia di Chiavi e del Certificato

4.5.1. Utilizzo della Chiave Privata e del Certificato del Sottoscrittore

Il Soggetto deve utilizzare la sua chiave privata corrispondente al Certificato solo per la creazione di firme elettroniche, e qualsiasi altro utilizzo (ad esempio, autorizzazione e crittografia) è proibito.
Una chiave privata corrispondente a un Certificato scaduto o revocato non deve essere utilizzata per la creazione di firme elettroniche.
Il Soggetto è tenuto a garantire una protezione adeguata della chiave privata e dei dati di attivazione (password e altri fattori di autenticazione statici o dinamici).
Durante l'utilizzo, devono essere seguite le limitazioni stabilite nella Sezione 1.4.

4.5.2. Utilizzo della Chiave Pubblica e del Certificato della Parte Affidante

Per mantenere il livello di sicurezza garantito dal Provider, nel corso dell'accettazione della firma elttronica verificata, si raccomanda alla Parte Affidante di procedere con prudenza, in particolare per quanto riguarda i seguenti aspetti:

- La Parte Affidante deve verificare la validità e lo stato di revoca del Certificato;
- I Certificati per le firme elettroniche e le relative chiavi pubbliche devono essere utilizzati solo per la convalida delle firme elettroniche;
- Le verifiche relative al Certificato devono essere effettuate per l'intera catena di

certificati;

- La verifica della firma elettronica deve essere eseguita con un'applicazione affidabile, che sia conforme alle specifiche tecniche pertinenti, possa essere configurata in modo resiliente, sia stata impostata correttamente e funzioni in un ambiente privo di virus;In caso di Certificati personali relativi a un'organizzazione, si raccomanda di verificare che il titolo del Firmatario, in base al quale è autorizzato a firmare il documento, possa essere identificato dal certificato (ad esempio, indicato nel campo "Titolo");Si raccomanda di verificare che il Certificato sia stato emesso in conformità alla Politica del Certificato appropriata;
- Quando si accetta una firma elettronica qualificata, si raccomanda di verificare che il Certificato sia stato emesso sulla base di una Politica del Certificato che richiede un Dispositivo di Creazione di Firma Elettronica Qualificata;
- Si raccomanda di verificare il valore massimo dell'obbligazione assunta in un'unica volta indicato nel Certificato (l'Autorità di Certificazione non è responsabile per i reclami derivanti da documenti elettronici emessi e firmati relativi a transazioni che superano tali limiti e per i danni causati in questo modo);
- La Parte Affidante deve considerare eventuali restrizioni indicate nel Certificato o nei regolamenti a cui il Certificato fa riferimento.

Il Provider mette a disposizione un servizio per i suoi Clienti e Parti Affidanti che possono utilizzare per verificare i Certificati emessi.

4.6. Rinnovo del Certificato

Il rinnovo del Certificato è il processo in cui il Provider emette un nuovo Certificato per un nuovo periodo di validità per la stessa chiave pubblica con informazioni di identità del Soggetto invariate. Il Soggetto deve avviare il rinnovo del Certificato prima della data di scadenza del Certificato. Il rinnovo del Certificato significa tecnicamente l'emissione di un nuovo Certificato, con gli stessi dati di identificazione del Soggetto, ma con un nuovo periodo di validità. Altri dati possono cambiare nel Certificato, come i riferimenti a CRL, OCSP o la chiave del provider utilizzata per la firma del Certificato.

4.6.1. Circostanze per il Rinnovo del Certificato

Il rinnovo del Certificato è consentito solo quando tutte le seguenti condizioni sono soddisfatte:

- La richiesta di rinnovo del Certificato è stata presentata entro il periodo di validità del Certificato
- Il Certificato da rinnovare non è revocato;
- La chiave privata corrispondente al Certificato non è compromessa;
- Le informazioni di identità del Soggetto sono ancora valide.

Il Provider accetterà una domanda di rinnovo del Certificato solo all'interno dell'accordo di servizio.

Se uno qualsiasi dei dati del Soggetto indicati nel Certificato è cambiato, allora un Certificato deve essere richiesto nell'ambito della modifica del Certificato (vedere sezione 4.8.).Durante il rinnovo del Certificato, il Soggetto viene informato se i termini e le condizioni sono cambiati dall'ultima emissione del Certificato.

Se il Soggetto non è lo stesso del Sottoscrittore, le informazioni suddette vengono fornite anche al Sottoscrittore.

4.6.2. Chi può richiedere il Rinnovo

Il rinnovo del Certificato deve essere avviato da una persona che è autorizzata a presentare una domanda per un nuovo Certificato dello stesso tipo per conto del Soggetto al momento della presentazione della domanda di rinnovo.
Il richiedente deve dichiarare nella domanda di rinnovo del Certificato che i dati di identificazione del Soggetto indicati nel Certificato sono ancora validi.
Il Provider ha il diritto di avviare il rinnovo del Certificato se la chiave di firma del servizio utilizzata per l'emissione del Certificato deve essere sostituita.La richiesta di rinnovo del certificato viene firmata con il certificato valido da rinnovare.

4.6.3. Elaborazione delle Richieste di Rinnovo del Certificato

Durante la valutazione della domanda di rinnovo del Certificato, il Provider verifica che:

- L'Applicazione di rinnovo del Certificato presentata sia autentica;
- Il presentatore dell'Applicazione di rinnovo del Certificato abbia l'autorizzazione e il diritto appropriati;
- Il presentatore dell'Applicazione di rinnovo del Certificato abbia dichiarato che i dati del Soggetto da indicare nel Certificato sono invariati e accurati;
- Le prove di identificazione del certificato precedente siano ancora valide;
- L'Applicazione di rinnovo del Certificato sia stata presentata durante il periodo di validità del Certificato;
- Il Certificato da rinnovare esista e non sia revocato;
- Sulla base delle informazioni attualmente disponibili sugli algoritmi crittografici utilizzati, essi saranno ancora applicabili anche durante il periodo di validità previsto del Certificato da emettere.

4.6.4. Notifica della Nuova Emissione del Certificato

Il Provider informa con un'e-mail il Soggetto e il Sottoscrittore dell'emissione del Certificato. Un codice di revoca univoco è associato al certificato e comunicato al Soggetto e al Sottoscrittore.
I termini e le condizioni attuali vengono comunicati al Soggetto e al Sottoscrittore.

4.6.5. Condotta che Costituisce l'Accettazione di un Certificato Rinnovato

Durante il processo di rinnovo del Certificato, non c'è generazione di chiavi, quindi non è necessario consegnare la chiave al Soggetto. Il Certificato rinnovato può essere ricevuto (scaricato) senza incontro personale.
Se la chiave privata del Soggetto si trova su un Dispositivo di Creazione di Firma Elettronica, allora il Soggetto installa il Certificato nel dispositivo.
Il soggetto accetta il Certificato con il suo utilizzo senza ulteriore dichiarazione.

4.6.6. Pubblicazione del Certificato Rinnovato da parte della CA

Il Provider divulga il Certificato rinnovato con lo stesso metodo del Certificato originale.

4.6.7. Notifica ad Altre Entità dell'Emissione del Certificato

Se il Certificato è stato emesso affinché il Soggetto possa creare una firma elettronica per conto di un'Organizzazione, il contatto dell'Organizzazione Rappresentata viene notificato dal Provider

dell'emissione del Certificato senza indugio.

4.7. Modifica del Certificato

La modifica del Certificato non è consentita. Un certificato con dati errati deve essere revocato.
Se l'errore è stato causato dal Provider o dall'Autorità di Registrazione, il certificato errato verrà revocato e il nuovo verrà emesso senza alcun costo aggiuntivo per il cliente.
Se l'errore è stato causato dal Soggetto e/o dal Sottoscrittore, il certificato verrà revocato e il nuovo verrà emesso con la procedura ordinaria.

4.8. Revoca o Sospensione del Certificato

La revoca del Certificato termina la validità del Certificato prima della scadenza. La revoca del Certificato è un cambiamento di stato permanente e irreversibile; il certificato revocato non sarà mai più valido.
L'utilizzo della chiave privata appartenente al Certificato revocato deve essere interrotto immediatamente.
Se possibile, la chiave privata appartenente al Certificato revocato deve essere distrutta immediatamente dopo la revoca.
La sospensione è una forma di revoca che sospende la validità del Certificato fino a quando:

- Viene richiesta una revoca o
- Lo stato di sospensione viene rimosso e il certificato viene ripristinato.

Regolamenti sulla responsabilità relativi alla revoca:

- Prima che la richiesta di revoca sia ricevuta dal Provider, il Soggetto e il Sottoscrittore sono responsabili per i danni che ne derivano.
- Se il Provider ha già pubblicato lo stato di revoca del Certificato, il Provider non si assume alcuna responsabilità se la Parte Affidante considera il Certificato valido.

4.8.1. Circostanze per la Revoca

L'Autorità di Certificazione agisce sulla revoca del Certificato dell'utente finale nei seguenti casi:

1. Modifica del Certificato a causa di un cambiamento dei dati relativi al Soggetto;
2. Il Provider viene a conoscenza che i dati nel Certificato non corrispondono alla realtà;
3. Se il Provider ha emesso il Certificato sulla base di un documento di una terza parte, e la terza parte ritira tale documento per iscritto;
4. Il Soggetto o il Sottoscrittore richiedono la revoca del Certificato utilizzando i canali definiti;
5. Il Provider viene a conoscenza che la chiave privata non è in possesso esclusivo del Soggetto o, nel caso del Servizio di Firma Remota, non ha il solo controllo sulla chiave privata;
6. Il Provider viene a conoscenza che il certificato è stato utilizzato illegalmente;
7. Il Sottoscrittore non ha adempiuto a uno dei suoi obblighi finanziari secondo i termini e le condizioni;
8. La cessazione del servizio;
9. Il Provider viene a conoscenza che la chiave pubblica nel Certificato non è conforme ai requisiti definiti nella Sezione 6;
10. Il Provider viene a conoscenza che il Certificato non è stato emesso in conformità con la relativa Politica del Certificato di Firma Qualificata e la Dichiarazione sulle Pratiche di Certificazione;
11. Il Provider viene a conoscenza che la chiave privata dell'unità di certificazione

dell'emittente del Certificato potrebbe essere compromessa;

12. Il formato e il contenuto tecnico del Certificato presentano un rischio inaccettabile per le Parti Affidanti (ad esempio, se l'algoritmo crittografico o la dimensione della chiave utilizzati non sono più sicuri);
13. Il Provider non è più autorizzato a emettere Certificati e la manutenzione non viene fornita per i servizi CRL e OCSP esistenti;
14. Il Provider ha cessato le sue attività;
15. La legge rende la revoca obbligatoria;
16. Il certificato di sicurezza QSCD, monitorato dal Provider, non è più valido.

4.8.2. Chi può richiedere la Revoca

La revoca del Certificato può essere avviata da:

- Il Sottoscrittore;
- Il Soggetto;
- In caso di Certificato Organizzativo, il rappresentante autorizzato dell'Organizzazione;
- La persona di contatto specificata nell'accordo di servizio;
- Il Provider.

4.8.3. Procedura per la richiesta di Revoca e Sospensione

Il Provider garantisce le seguenti possibilità per presentare una richiesta di revoca:

- In formato elettronico automatico - disponibile 24/7 - utilizzando il codice di revoca del certificato fornito al Soggetto e al Sottoscrittore quando il certificato è stato creato. Il Provider può inoltre autenticare la richiesta utilizzando i dati disponibili nel record del certificato.
- In formato elettronico sul sito web del Provider. Il Provider verificherà il diritto del richiedente a revocare il certificato utilizzando i dati disponibili nel record del certificato (ad es. e-mail, telefono cellulare).

La ragione della revoca deve essere specificata. Se la revoca è stata richiesta dal Cliente e non ne specifica la ragione, il Provider considera che la ragione della revoca è che il Soggetto non vuole più utilizzare il Certificato.
In caso di revoca andata a buon fine, il Provider notifica il Soggetto e il Sottoscrittore dell'avvenuta revoca tramite e-mail.
Il Provider registra ogni richiesta di revoca o sospensione.

4.8.4. Periodo di grazia per la richiesta di Revoca

Il Provider non applica un periodo di grazia durante l'evasione delle richieste di revoca.

4.8.5. Tempo entro il quale la CA elaborerà la richiesta di Revoca

Il Provider elabora le richieste di revoca presentate in formato elettronico immediatamente se il codice di revoca viene inviato o entro 24 ore.
Il momento di arrivo è quando il Cliente fornisce tutti i dati necessari per la revoca.

4.8.6. Requisiti di Controllo della Revoca per le Parti Affidanti

Per mantenere il livello di sicurezza garantito dal Provider, prima di adottare e utilizzare le informazioni indicate nel Certificato, è necessario che le Parti Affidanti agiscano con la dovuta cautela. Si raccomanda in particolare di verificare tutti i Certificati situati nella catena di Certificati in conformità agli standard tecnici pertinenti. La verifica deve coprire la verifica della validità dei

Certificati, dei requisiti di politica e dell'uso della chiave, e il controllo delle informazioni di revoca basate su CRL o OCSP a cui si fa riferimento.

4.8.7. Circostanze per la Sospensione

Il Provider garantisce la possibilità di sospensione temporanea del Certificato.
Il Provider ha diritto alla sospensione del Certificato per i seguenti motivi:

- Il Sottoscrittore non paga entro il termine di pagamento.
- Se il Provider presume che i dati indicati sul Certificato non corrispondano alla realtà. Se il Provider viene a conoscenza di tali condizioni, avvia la sospensione o la revoca del Certificato.
- Se il Provider presume che la chiave privata appartenente al Certificato non sia in possesso del Soggetto, e ciò è confermato da prove sostanziali. Se il Provider viene a conoscenza che il Dispositivo di Creazione della Firma Elettronica è posseduto da una persona non autorizzata, il Provider sospende ogni Certificato che contiene.

Il Provider non accetta richieste di sospensione relative a Certificati non validi, oltre a giustificare il motivo del rifiuto. I certificati sospesi possono essere riattivati.

4.8.8. Chi può richiedere la Sospensione

La sospensione di un Certificato può essere richiesta dalle stesse persone idonee a avviare la revoca del Certificato (vedere sezione 4.8.2).

4.8.9. Procedura per la richiesta di Sospensione e Ripristino

Il Provider garantisce l'opportunità di sospensione o ripristino del certificato utilizzando lo stesso canale e gli stessi tempi utilizzati per la revoca (vedere sezione 4.8.3).
Il Provider registra ogni richiesta di sospensione o ripristino. In caso di sospensione riuscita, il Provider notifica il Soggetto e il Sottoscrittore della sospensione tramite e-mail.

4.8.10. Frequenza di emissione di CRL

Il Provider emette una nuova Lista di Revoca dei Certificati (CRL) almeno una volta al giorno.
La validità di queste liste di revoca dei certificati è al massimo di 25 ore.

4.8.11. Latenza massima per le CRL

Trascorrono al massimo 5 minuti tra la generazione e la divulgazione della lista di revoca (CRL).

4.8.12. Disponibilità del Controllo di Revoca/Stato Online

Il Provider fornisce un servizio di stato del Certificato online (OCSP). Il servizio di stato è conforme ai requisiti della Sezione 4.9.

4.8.13. Requisiti speciali per la compromissione delle chiavi

In caso di compromissione di una chiave CA, il Provider compie ogni sforzo ragionevole per notificare l'incidente alle Parti Affidanti. Pubblica qualsiasi cambiamento di stato sui certificati del provider sulla sua pagina web.
Questo evento è trattato come un disastro. Tutti gli abbonati e le altre entità con un rapporto con la CA, le altre parti affidanti saranno informate.
In caso di Certificati compromessi emessi dal Provider, il Provider è in grado di revocare il Certificato dell'utente finale appartenente alla chiave privata compromessa. Le informazioni sulla

ragione della revoca (reasonCode) in questo caso sono impostate sul valore "keyCompromise".

4.8.14. Ritardo massimo per la disponibilità dello stato di revoca

Lo stato OCSP di revoca o sospensione sarà disponibile entro 60 minuti dopo che la revoca o la sospensione è stata confermata.

4.9. Servizi di Stato del Certificato

Il Provider fornisce le seguenti possibilità per la query sullo stato del Certificato:

- OCSP - servizio di query sullo stato di revoca del Certificato online,
- CRL - liste di revoca dei certificati.
- Un servizio REST per le Autorità di Registrazione che elenca tutti gli eventi del certificato (creazione, revoca, sospensione, riattivazione) dato il codice di revoca del Certificato fornito dal Soggetto o dal Sottoscrittore.

In caso di revoca, il nuovo stato del Certificato appare istantaneamente nei registri di revoca del Provider dopo il completamento riuscito del processo. Da quel momento, le risposte OCSP fornite dal Provider devono contenere il nuovo stato di revoca del certificato.
Lo stato di revoca del certificato viene mantenuto per 20 anni dopo la revoca del certificato. La CRL include l'OID "ExpiredCertsOnCRL" e la risposta OCSP include, per i certificati scaduti e revocati, l'attributo "ArchiveCutOff".
Il Provider emette una CRL straordinaria e finale con il valore del campo "next update" come definito in ETSI EN 319411-1 in caso di revoca del Certificato a causa della compromissione della chiave, immediatamente dopo aver registrato l'evento.
La risposta OCSP emessa dal Provider non deve contenere informazioni di stato "buono" per i Certificati che non sono stati emessi dalla data unità di certificazione (OCSP positivo).
In caso di cessazione del Provider, le liste dei certificati revocati verranno mantenute online per un periodo non inferiore a cinque anni.

4.9.1. Caratteristiche Operative

Ogni unità di certificazione del Provider emette una lista di revoca con la frequenza seguente:

- L'unità di certificazione "TrustPro QTSP Qualified CA I" emette una CRL al massimo una volta ogni 24 ore.

La data di efficacia delle liste di revoca "thisUpdate" segna anche il momento in cui l'unità di certificazione ha assemblato e iniziato a firmare la lista di revoca. Successivamente, in caso di liste di revoca lunghe, la pubblicazione della lista di revoca può richiedere anche 1 o 2 minuti. L'apparizione della successiva lista di revoca ("nextUpdate") segna il momento successivo, a partire dal quale la lista è pubblicamente disponibile. Di conseguenza, l'intervallo di tempo tra la data di entrata in vigore della lista di revoca e la data di pubblicazione della successiva lista di revoca può essere più lungo degli intervalli di tempo sopra, ma ciò non influisce sul fatto che l'intervallo di tempo tra la comparsa delle CRL è al massimo di 24 ore, e (in caso di una CRL relativa ai Certificati dell'Autorità di Certificazione) 1 mese.
Poiché il modo più veloce e semplice per determinare la validità del certificato è il servizio OCSP, l'Autorità di Certificazione raccomanda l'uso di OCSP ai suoi Clienti.
Il Provider fornisce il servizio OCSP in conformità al principio del "responder autorizzato" RFC 6960, quindi ogni sua unità di certificazione certifica separatamente sul responder OCSP, che fornisce informazioni sullo stato di revoca dei Certificati emessi dall'unità di certificazione (sezione 1.3.1).
Il servizio OCSP è pubblicamente e liberamente disponibile per chiunque. Non è necessaria

l'autenticazione.
Il servizio OCSP può essere raggiunto tramite gli URL indicati sui Certificati.
Le risposte OCSP contengono sempre le informazioni correnti elencate nel registro di revoca del Provider, ma se il tempo "thisUpdate" della risposta OCSP è precedente al tempo per il quale viene effettuata la verifica - che è o precedente o coincide con il tempo della query - allora la risposta OCSP non è una prova chiara per una terza parte riguardo allo stato di revoca del Certificato.

4.9.2. Disponibilità del Servizio

Il Provider assicura che la disponibilità del Repository dei Certificati e dei termini e condizioni relativi ai Certificati emessi dal Provider sia almeno del 99.953% all'anno, e la durata del downtime non deve superare al massimo 3 ore.
Il Provider assicura che la disponibilità delle informazioni sullo stato di revoca e del servizio di gestione della revoca sia almeno del 99.953% all'anno, e la durata dei downtime non deve superare al massimo 3 ore in nessuna occasione.
Il tempo di risposta del servizio di stato di revoca in caso di funzionamento normale è inferiore a 10 secondi.

4.9.3. Fine dell'Abbonamento

Il Provider può revocare i Certificati dell'utente finale in caso di risoluzione del contratto stipulato con il Sottoscrittore.

4.9.4. Servizio di Deposito e Recupero Chiavi (Key Escrow and Recovery)

Il Provider non fornisce un servizio di deposito chiavi per una chiave privata appartenente a un Certificato di firma.

5. Controlli su Strutture, Gestione e Operativi

Il Provider applica precauzioni fisiche, procedurali e di sicurezza del personale che sono conformi agli standard riconosciuti, insieme alle procedure amministrative e di governance che le applicano.Il Provider tiene un registro delle unità e delle risorse di sistema relative alla fornitura del servizio e conduce una valutazione dei rischi su di esse. Utilizza misure di protezione proporzionali ai rischi relativi ai singoli elementi.
Il Provider monitora le richieste di capacità e si assicura che la potenza di elaborazione e lo spazio di archiviazione adeguati siano disponibili per la fornitura del servizio.

5.1. Controlli Fisici

Il Provider si preoccupa che l'accesso fisico ai servizi critici sia controllato e mantiene al minimo il rischio fisico degli asset relativi ai servizi critici.
Lo scopo delle precauzioni fisiche è prevenire l'accesso illegittimo, i danni e l'accesso non autorizzato alle informazioni del Provider e alle zone fisiche.
I servizi che elaborano informazioni critiche e sensibili sono implementati in un'area sicura fornita da un fornitore selezionato.
La protezione fornita è proporzionale alle minacce identificate nell'analisi dei rischi che il Provider ha eseguito.
Per fornire un'adeguata sicurezza:

- Il Provider implementa i servizi fortemente protetti in una sala computer protetta. Questa sala computer è stata progettata e costruita specificamente per questo scopo, e la sua progettazione ha permesso un'applicazione uniforme di vari aspetti della protezione (la posizione e la struttura del sito, l'accesso fisico (controllo degli accessi e supervisione), l'alimentazione, l'aria condizionata, la protezione contro le perdite d'acqua e le inondazioni, la prevenzione e la protezione antincendio, l'archiviazione dei media, ecc.).
- L'ufficio del Servizio Clienti del Provider è stato progettato per essere in grado di soddisfare i requisiti per i servizi di registrazione a costi realistici.
- Il Provider ha costruito le sue unità di registrazione mobili in modo che rispettino i requisiti imposti al servizio di registrazione.
- Il Provider richiede ai suoi uffici esterni e alle unità mobili di avere lo stesso livello di sicurezza della sicurezza dell'ufficio di registrazione del Provider e delle unità mobili. Le condizioni e le aspettative del Provider sono registrate nel contratto con l'Autorità di Registrazione Locale.
- Il Provider implementa ogni servizio critico e ogni strumento necessario in una zona di sicurezza separata. Tutti i dispositivi necessari per questo sono posizionati in una sala computer protetta.

5.1.1. Posizione e Costruzione del Sito

Il sistema IT del Provider si trova e opera all'interno di un Data Centre adeguatamente protetto con protezione fisica e logica che previene l'accesso illegittimo. Vengono applicate soluzioni difensive - come ad esempio sorveglianza, serrature di sicurezza, sistemi di rilevamento delle intrusioni, sistema di videosorveglianza, sistema di controllo degli accessi.

5.1.2. Accesso Fisico

Il Provider protegge i dispositivi e le attrezzature che partecipano alla fornitura del servizio dall'accesso fisico non autorizzato al fine di prevenire la manomissione dei dispositivi.

Il Provider assicura che:

- Ogni ingresso al Data Centre sia registrato;
- Le persone senza autorizzazione indipendente possono rimanere nel Data Centre solo in casi giustificati, per il tempo richiesto e accompagnate dal personale con i diritti appropriati;
- I registri degli ingressi devono essere archiviati continuamente e disponibili per la valutazione.

In presenza di persone non autorizzate:

- I supporti di dati contenenti informazioni sensibili sono fisicamente fuori portata;
- I terminali con accesso effettuato non vengono lasciati senza supervisione;
- Non viene svolto alcun processo di lavoro durante il quale informazioni riservate potrebbero essere rivelate.

Quando lascia la sala computer, l'amministratore deve verificare che:

- Ogni attrezzatura del Data Centre sia in uno stato operativo adeguatamente sicuro;
- Non ci sia alcun terminale lasciato con accesso effettuato;
- I dispositivi di archiviazione fisici siano adeguatamente bloccati;
- I sistemi e i dispositivi che forniscono protezione fisica funzionino correttamente;
- Il sistema di allarme sia stato attivato.

Ci sono persone responsabili designate per condurre valutazioni regolari della sicurezza fisica. I risultati degli esami vengono registrati nelle appropriate voci di registro.

5.1.3. Alimentazione e Aria Condizionata

Il Fornitore applica un'unità di alimentazione ininterrotta nel Data Centre che:

- Ha una capacità adeguata per garantire l'alimentazione per i sistemi IT del Data Centre e le strutture sussidiarie;
- Protegge le apparecchiature IT dalle fluttuazioni di tensione nella rete esterna, interruzioni di corrente, picchi e altro;
- In caso di interruzione di corrente prolungata ha una propria attrezzatura per la generazione di energia, che - consentendo il rifornimento - è in grado di fornire l'energia necessaria per qualsiasi periodo di tempo.

L'aria dell'ambiente esterno non entra direttamente nel Data Center. La purezza dell'aria del Data Center è garantita da un sistema di filtri adeguato per rilevare una varietà di contaminanti dall'aria (polvere, inquinanti, e materiali corrosivi, sostanze tossiche o infiammabili). Il sistema di ventilazione fornisce la quantità necessaria di aria fresca con un'adeguata filtrazione per le condizioni di lavoro sicure degli operatori.
L'umidità viene ridotta al livello richiesto dai sistemi IT.
Il Fornitore utilizza sistemi di raffreddamento con prestazioni adeguate per fornire la temperatura operativa necessaria, per prevenire il surriscaldamento dei dispositivi IT.

5.1.4. Esposizione all'Acqua

Il Data Center del Fornitore è adeguatamente protetto dall'intrusione di acqua e dalle inondazioni. L'intera area della zona di sicurezza è priva di servizi igienici, non ci sono scarichi o tubi dell'acqua vicino ad essa. L'intera area della zona di sicurezza idrica è monitorata da un sistema di rilevamento delle intrusioni. Nella sala computer protetta la sicurezza è ulteriormente aumentata dall'uso di un pavimento sopraelevato.

5.1.5. Prevenzione e Protezione Antincendio

Nel Data Center del Fornitore, opera un sistema di protezione antincendio approvato dal

competente comando dei vigili del fuoco. Rilevatori di fumo e incendio allertano automaticamente i vigili del fuoco. Un sistema di estinzione automatico basato su vapore acqueo è stato installato nella sala computer, che non è pericoloso per la vita umana e non danneggia le apparecchiature IT.
Ci sono il tipo e la quantità di estintori manuali in conformità con i regolamenti pertinenti in posizioni chiaramente visibili in ogni stanza.

5.1.6. Archiviazione dei Media

Il Provider non utilizza l'archiviazione di media fisici rimovibili.

5.1.7. Smaltimento dei Rifiuti

Il Fornitore assicura lo smaltimento conforme agli standard ambientali degli asset superflui e dei media.
Il Provider non utilizza i supporti di archiviazione elettronici contenenti informazioni classificate come riservate anche per l'archiviazione di dati non classificati come riservati dopo averne cancellato il contenuto e dispositivi come questi non devono essere portati fuori dai locali del Provider. Il Provider distrugge fisicamente - secondo le regole di smaltimento - i supporti di archiviazione difettosi o per qualsiasi altro motivo inutilizzabili, ridondanti, contenenti informazioni classificate come riservate.

5.1.8. Backup

Il Provider crea un backup giornaliero dal quale l'intero servizio potrebbe essere ripristinato in caso di un errore fatale. I backup - che includono almeno l'ultimo backup completo - sono conservati in un luogo esterno la cui protezione fisica e operativa è identica al sito primario. La trasmissione sicura dei dati dal sito primario alle posizioni di backup è risolta.

5.2. Controlli Procedurali

Il Provider si preoccupa che i suoi sistemi siano gestiti in modo sicuro, secondo le regole e con un rischio minimo di difetti.
Le precauzioni procedurali hanno l'obiettivo di integrare, e allo stesso tempo intensificare, l'efficacia delle misure di sicurezza fisiche, insieme a quelle applicabili al personale, attraverso la nomina e l'isolamento di ruoli fidati, la documentazione delle responsabilità dei vari ruoli, nonché la specificazione del numero di personale e dei ruoli di esclusione necessari per i vari compiti, inoltre l'identificazione e l'autenticazione attese nei vari ruoli.
Il sistema di governance interno del Provider assicura che il suo funzionamento sia conforme ai regolamenti legali, così come ai suoi regolamenti interni. Nel suo sistema, una persona responsabile deve essere chiaramente assegnata per ogni data unità di sistema e processo.
Gli individui responsabili di un dato elemento di sistema o processo sono assegnati in modo inequivocabile a ogni elemento di sistema e a ogni processo nel suo sistema. I compiti relativi allo sviluppo e alle operazioni sono nettamente separati nel sistema del Provider. L'attività di auditing del revisore di sistema indipendente e del revisore interno del Provider garantisce il funzionamento appropriato del sistema.

5.2.1. Ruoli Fiduciari

Il Provider crea ruoli fiduciari (nella formulazione del regolamento, ambito di attività) per lo svolgimento dei suoi compiti. I diritti e le funzioni sono condivisi tra i vari ruoli fiduciari in modo tale che un utente da solo non sia in grado di bypassare le misure di protezione della sicurezza.

Il Provider definisce i seguenti ruoli fiduciari, con le seguenti responsabilità:

Manager con responsabilità generale per il sistema IT del Provider	Questo è il ruolo che supervisiona e gestisce il sistema informatico.
Responsabile della sicurezza	Questa persona ha la responsabilità generale per la sicurezza del servizio. Si occupa di garantire che tutte le misure di protezione siano implementate correttamente..
Amministratore di sistema	L'amministratore dell'infrastruttura è l'individuo incaricato di installare, configurare e mantenere i sistemi del Provider. È responsabile del funzionamento affidabile e continuo delle unità di sistema assegnate e del monitoraggio dello sviluppo della tecnologia. Si occupa anche di rilevare e proporre soluzioni per le vulnerabilità di ogni componente del sistema.
Operatore di sistema	Il system operator (operatore di sistema) è l'individuo che esegue le operazioni continue del sistema IT, come il backup e il ripristino dei dati.
Revisore di sistema	è l'individuo che verifica i set di dati registrati e archiviati del Provider. È responsabile di controllare che le misure di sicurezza implementate dal fornitore di servizi siano conformi alle normative vigenti. Inoltre, si occupa del monitoraggio e della revisione continua delle procedure esistenti.
RAO	Il ruolo dell'**Ufficiale dell'Autorità di Registrazione (RAO)** e dell'**Ufficiale dell'Autorità di Registrazione Locale** si riferisce agli individui incaricati di eseguire l'identificazione di persone fisiche e giuridiche, oltre ad autorizzare l'emissione dei certificati.

Per l'assegnazione dei ruoli di fiducia, il responsabile della sicurezza del Fornitore designa formalmente i dipendenti del Fornitore stesso. Solo le persone con un rapporto di lavoro o un contratto di collaborazione con il Fornitore possono ricoprire un ruolo di fiducia. Viene tenuta una registrazione aggiornata dei ruoli di fiducia e, in caso di qualsiasi modifica, l'autorità nazionale viene notificata senza indugio.

5.2.2. Ruoli che richiedono la separazione delle mansioni

I dipendenti del Fornitore possono ricoprire più ruoli di fiducia contemporaneamente, ma il Fornitore garantisce che:

- il responsabile della sicurezza e il responsabile della registrazione non ricoprano il ruolo di revisore di sistema indipendente
- l'amministratore di sistema non ricopra il ruolo di responsabile della sicurezza e di revisore di sistema indipendente;
- il responsabile generale del sistema IT non ricopra il ruolo di responsabile della sicurezza e di revisore di sistema indipendente.

In aggiunta a quanto sopra, il Fornitore ricerca la completa separazione dei ruoli di fiducia.

5.3. Controlli sul personale

Il Fornitore si assicura che la sua politica del personale e le sue pratiche di assunzione rafforzino e supportino l'affidabilità delle sue operazioni. L'obiettivo delle precauzioni applicabili al personale è ridurre il rischio di errori umani, furti, frodi e casi di uso improprio.
Il Fornitore si occupa della sicurezza del personale già in fase di assunzione, includendo la stipula dei contratti, così come la loro convalida al momento dell'impiego. Per tutti i ruoli di fiducia, i candidati devono possedere un valido certificato penale al momento della domanda. Ogni dipendente che ricopre un ruolo di fiducia e ogni parte esterna che entra in contatto con i servizi del Fornitore deve firmare un accordo di non divulgazione.
Allo stesso tempo, il Fornitore assicura che i suoi dipendenti ottengano un know-how comune e generale, insieme alle conoscenze professionali specialistiche necessarie per svolgere i vari compiti.

5.3.1. Qualifiche, esperienza e requisiti di idoneità

Il Fornitore richiede almeno un diploma di istruzione intermedia come requisito di assunzione e continua a garantire che i dipendenti ricevano una formazione adeguata. Immediatamente dopo l'assunzione, il Fornitore offre un corso di formazione ai nuovi dipendenti, nel corso del quale acquisiscono le conoscenze necessarie per svolgere il lavoro. Il Fornitore di solito supporta lo sviluppo professionale dei dipendenti, ma si aspetta anche che questi sviluppino autonomamente le proprie competenze nei rispettivi campi.
I ruoli di fiducia possono essere ricoperti presso il Fornitore solo da persone che non hanno influenze esterne e che possiedono le competenze necessarie, convalidate dal Fornitore.

5.3.2. Procedure di verifica del background

Il Fornitore assume per ruoli di fiducia o dirigenziali solo dipendenti che

- hanno un casellario giudiziario pulito, contro cui non sono in corso procedimenti e
- che non sono soggetti a inabilitazioni professionali che vietano l'esercizio di servizi correlati alla firma elettronica.

Durante il processo di assunzione, il Fornitore verifica l'autenticità delle informazioni pertinenti fornite nel curriculum del candidato.

5.3.3. Requisiti di formazione

Il Fornitore forma i dipendenti appena assunti, nel corso del quale acquisiscono:

- conoscenze di base sulla PKI (Infrastruttura a Chiave Pubblica);
- le specificità e le modalità di gestione del sistema IT del Fornitore;

- le conoscenze speciali necessarie per svolgere le loro attività;
- i processi e le procedure definiti nei regolamenti pubblici e interni del Fornitore;
- le conseguenze legali delle singole attività
- le normative applicabili sulla sicurezza informatica nella misura necessaria al loro specifico ambito di attività;
- le norme sulla protezione dei dati.

Il Fornitore forma i dipendenti addetti alla registrazione riguardo ai pericoli e ai rischi legati alla verifica dei dati da inserire nel Certificato.
Prima della loro nomina, i dipendenti addetti alla registrazione sostengono e superano un esame sulla conoscenza dei requisiti e delle procedure relative alla verifica dei dati, e questo fatto viene documentato dal Fornitore. Solo i dipendenti che hanno superato la formazione ottengono l'accesso al sistema IT di produzione del Fornitore.

5.3.4. Frequenza e requisiti di aggiornamento

Il Fornitore si assicura che i dipendenti possiedano le conoscenze necessarie in modo continuativo, per cui, se necessario, vengono tenuti corsi di formazione aggiuntivi o di aggiornamento.
La formazione aggiuntiva viene svolta se ci sono modifiche rilevanti nei processi o nel sistema IT del Fornitore. La formazione è adeguatamente documentata, in modo che il programma e l'ambito dei dipendenti partecipanti possano essere chiaramente determinati.

5.3.5. Frequenza e sequenza della rotazione delle mansioni

Il Fornitore non applica la rotazione obbligatoria tra i singoli schemi di lavoro.

5.3.6. Sanzioni per azioni non autorizzate

Il Fornitore disciplina le possibilità di sanzione dei dipendenti in contratto di lavoro in caso di mancanze, errori, danni accidentali o intenzionali. Se il dipendente - per negligenza o intenzionalmente - viola i suoi obblighi, il Fornitore può prendere sanzioni contro di lui, che stabilisce tenendo conto dell'infrazione e delle conseguenze.

5.3.7. Requisiti per i collaboratori esterni

Il Fornitore seleziona le persone impiegate con contratto di collaborazione o subappalto per svolgere gli altri compiti, scegliendo, se possibile, da un elenco di fornitori qualificati. Il Fornitore stipula un contratto scritto prima di lavorare con i fornitori.
Ogni parte contraente - prima dell'inizio del lavoro attivo - firma una dichiarazione di riservatezza in cui accetta che i segreti aziendali appresi in seguito non saranno divulgati a persone non autorizzate e non saranno sfruttati in altro modo. La dichiarazione di riservatezza include sanzioni in caso di violazione. Si prevede che i collaboratori esterni impiegati con il contratto abbiano competenze tecniche appropriate, e il Fornitore non tiene per loro corsi di formazione

5.3.8. Documentazione fornita al personale

Il Fornitore garantisce continuamente ai dipendenti la disponibilità della documentazione e dei regolamenti aggiornati necessari per svolgere i loro ruoli.
Ogni dipendente che ricopre un ruolo di fiducia riceve i seguenti documenti:

- i regolamenti di sicurezza organizzativa del Fornitore,
- l'accordo di riservatezza firmato,
- materiali didattici in occasione della formazione pianificata o speciale per la specifica

forma di istruzione.

Tutti i dipendenti sono informati con una comunicazione scritta di eventuali modifiche ai regolamenti di sicurezza organizzativa.

5.4. Procedure di registrazione dei controlli

Al fine di mantenere un ambiente IT sicuro, il Fornitore implementa e gestisce un sistema di registrazione e controllo degli eventi che copre l'intero sistema IT.

5.4.1. Tipi di eventi registrati

Il Fornitore registra ogni evento legato alla sicurezza che può fornire informazioni su cambiamenti avvenuti nel sistema IT o nel suo ambiente fisico, in conformità con le pratiche di sicurezza informatica generalmente accettate. Per ogni voce del registro, memorizza i seguenti dati:

- l'orario dell'evento;
- il tipo di evento
- il successo o il fallimento dell'implementazione (se applicabile);
- l'identificazione dell'utente o del sistema che ha attivato l'evento.

Tutti i registri degli eventi essenziali sono a disposizione dei revisori di sistema indipendenti, che esaminano la conformità delle operazioni del Fornitore.

5.4.2. Frequenza di elaborazione dei registri di controllo.

I revisori di sistema indipendenti del Fornitore valutano i file di registro generati con la frequenza definita nelle procedure di sicurezza.

Durante la valutazione, viene assicurata l'autenticità e l'integrità dei registri esaminati, i messaggi di errore nei registri vengono controllati e, se necessario, le differenze vengono documentate e vengono prese misure per eliminare la causa della deviazione.

Per la valutazione del sistema IT, il Fornitore utilizza anche strumenti di valutazione automatizzati, che vengono impiegati per monitorare le voci di registro risultanti in base a criteri preimpostati e, ove necessario, allertare il personale operativo.

Il fatto dell'indagine, i risultati dell'indagine e le misure intraprese per prevenire le carenze riscontrate sono adeguatamente documentati.

5.4.3. Periodo di conservazione dei registri di controllo

Prima della cancellazione dal sistema online, i registri vengono archiviati e la loro conservazione sicura è garantita dal Fornitore per 6 mesi.

Per tale periodo di tempo, il Fornitore garantisce la leggibilità dei dati archiviati e mantiene i software e gli hardware necessari a tal fine.

5.4.4. Protezione dei registri di controllo

Il Fornitore protegge i registri creati per il tempo di conservazione richiesto. Durante l'intero periodo di conservazione, sono assicurate le seguenti proprietà dei dati dei registri:

- protezione contro la divulgazione non autorizzata: solo le persone autorizzate - principalmente i revisori di sistema indipendenti - accedono ai registri;
- disponibilità: alle persone autorizzate viene concesso l'accesso ai registri;
- integrità: viene prevenuta qualsiasi alterazione dei dati, cancellazione nei file di registro e modifica dell'ordine delle voci, ecc.

Il Fornitore protegge le registrazioni dei registri con marche temporali qualificate e le memorizza in modo da escludere l'inserimento e la cancellazione non tracciabili delle voci del registro.

I file di registro sono protetti contro danni accidentali e dolosi tramite backup. In caso di voci di registro contenenti dati personali, il Fornitore si assicura della conservazione riservata dei dati. Solo le persone che ne hanno assolutamente bisogno per il loro lavoro hanno il diritto di accedere alle voci di registro. Il Fornitore verifica gli accessi in modo sicuro. Il Fornitore conserva i file di registro in un ambiente sicuro. Mantiene copie dei file presso il secondo sito operativo.

5.4.5. Procedure di backup dei registri di controllo.

I file di registro giornalieri vengono creati dalle voci di registro generate in modo continuo durante l'operazione in ogni sistema.
I file di registro giornalieri vengono archiviati in due copie dopo la valutazione e conservati fisicamente separati l'uno dall'altro, in siti distinti per il tempo richiesto.
Il processo esatto dei backup è definito nei regolamenti sui backup del Fornitore

5.4.6. Sistema di raccolta dei controlli

Ogni applicazione raccoglie e invia automaticamente le registrazioni al sistema di registrazione. Le funzioni di registrazione iniziano automaticamente al momento dell'avvio del sistema e vengono eseguite in modo continuo per l'intero periodo di funzionamento del sistema.
In caso di anomalia nei sistemi di esame e registrazione automatici, il Fornitore sospende il funzionamento delle aree correlate fino a quando l'incidente non viene risolto.

5.4.7. Notifica al soggetto che ha causato l'evento

Le persone, le organizzazioni e le applicazioni che hanno causato l'evento di errore non vengono sempre notificate, ma se necessario, il Fornitore le coinvolge nell'indagine sull'evento. I Clienti interessati dall'attivazione dell'evento hanno il dovere di cooperare con il Fornitore per l'analisi dell'evento.

5.4.8. Valutazioni della vulnerabilità.

Il Fornitore esamina periodicamente gli eventi straordinari ed esegue un'analisi della vulnerabilità, in base alla quale il Fornitore, se necessario, prende misure per aumentare la sicurezza del sistema.

5.5. Archiviazione dei registri

5.5.1. Tipi di registri archiviati.

I principali tipi di registri archiviati a lungo termine dal Fornitore sono:

- tutti i documenti relativi all'accreditamento del Fornitore (documento);
- tutte le versioni emesse delle Politiche sui Certificati e delle Dichiarazioni sulle Pratiche di Certificazione (documenti);
- tutte le versioni emesse dei Termini e Condizioni (documenti);
- i contratti relativi all'operatività del Fornitore (documenti);
- tutte le informazioni relative alla registrazione del Soggetto e del Sottoscrittore (registri);
- le informazioni relative al Certificato per l'intero ciclo di vita (registri).

5.5.2. Periodo di conservazione dell'archivio

Il Fornitore conserva i dati archiviati per **20 anni** dopo la data di scadenza del certificato correlato.

5.5.3. Protezione dell'archivio

Il Fornitore memorizza tutti i dati archiviati in **due copie** in luoghi fisicamente separati l'uno dall'altro. Una copia autentica, cartacea o elettronica, viene creata in conformità con la legge applicabile dall'unica copia autentica cartacea del documento disponibile.
Ognuna delle due sedi soddisfa i requisiti di sicurezza per l'archiviazione e altri requisiti. Durante la conservazione dei dati archiviati, viene garantito che:

- la loro **integrità** sia preservata;
- siano protetti da **accessi non autorizzati**;
- siano **disponibili**;
- ne venga preservata l'**autenticità**.

I documenti elettronici archiviati sono muniti di una firma o un sigillo elettronico qualificato e di una marca temporale qualificata.

5.5.4. Procedure di backup dell'archivio

Il Fornitore conserva i documenti cartacei in una singola copia originale e ne crea una copia elettronica autentica in conformità con la legislazione pertinente. Le copie elettroniche sono conservate secondo le stesse regole degli altri documenti elettronici protetti.

5.5.5. Sistema di raccolta dell'archivio

Le voci di registro vengono generate nel sistema informatico protetto del Fornitore, e solo i file di registro che sono protetti elettronicamente con marche temporali qualificate possono uscirne.
Una copia originale dei documenti creati durante la fornitura del servizio è conservata e protetta dal Fornitore in un proprio sistema di archiviazione dati interno.

5.5.6. Procedure per ottenere e verificare le informazioni dell'archivio

I documenti archiviati sono protetti da accessi non autorizzati.
L'accesso controllato ai documenti archiviati è disponibile solo per le persone idonee:

- i **Clienti** hanno il diritto di vedere i dati conservati su di loro;
- in caso di **contenzioso legale**, al fine di fornire prove, devono essere forniti i dati necessari.

5.6. Sostituzione della chiave CA

Il Fornitore garantisce che le Unità di Certificazione utilizzate possiedano continuamente una chiave e un Certificato validi per il loro funzionamento. A tal fine, con sufficiente anticipo rispetto alla scadenza dei loro Certificati e alla scadenza d'uso delle chiavi a essi correlate, genera una nuova coppia di chiavi per le Unità di Certificazione e informa tempestivamente i suoi Clienti. La nuova chiave del fornitore viene generata e gestita in conformità con questo regolamento.

5.7. Compromissione e ripristino in caso di disastro

Il Fornitore mantiene un sito di **Disaster Recovery**, a una distanza di sicurezza dalla sede principale, con una replica dell'infrastruttura hardware e software di produzione. Viene mantenuto un backup completo dei dati tra l'infrastruttura principale e quella di disaster recovery.
In caso di disastro, il Fornitore prende tutte le misure necessarie per minimizzare i danni derivanti dall'indisponibilità del servizio e ripristina i servizi il più rapidamente possibile.
In base alla valutazione dell'incidente avvenuto, il Fornitore apporta gli emendamenti e le misure correttive necessarie per prevenire il ripetersi dell'incidente in futuro.
Una volta risolto il problema, l'evento viene segnalato all'Autorità Nazionale, in qualità di autorità

di vigilanza.
Il Fornitore testa periodicamente il passaggio al sistema di Disaster Recovery e rivede i suoi piani di continuità aziendale.

5.7.1. Corruzione di risorse, software e dati

I sistemi IT del Fornitore sono costruiti con componenti hardware e software affidabili. Le funzioni critiche sono implementate utilizzando elementi di sistema ridondanti in modo che, in caso di guasto di un elemento, possano continuare a operare.
Il piano di continuità aziendale del Fornitore include requisiti precisi per le attività da svolgere in caso di guasto di un componente critico del sistema.

5.7.2. Procedure in caso di compromissione della chiave privata dell'entità

In caso di compromissione della chiave privata del Fornitore di Servizi Fiduciari, verranno intraprese le seguenti azioni senza indugio:

- tutti i Certificati interessati del Fornitore di Servizi Fiduciari saranno revocati;
- verrà generata una nuova chiave privata del fornitore per il ripristino dei servizi;
- i dati del Certificato del fornitore revocato saranno divulgati secondo il metodo regolamentato nella Sezione 2.2;
- le informazioni relative alla compromissione saranno divulgate a ogni Sottoscrittore e Soggetto;
- il Fornitore pubblicherà un avviso sulla revoca della chiave pubblica del fornitore.

5.7.3. Capacità di continuità aziendale dopo un disastro

Le attività da svolgere in caso di interruzione del servizio a causa di disastri naturali o di altro tipo sono definite nel piano di continuità aziendale del Fornitore.
Il Fornitore ha un fornitore esterno che esegue il piano di disaster recovery per i sistemi IT.

5.8. Cessazione dei Servizi Fiduciari Qualificati

Nella fase di cessazione, il Fornitore deve eseguire le attività definite nel suo **Piano di Cessazione**:

- l'Autorità Nazionale, le Parti Contraenti e i Sottoscrittori devono essere informati della cessazione pianificata in tempo utile (almeno 90 giorni prima);
- il Fornitore di Servizi Fiduciari deve fare ogni sforzo per garantire che, prima della cessazione del servizio, un altro fornitore si faccia carico dei registri e degli obblighi di servizio;
- la nuova emissione di Certificati deve essere interrotta;
- i Certificati del Fornitore devono essere revocati e le chiavi private del fornitore devono essere distrutte;
- dopo la cessazione del servizio, deve essere eseguito un backup completo del sistema e un'archiviazione, inclusa l'ultima CRL (Certificate Revocation List) emessa;
- i dati archiviati devono essere consegnati al fornitore che subentra nei servizi;
- nel caso in cui non si trovi un altro fornitore a nessuna condizione, tutti i certificati degli utenti finali devono essere revocati e una CRL finale deve essere mantenuta fino alla data di scadenza dell'ultimo certificato utente finale emesso.

6. Controlli tecnici di sicurezza

Il Fornitore utilizza sistemi composti da apparecchiature affidabili e tecnicamente valutate per la sicurezza per la fornitura dei suoi servizi. Il Fornitore gestisce le chiavi crittografiche del fornitore per l'intero ciclo di vita all'interno di un **Hardware Security Module** che possiede una Certificazione appropriata.
Sia il Fornitore che il fornitore di sistema e i subappaltatori hanno una significativa e lunga esperienza con prodotti, tecnologie e standard PKI (Infrastruttura a Chiave Pubblica).

6.1. Generazione e installazione della coppia di chiavi

Il Fornitore si assicura che la generazione e la gestione di tutte le chiavi private da esso generate - per sé, per i suoi dipartimenti (ad esempio, Repository dei Certificati, Autorità di Registrazione) e per i Soggetti - siano sicure e conformi ai requisiti normativi in vigore e agli standard del settore.

6.2. Generazione della coppia di chiavi

Il Fornitore utilizza algoritmi di generazione delle chiavi che sono conformi ai requisiti stabiliti nella seguente normativa:

ETSI TS 119 312 [8];

In caso di generazione di una propria coppia di chiavi, il Fornitore garantisce che:

- la creazione della chiave privata del fornitore venga effettuata in un ambiente protetto (vedi sezione 5.1), con due persone autorizzate che ricoprono un ruolo di fiducia (vedi sezione 5.2.1) contemporaneamente, escludendo la presenza di altre persone non autorizzate.
- la creazione della chiave privata del fornitore venga effettuata in dispositivi conformi (vedi sezione 6.3).
- la produzione della chiave privata del fornitore venga eseguita utilizzando l'applicazione di gestione centrale della CA (Certification Authority).
- la creazione delle chiavi venga effettuata in un ambiente protetto con la presenza esclusiva di persone che ricoprono ruoli di fiducia.
- in caso di Politiche sui Certificati che richiedono l'uso di un Dispositivo Qualificato per la Creazione della Firma, la chiave privata di firma venga generata nel Dispositivo Qualificato per la Creazione della Firma del Soggetto, il che rende impossibile la divulgazione della chiave privata di firma.
- se la chiave privata viene consegnata al Soggetto, le chiavi del firmatario generate al di fuori di un Dispositivo Qualificato per la Creazione della Firma vengano conservate in un ambiente adeguatamente sicuro dal Fornitore per prevenire la divulgazione. Dopo la consegna documentata della chiave privata del firmatario al Soggetto, il Fornitore distrugge ogni copia della chiave privata consegnata che ha conservato, in modo tale che il suo ripristino e utilizzo diventino impossibili.

6.2.1. Consegna della chiave privata al Sottoscrittore

Se il Fornitore genera la chiave privata del Soggetto, devono essere soddisfatti i seguenti requisiti:

- Durante l'intero servizio, il Fornitore deve conservare in modo sicuro le chiavi private da esso generate per i Soggetti e i dati di attivazione per prevenire la divulgazione, la copia, la modifica, il danneggiamento e l'utilizzo da parte di persone non autorizzate.
- Il Fornitore deve utilizzare una procedura di identificazione che garantisca che le chiavi private possano essere utilizzate solo dal Soggetto.

Se il Fornitore non genera la chiave privata del Soggetto:

- In caso di Politiche sui Certificati che non richiedono l'uso di un Dispositivo Qualificato per la Creazione della Firma, il Cliente genera la chiave privata.
- In caso di Politiche sui Certificati che richiedono l'uso di un Dispositivo Qualificato per la Creazione della Firma, il Cliente genera sempre la chiave privata all'interno del Dispositivo Qualificato per la Creazione della Firma.

6.2.2. Consegna della chiave pubblica CA alle Parti Contraenti

Il Fornitore di Servizi Fiduciari deve mettere a disposizione delle Parti Contraenti i suoi Certificati di fornitore di livello superiore in modo tale da rendere impossibili gli attacchi volti alla modifica delle chiavi.
La chiave pubblica è contenuta nel Certificato. Il Fornitore pubblica i certificati a questo indirizzo: https://docs.trustpro.eu.

6.2.3. Dimensioni delle chiavi

Il Fornitore utilizza algoritmi e dimensioni minime delle chiavi che sono conformi ai requisiti stabiliti nel seguente standard:

ETSI TS 119 312 [8].

Il Fornitore utilizza chiavi RSA di almeno 4096 bit in ogni Certificato root attualmente attivo.

6.2.4. Scopi di utilizzo della chiave

La chiave privata dell'unità di certificazione root del Fornitore può essere utilizzata solo per i seguenti scopi:

- Emissione del Certificato autofirmato dell'unità di certificazione root stessa.
- Emissione di certificati utente finale.
- Per firmare il Certificato del risponditore OCSP o la risposta OCSP.
- Per firmare le CRL.

Il Fornitore include le estensioni di "Uso della Chiave" nei certificati utente finale, definendo l'ambito di utilizzo del Certificato e, nelle applicazioni compatibili con X.509v3 [30], limita tecnicamente l'utilizzo dei Certificati.

6.2.5. Protezione della chiave privata e controlli ingegneristici del modulo crittografico

Il Fornitore garantisce la gestione sicura delle chiavi private da esso detenute e previene la divulgazione, la copia, la cancellazione, la modifica e l'utilizzo non autorizzato della chiave privata.
Il Fornitore conserverà le chiavi private solo per il tempo strettamente necessario alla fornitura del servizio.

6.2.6. Standard e controlli dei moduli crittografici

I sistemi del Fornitore che emettono Certificati, firmano risposte OCSP e liste CRL conservano le chiavi private in dispositivi hardware che sono conformi a:

- i requisiti di ISO/IEC 19790 [9], o
- i requisiti di FIPS 140-2 [10] 3,
- o i requisiti di un livello superiore, oi requisiti dell'accordo del gruppo di lavoro CEN 14167-2 [11], o
- sono sistemi affidabili che sono valutati a un livello di garanzia 4 o superiore secondo

ISO/IEC 15408 [12] o un sistema di criteri di sicurezza equivalente. La valutazione deve essere basata sul piano di sicurezza appropriato che soddisfa i requisiti del presente documento, o su appositi stanziamenti di sicurezza.

6.2.7. Controllo multi-persona della chiave privata

Il Fornitore implementa il controllo "2 su 5" all'attivazione delle funzioni di gestione della chiave privata. I parametri sono determinati in modo che la presenza simultanea di almeno due dipendenti che ricoprono ruoli di fiducia sia necessaria per le operazioni critiche eseguite con le sue chiavi private del fornitore.

6.2.8. Deposito della chiave privata (Escrow)

Il Fornitore non deposita in escrow la propria chiave privata del fornitore.

6.2.9. Backup della chiave privata

Il Fornitore esegue copie di sicurezza delle sue chiavi private del fornitore, prima di mettere la chiave privata in servizio in un ambiente protetto, in presenza simultanea di almeno due persone che ricoprono ruoli di fiducia, con l'esclusione di altre persone.
Gli stessi standard di sicurezza rigorosi sono applicati alla gestione e alla conservazione dei backup come per il funzionamento del sistema di produzione.

6.2.10. Archiviazione della chiave privata

Il Fornitore non archivia le sue chiavi private né le chiavi private del firmatario utente finale.

6.2.11. Trasferimento della chiave privata in o da un modulo crittografico

Tutte le chiavi private del fornitore sono create in un Hardware Security Module che soddisfa i requisiti.

6.2.12. Conservazione della chiave privata sul modulo crittografico

Il Fornitore conserva le sue chiavi private utilizzate per la fornitura del servizio negli Hardware Security Modules.

6.2.13. Metodo di attivazione della chiave privata

Il Fornitore conserva le sue chiavi private in un Hardware Security Module sicuro. La chiave può essere attivata solo tramite le corrispondenti schede operatore e le chiavi private all'interno dell'Hardware Security Module non possono essere utilizzate prima di attivare il modulo. Il Fornitore conserva le schede operatore in un ambiente sicuro e tali schede possono essere raggiunte solo da dipendenti autorizzati del Fornitore.
Il Fornitore garantisce che le firme possano essere create solo con la chiave privata del certificato dell'unità root in caso di comandi emessi direttamente dal funzionario di fiducia debitamente autorizzato a farlo.
In caso di chiavi private utente finale generate dal Fornitore, esso garantisce che le chiavi private e i dati di attivazione della chiave privata siano generati e gestiti in modo adeguatamente sicuro che esclude la possibilità di un uso non autorizzato della chiave privata.

6.2.14. Metodo di disattivazione della chiave privata

La chiave privata gestita dai dispositivi crittografici viene disattivata se il dispositivo viene rimosso dallo stato attivo. Ciò può verificarsi nei seguenti casi:

- l'utente disattiva la chiave,
- l'alimentazione del dispositivo viene interrotta (spento o problema di alimentazione),
- il dispositivo entra in uno stato di errore.

La chiave privata disattivata in questo modo non può essere utilizzata fino a quando il modulo non è nuovamente in stato attivo.

6.2.15. Metodo di distruzione della chiave privata

Il Fornitore distrugge le chiavi private del fornitore memorizzate nel sicuro Hardware Security Module secondo le procedure e i requisiti definiti nella guida utente e nei documenti di certificazione dell'Hardware Security Module utilizzato.
Il Fornitore distrugge ogni copia di backup della chiave privata in modo documentato, in modo tale che il suo ripristino e utilizzo diventino impossibili.

6.2.16. Periodi operativi dei certificati e periodi di utilizzo della coppia di chiavi

Il periodo di validità dei certificati dell'unità di certificazione root del Fornitore e delle chiavi private a essi appartenenti non deve superare il tempo fino al quale gli algoritmi crittografici utilizzati possono essere usati in sicurezza secondo la decisione algoritmica dell'Autorità Nazionale.
I certificati CA sono validi per 20 anni e il certificato utente finale standard è valido per 3 anni. Su richiesta del Sottoscrittore, il Fornitore può emettere certificati utente finale con un tempo di validità diverso.

6.3. Dati di Attivazione

I dipendenti del **Fornitore** gestiscono in modo sicuro i dispositivi per l'attivazione delle chiavi private e i dati di attivazione, li proteggono utilizzando misure tecniche e organizzative e le password vengono archiviate unicamente in formato crittografato.

6.4. Controlli di Sicurezza Informatica

6.4.1. Requisiti Tecnici Specifici per la Sicurezza Informatica

Durante la configurazione e il funzionamento del suo sistema informatico, il **Fornitore** garantisce il rispetto dei seguenti requisiti:

- l'identità dell'utente è verificata con controlli di autenticazione a due fattori;
- i ruoli sono assegnati agli utenti e si assicura che tutti gli utenti abbiano solo le autorizzazioni appropriate per il proprio ruolo;
- viene creata una voce di log per ogni transazione, e le voci di log sono archiviate;
- per i processi critici per la sicurezza, si garantisce che i domini della rete interna del **Fornitore** siano adeguatamente protetti da accessi non autorizzati.

6.4.2. Controlli Tecnici del Ciclo di Vita

Il fornitore ha definito come azienda fornitrice un sistema di gestione della sicurezza delle informazioni certificato secondo lo standard ISO 27001 [14].

I controlli di sicurezza fondamentali forniti dal fornitore sono:

- Controllo degli accessi
- Sicurezza degli asset
- Sicurezza operativa
- Sicurezza nello sviluppo del software
- Gestione degli incidenti
- Continuità aziendale
- Sicurezza della rete

6.5. Precisione Temporale

La precisione dell'ora di sistema è garantita dal protocollo **NTP** (Network Time Protocol). La sorgente temporale esterna è un istituto metrologico nazionale affidabile e ufficiale.

7. Profili del Certificato, CRL e OCSP

I certificati CA hanno la seguente struttura:

Version	Version 3
Serial Number	Serial number of the certificates
Signature	sha256, RSA
Issuer (ETSI 319 412-2 par. 4.2.3.1)	Issuer DN: **countryName**:"IE" **organizationName**: "TrustPro QTSP Ltd" **L**="Dublin" **OU**="QTSP" **organizationIdentifier** : "NTRIE-637218" **commonName**: [ROOT CA NAME]
Validity Period	20 anni (scadono 20 anni dalla data di emissione)
Subject	Issuer DN: **countryName**:"IE" **organizationName**: "TrustPro QTSP Ltd"**organizationIdentifier**:"NTRIE-637218" **L**="Dublin", **OU**="QTSP" **commonName** : [CA NAME]
SubjectPublicKeyInfo	Public Key 4096 bit Algorithm: RSA
Extensions	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
Basic Constraint (critical)	Subject Type: CA Path Length Constraint: 0
KeyUsage (critical)	CertSign, cRLSign
Policy Constraints	requireExplicitPolicy : 0

7.1. Profili dei certificati

I certificati per l'utente finale emessi dal **Fornitore** e i certificati dell'unità di certificazione del fornitore utilizzati durante il servizio sono conformi alle seguenti raccomandazioni e requisiti:

- ITU X.509 V3 Tecnologia dell'informazione - Interconnessione di sistemi aperti - L'elenco: Framework di certificati a chiave pubblica e attributi [15]
- RFC 5280 [16]
- RFC 6818 [17]
- ETSI EN 319 41 1-1 [2]
- ETSI EN 319 41 1-2 [3]
- ETSI EN 319 412- l [4]
- ETSI EN 319 412-2 [5]
- ETSI EN 319 412-3 [6]
- ETSI EN 319 412-5 [7]

7.1.1. Numero di Versione

I certificati dell'unità di certificazione utilizzati dal **Fornitore** e i certificati per l'utente finale emessi dal **Fornitore** sono certificati "v3" in base alla specifica X.509 V3 [15].

7.1.2. Estensioni del Certificato

Il **Fornitore** utilizza esclusivamente le estensioni del certificato in conformità con la specifica X.509 [15] e con la IETF RFC 3739 [18] (clausola 3.2.6). L'utilizzo è conforme allo standard ETSI 319 412-5 [7].

7.1.3. Identificatori dell'Oggetto Algoritmo

La denominazione dell'algoritmo che è stato utilizzato per certificare il certificato. I seguenti algoritmi sono utilizzati dall'Autorità di Certificazione per sigillare i certificati dell'utente finale:

SHA256With RSAEncryption.

7.1.4. Forme del Nome

Il **Fornitore** utilizza un **nome distinto** (distinguished name) - composto da attributi definiti negli standard di profilo del certificato sopra citati per l'identificazione del Soggetto nei certificati emessi in base a questa Dichiarazione di Prassi di Certificazione.

Il Certificato contiene l'identificatore globalmente univoco del Soggetto, compilato come definito nella Sezione 3.1.1.

Il valore nel campo "**Issuer DN**" (DN dell'Emittente) del Certificato è identico al valore nel campo "**Subject DN**" (DN del Soggetto) del certificato dell'emittente.

7.1.5. Vincoli del Nome

Il **Fornitore** non utilizza vincoli di nome (name constraints) con l'uso del campo "**nameConstraints**".

7.1.6. Identificatori dell'Oggetto della Politica del Certificato

Il **Fornitore** include l'estensione non critica "Certificate Policy" (Politica del Certificato) nei certificati in base ai requisiti della Sezione 7.1.2.

I seguenti identificatori di oggetto (Object Identifiers) identificano le politiche ETSI EN 319411-2 [3].

OID	Policy	Person	QSCD	SCD
1.3.6.1.4.1.52969.1.1	QCP-n	Natural	no	no
1.3.6.1.4.1.52969.1.2	QCP-1	Legal	no	no
1.3.6.1.4.1.52969.1.3	QCP-n-qscd	Natural	yes	no
1.3.6.1.4.1.52969.1.4	QCP-1-qscd	Legal	Yes	No

7.1.7. Dettagli del profilo del certificato per l'utente finale

In questa sezione sono descritti i dettagli dei campi del certificato supportati per ogni politica di certificazione.

7.1.7.1. Politica QCP-n: certificato qualificato per persona fisica

Serial Number	Certificate serial number
Issuer DN	**CN**= [CA NAME] **C** =" IE" O= "TrustPro QTSP Ltd" **OU**=" QTSP"**L**=" Dublin" organizationIdentifier= " NTRIE-637218 "

Subject DN	**CN**= [subject given name and subject surname], **SN**=[subject surname], **G**=[subject given name], **email**=[subject email], **dnQualifier**=[subject unique ID], **C**= [subject country], **serialNumber**= [according to ETSI EN 319 412-1 par. 5.1.3]
Validity Period	3 anni come definite nel contratto stipulato con il sottoscrittore
SubjectPublicKeyInfo	Public Key 2048 bit Algorithm: RSA
Extensions	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
Basic Constraint	Subject Type: NO CA Path Length Constraint: none
KeyUsage	No repudiation
Certificate Policies	Policy OID 0.4.0.1941 12.1.0: qualified certificates issued to natural persons Policy OID, 1.3.6.1.4.1.52969 .1 .1, CP URL: https://docs.trustpro.eu/trustpro-cpcps-en.pdf
CRL distribution point	http://ca.trustpro.eu/crls/[CANAME].crl
Authority Information Access	OCSP, http://ca.trustpro.eu/ocsp/
QC Statements	id-etsi-qcs-QcCompliance (OID 0.4.0.1862.1.1); id-etsi-qcs-QcRetentionPeriod (OID 0.4.0.1862.1.3) = 20; id-etsi-qcs-QcPDS (OID 0.4.0.1862.1.5) = https://docs.trustpro.eu/trustpro-pds-en.pdf , “en”

7.1.7.2. Policy QCP-1: certificato qualificato per persona giuridica

Serial Number	Certificate serial number
Issuer DN	**CN**= [CA NAME] C =" IE" O= "TrustPro QTSP Ltd" OU=" QTSP" **L**="Dublin" **organizationIdentifier**= " NTRIE-637218 "
Subject DN	**CN**= [subject common name], **dnQualifier**=[subject unique ID], **C**=[subject country], **serialNumber**=[according to ETSI EN 319 412-1 par. 5.1 .4]
Validity Period	3 anni o come definito nel contratto con il sottoscrittore.
SubiectPublicKeyInfo	Public Key 2048-bit Algorithm: RSA
Extensions	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
Basic Constraint	Subject Type: NO CA Path Length Constraint: none
KeyUsage	No repudiation
Certificate Policies	Policy OID 0.4.0.194112.1.1: qualified certificates issued to legal persons Policy OID, 1.3.6.1.4.1.52969.1.2, CP URL: https://docs.trustpro.eu/trustpro-cpcps-en.pdf
CRL distribution point	http://ca.trustpro.eu/crls/[CANAME].crl
Authority Information	OCSP, http://ca.trustpro.eu/ocsp/

QC Statements	id-etsi-qcs-QcCompliance (OID 0.4.0.1862.1.1); id-etsi-qcs-QcRetentionPeriod (OID 0.4.0.1862.1.3) = 20; id-etsi-qcs-QcPDS (OID 0.4.0.1862.1.5) = https://docs.trustpro.eu/trustpro-pds-en.pdf, “en”; id-etsi-qct-eseal 2 (OID 0.4.0.1862.1.6.2)

7.1.7.3. Policy OCP-n-qscd: Certificato qualificato per persona fisica su QSCD

Serial Number	Certificate serial number
Issuer DN	**CN**=[CA NAME] **C** =“IE” **O**=“TrustPro QTSP Ltd” **OU**=”QTSP” **L**=”Dublin” **organizationIdentifier**=” NTRIE-637218”
Subject DN	**CN**= [subject given name and subject surname], **SN**=[subject surname], **G**=[subject given name], **email**=[subject email], **dnQualifier**=[subject unique ID], **C**= [subject country], **serialNumber**= [according to ETSI EN 319 412-1 par. 5.1.3]
Validity Period	3 anni o come definito nel contratto con il sottoscrittore.
SubjectPublicKeyInfo	Public Key 2048-bit Algorithm: RSA
Extensions	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
Basic Constraint	Subject Type: NO CA Path Lenoth Constraint: none
KeyUsage	No repudiation
Certificate Policies	Policy OID 0.4.0.1941 12.1.2: qualified certificates issued to natural persons with private key on QSCD Policy OID, 1.3.6.1 .4.1.52969.1.3,CP URL: https://docs.trustpro.eu/trustpro-cpcps-en.pdf
CRL distribution point	http://ca.trustpro.eu/crls/[CANAME].crl
Authority Information Access	OCSP, http://ca.trustpro.eu/ocsp/
QC Statements	id-etsi-qcs-QcCompliance (OID 0.4.0.1862.1.1); id-etsi-qcs-QcRetentionPeriod (OID 0.4.0.1862.1.3) = 20; id-etsi-qcs-QcSSCD (OID 0.4.0.1862.1.4) id-etsi-qcs-QcPDS (OID 0.4.0.1862.1 .5) = https://docs.trustpro.eu/trustpro-pds-en.pdf, “en”

7.1.7.4. Policy OCP-1-qscd: Certificato qualificato per persona giuridica su QSCD

Serial Number	Certificate serial number
Issuer DN	**CN**= [CA NAME] C =" IE" **O**= "TrustPro QTSP Ltd" **OU**=" QTSP" **L**=" Dublin” **organizationIdentifier**=" NTRIE-637218 "

Subject DN	**CN**= [subject common nome], **dnQualifier**=[subject unique ID], **C**=[subject country], **serialNumber**=[according to ETSI EN 319 412-1 par. 5.1.4]
Validity Period	3 anni o come definito nel contratto con il sottoscrittore.
SubjectPublicKeyInfo	Public Key 2048-bit Algorithm: RSA
Extensions	
Authority Key Identifier	SHA-1 160 bit
Subject Key Identifier	SHA-1 160 bit
Basic Constraint	Subject Type: NO CA[s}] Path Length Constraint: none
KeyUsage	No repudiation
Certificate Policies	Policy OID 0.4.0.194112.1.3: qualified certificates issued to legal persons with private key on QSCD Policy OID, 1.3.6.1.4.1.52969.1.4, CP URL: https://docs.trustpro.eu/trustpro-cpcps-en.pdf
CRL distribution point	http://ca.trustpro.eu/crls/[CANAME].crl
Authority Information Access	OCSP, http://ca.trustpro.eu/ocsp/
QC Statements	id-etsi-qcs-QcCompliance (OID 0.4.0.1862.1.1); id-etsi-qcs-QcRetentionPeriod (OID 0.4.0.1862.1.3) = 20; id-etsi-qcs-QcSSCD (OID 0.4.0.1862.1.4); id-etsi-qcs-QcPDS (OID 0.4.0.1862.1.5) = https://docs.trustpro.eu/trustpro-pds-en.pdf, “en”; id-etsi-qct-eseal 2 (OID 0.4.0.1862.1.6.2)

7.2. Profilo della CRL

7.2.1. Numeri di Versione

L'Autorità di Certificazione emette liste di revoca dei certificati (CRL) in **Versione 2**, in conformità con la specifica RFC 5280 [16].

7.2.2. Estensioni della CRL e delle Voci della CRL

Le liste di revoca emesse dall'Autorità di Certificazione devono includere i seguenti campi:

Versione	2
Identificatore dell'algoritmo di firma	sha256With RSA Encryption
Firma	Issued by TrustPro QTSP Qualified CA private key
Emittente	L'identificatore univoco dell'unità di certificazione emittente della lista di revoca.
Attuale aggiornamento	la data di entrata in vigore della lista di revoca. Il valore è espresso in base al fuso orario **UTC** (Tempo Coordinato Universale) con codifica secondo la **RFC 5280 [16]**. Nel caso delle liste di revoca emesse dall'Autorità di Certificazione, questo valore coincide con l'orario di emissione.

Prossimo Aggiornamento	L'ora di emissione della prossima lista di revoca (vedi Sezione 4.10.). Il valore è espresso in base al fuso orario **UTC** (Tempo Coordinato Universale) con codifica secondo la **RFC 5280 [16]**.
Certificati revocati	La lista dei certificati sospesi o revocati con il numero di serie del certificato e con l'orario di sospensione o revoca.
Numero CRL	non-critico, in questo campo sono indicati i numeri di serie consecutivi delle liste di revoca.

7.3. Profilo OCSP

Il **Fornitore** gestisce un servizio di controllo dello stato dei certificati online in conformità con lo standard **RFC 6960 [20]**. La risposta OCSP è firmata dalla chiave privata della CA **TrustPro QTSP**.

7.3.1. Numeri di Versione

Il **Fornitore** supporta le richieste e le risposte per lo stato dei certificati online conformi alla **Versione 1**, secondo gli standard **RFC 6960 [20]**.

7.3.2. Estensioni OCSP

Il **Fornitore** può includere facoltativamente la seguente estensione OCSP:

- **ArchiveCutoff** - non critical

L'Autorità di Certificazione può indicare, con una notazione standard conforme alla specifica **RFC 6960 [20]**, di conservare le informazioni di revoca anche dopo la scadenza del certificato.
Il **Fornitore** può includere la seguente estensione di registrazione OCSP:

- **Reason Code** (Codice Motivo) - non critica - con il motivo della revoca.

Nel caso di certificati sospesi, questo campo è obbligatorio e il suo valore deve essere: "**certificateHold**" **(6)**

8. Audit di Conformità e Altre Valutazioni

L'operato del **Fornitore** è supervisionato da un'**Autorità Nazionale** in linea con le normative dell'Unione Europea. L'Autorità Nazionale può condurre ispezioni in loco presso la sede del Fornitore. Prima dell'ispezione in loco, il Fornitore fa sottoporre le proprie operazioni a una verifica da parte di un **revisore esterno** e invia il rapporto dettagliato della verifica all'Autorità Nazionale entro 3 giorni dalla sua ricezione. La verifica accerta se l'operato del Fornitore rispetta i requisiti del Regolamento eIDAS [1] e della relativa legislazione nazionale.

8.1. Frequenza o Circostanze della Valutazione

Il **Fornitore** fa eseguire una valutazione di conformità annuale sul sistema informatico che eroga i servizi

8.2. Identità/Qualifiche del Valutatore

Il **Fornitore** esegue gli audit interni con l'aiuto di dipendenti e collaboratori con il ruolo di **revisore di sistema indipendente**.
La valutazione di conformità a eIDAS e ETSI può essere eseguita da un'organizzazione con un mandato di qualifica rilasciato dall'organismo di accreditamento nazionale di uno Stato membro dell'UE.

8.3. Relazione del Valutatore con l'Entità Valutata

L'audit esterno è eseguito da un **organismo di valutazione della conformità (CAB)**, che:

- è indipendente dai proprietari, dalla gestione e dalle operazioni del Fornitore esaminato;
- è indipendente dall'organizzazione esaminata, ovvero né il revisore stesso né i suoi familiari diretti hanno alcun rapporto di lavoro o di affari con il Fornitore;
- la retribuzione non dipende dai risultati delle attività svolte durante l'audit.

8.4. Argomenti Trattati dalla Valutazione

Il **CAB** esegue l'audit esterno per valutare la conformità a questo documento, agli standard europei e agli standard applicabili.

8.5. Azioni Intraprese in Caso di Deficienze

Il **Fornitore** deve rispondere per iscritto ai problemi sollevati dal revisore indipendente, riportando le misure adottate per evitarli in occasione della successiva revisione da parte dell'autorità.

9. Altre Questioni Commerciali e Legali

9.1. Tariffe

Il **Fornitore** pubblica le tariffe e i prezzi sulla propria pagina web e li rende disponibili per la consultazione presso il suo servizio clienti.Il **Fornitore** può modificare unilateralmente il listino prezzi. Il Fornitore pubblica qualsiasi modifica al listino prezzi 30 giorni prima che diventi effettiva. Le modifiche non influiranno sul prezzo dei servizi pagati in anticipo.

9.1.1. Tariffe per l'Emissione o il Rinnovo dei Certificati

Vedere la sezione: 9.1

9.1.2. Tariffe per l'Accesso ai Certificati

Il Fornitore garantisce l'accesso online gratuito al suo Archivio dei Certificati per le Parti Contraenti Affidanti.

9.1.3. Tariffe per l'Accesso alle Informazioni di Revoca o di Stato

Il Fornitore fornisce accesso online gratuito al servizio CRL e OCSP.

9.1.4. Tariffe per Altri Servizi e Politica di Rimborso

Vedere la sezione: 9.1.

9.2. Responsabilità Finanziaria

Il **Fornitore** ha stipulato un'assicurazione adeguata per coprire i rischi dell'attività ed eventuali danni derivanti dal servizio di certificazione.

9.3. Riservatezza delle Informazioni Commerciali

Il **Fornitore** gestisce i dati dei clienti in conformità con le normative legali. Il Fornitore dispone di un regolamento sul trattamento dei dati (vedi sezione 9.4), che disciplina in particolare il trattamento dei dati personali.

9.3.1. Ambito delle Informazioni Riservate

Il **Fornitore** tratta come riservate:

- tutti i dati del Cliente, con l'eccezione di quelli che non sono considerati riservati nella sezione 9.3.2;
- oltre ai dati del Cliente:
    - chiavi private e codici di attivazione,
    - richieste di certificato e contratti di servizio,
    - dati relativi alle transazioni e dati di log,
    - regolamenti non pubblici,
    - tutti i dati la cui divulgazione pubblica avrebbe un effetto negativo sulla sicurezza del servizio.

9.3.2. Informazioni non Rientranti nell'Ambito delle Informazioni Riservate

Il **Fornitore** considera pubblici tutti i dati che possono essere ottenuti da una fonte pubblica, o alla

cui divulgazione il Sottoscrittore ha dato il proprio consenso scritto in anticipo.

9.3.3. Responsabilità di Proteggere le Informazioni Riservate

Il **Fornitore** è responsabile della protezione dei dati riservati che gestisce.
Il **Fornitore** obbliga i propri dipendenti, subappaltatori e partner affiliati a proteggere tutti i dati riservati tramite la firma di dichiarazioni di riservatezza o tramite contratto.

9.4. Riservatezza delle Informazioni Personali

Il **Fornitore** si occupa della protezione dei dati personali che gestisce; l'operato e i regolamenti del Fornitore sono conformi ai requisiti della legislazione applicabile.
Il **Fornitore** conserva, anche dopo la scadenza dell'obbligo di conservazione, i dati personali registrati e le informazioni sul Cliente in conformità con i requisiti legali.

9.4.1. Piano per la Riservatezza

Il **Fornitore** dispone di una **Informativa sulla Privacy** per il trattamento dei dati che contiene requisiti dettagliati per la gestione dei dati personali. L'Informativa sulla Privacy per il trattamento dei dati è pubblicata sulla pagina web dell'Autorità di Certificazione **TrustPro QTSP Ltd** al seguente URL:https://docs.trustpro.eu

9.4.2. Informazioni Trattate come Private

Il **Fornitore** protegge tutti i dati personali relativi all'interessato o che contengono conclusioni sull'interessato che non sono accessibili pubblicamente dal Certificato o da altre fonti di dati pubbliche.

9.4.3. Informazioni non Ritenute Private

Il **Fornitore** può divulgare i dati dei Soggetti indicati nel Certificato in base al consenso scritto del Soggetto. Il Fornitore può indicare nel Certificato l'identificatore univoco del fornitore assegnato al Soggetto.

9.4.4. Responsabilità di Proteggere le Informazioni Private

Il **Fornitore** archivia in modo sicuro e protegge i dati personali relativi all'emissione del Certificato che non sono indicati nel Certificato.

9.4.5. Notifica e Consenso all'Uso di Informazioni Private

Il **Fornitore** divulga i dati personali indicati nei Certificati solo con il consenso scritto del Cliente.

9.4.6. Divulgazione a Seguito di Procedimento Giudiziario o Amministrativo

Nei casi definiti dall'Autorità, il **Fornitore** può divulgare i dati personali archiviati relativi al Cliente senza notificarlo.

9.4.7. Altre Circostanze di Divulgazione delle Informazioni

Nessuna disposizione.

9.5. Diritti di Proprietà Intellettuale

Durante la sua attività commerciale, il **Fornitore** non deve ledere alcun diritto di proprietà intellettuale di terzi.
Il presente documento è di proprietà esclusiva del **Fornitore**. I Clienti, i Soggetti e le altre Parti Contraenti Affidanti hanno il diritto di utilizzare il documento solo in conformità con i requisiti della presente Dichiarazione di Prassi di Certificazione; qualsiasi altro uso per scopi commerciali o di altro tipo è rigorosamente vietato.

9.6. Dichiarazioni e Garanzie

Per i dettagli sulle garanzie e le responsabilità verso ciascun soggetto, fare riferimento all'accordo contrattuale tra CA, RA, richiedenti e soggetti.

9.7. Limitazioni della Garanzia

Fare riferimento alla Dichiarazione Informativa PKI (PKI Disclosure Statement) all'indirizzo: https://docs.trustpro.eu/trustpro-pds-en.pdf

9.8. Limitazioni di Responsabilità

Fare riferimento alla Dichiarazione Informativa PKI (PKI Disclosure Statement)all'indirizzo:https://docs.trustpro.eu/trustpro-pds-en.pdf

9.9. Indennizzi

Fare riferimento alla Dichiarazione Informativa PKI (PKI Disclosure Statement) all'indirizzo: https://docs.trustpro.eu/trustpro-pds-en.pdf

9.10. Durata e Recesso

Fare riferimento alla Dichiarazione Informativa PKI (PKI Disclosure Statement) all'indirizzo: https://docs.trustpro.eu/trustpro-pds-en.pdf

9.11. Comunicazioni Individuali con i Partecipanti

Fare riferimento alla Dichiarazione Informativa PKI (PKI Disclosure Statement) all'indirizzo: https://docs.trustpro.eu/trustpro-pds-en.pdf

9.12. Modifiche

Il **Fornitore** si riserva il diritto di modificare il presente documento in modo controllato in caso di cambiamenti nelle norme, nei requisiti di sicurezza, nelle condizioni di mercato o in altre circostanze.

9.13. Disposizioni per la Risoluzione delle Controversie

Fare riferimento alla Dichiarazione Informativa PKI (PKI Disclosure Statement) all'indirizzo: https://docs.trustpro.eu/trustpro-pds-en.pdf

9.14. Legge Applicabile

Fare riferimento alla Dichiarazione Informativa PKI (PKI Disclosure Statement) all'indirizzo: https://docs.trustpro.eu/trustpro-pds-en.pdf

9.15. Conformità con la Legge Applicabile

Fare riferimento alla Dichiarazione Informativa PKI (PKI Disclosure Statement) all'indirizzo: https://docs.trustpro.eu/trustpro-pds-en.pdf

9.16.Disposizioni Varie

9.16.1. Nullità parziale

Qualora alcune delle disposizioni del presente documento dovessero diventare invalide per qualsiasi motivo, le restanti disposizioni rimarranno in vigore senza modifiche.

9.16.2. Applicazione

Il **Fornitore** ha il diritto di richiedere il risarcimento dei danni e delle spese legali per il rimborso dei danni, delle perdite e delle spese causati dai suoi partner. Se in un caso particolare il Fornitore non esercita il proprio diritto al risarcimento, ciò non significa che in casi simili in futuro o in caso di violazione di altre disposizioni del presente documento rinuncerà all'applicazione delle richieste di risarcimento danni.

9.16.3. Forza Maggiore

Il **Fornitore** non è responsabile per l'esecuzione difettosa o ritardata dei requisiti stabiliti in questo documento se la causa del fallimento o del ritardo è una condizione che esula dal controllo del Fornitore.

Fonti:

Num.	Fonti
[1]	Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, sull'identificazione elettronica e i servizi fiduciari per le transazioni elettroniche nel mercato interno.
[2]	**ETSI EN 319 411-1** Firme elettroniche e infrastrutture (ESI); Requisiti di politica e di sicurezza per i fornitori di servizi fiduciari che emettono certificati; Parte 1: Requisiti generali.
[3]	**ETSI EN 319 411-2** Firme elettroniche e infrastrutture (ESI); Requisiti di politica e di sicurezza per i fornitori di servizi fiduciari che emettono certificati; Parte 2: Requisiti per i fornitori di servizi fiduciari che emettono certificati qualificati dell'UE.
[4]	**ETSI EN 319 412-1** Firme elettroniche e infrastrutture (ESI); Profili di certificato; Parte 1: Panoramica e strutture di dati comuni.
[5]	**ETSI EN 319 412-2** Firme elettroniche e infrastrutture (ESI); Profili di certificato; Parte 2: Profilo di certificato per i certificati emessi a persone fisiche.
[6]	**ETSI EN 319 412-3** Firme elettroniche e infrastrutture (ESI); Profili di certificato; Parte 3: Profilo di certificato per i certificati emessi a persone giuridiche.
[7]	**ETSI EN 319 412-5** Firme elettroniche e infrastrutture (ESI); Profili di certificato; Parte 5: Dichiarazioni QC.
[8]	**ETSI TS 119 312** Firme elettroniche e infrastrutture (ESI); Suite crittografiche.
[9]	**ISO/IEC 19790** Tecnologia dell'informazione -- Tecniche per la sicurezza -- Requisiti di sicurezza per i moduli crittografici.
[10]	**FIPS 140-2** Requisiti di sicurezza per i moduli crittografici.

[11]	**CEN 14167-2** Modulo Crittografico per Operazioni di Firma CSP con Backup — Profilo di Protezione
[12]	**ISO/IEC 15408** Tecnologia dell'informazione -- Tecniche per la sicurezza -- Criteri di valutazione per la sicurezza informatica
[13]	**RFC 3647** Internet X.509 Infrastruttura a Chiave Pubblica - Framework per le Politiche dei Certificati e le Prassi di Certificazione.
[14]	**ISO 27001** Tecnologia dell'informazione -- Tecniche per la sicurezza -- Sistemi di gestione per la sicurezza delle informazioni -- Requisiti.
[15]	**ITU X.509 V3** Tecnologia dell'informazione - Interconnessione di sistemi aperti - L'elenco: Quadri per i certificati a chiave pubblica e di attributo.
[16]	**RFC 5280** Internet X.509 Infrastruttura a Chiave Pubblica - Profilo del Certificato e della Lista di Revoca dei Certificati (CRL).
[17]	**RFC 6818** Aggiornamenti al Profilo del Certificato e della Lista di Revoca dei Certificati (CRL) dell'Infrastruttura a Chiave Pubblica Internet X.509.
[18]	**RFC 3739 Internet X.509** Infrastruttura a Chiave Pubblica: Profilo dei Certificati Qualificati.
[19]	**RFC 2560 X.509** Infrastruttura a Chiave Pubblica Internet - Protocollo per lo Stato dei Certificati Online (OCSP).
[20]	**RFC 6960 X.509** Infrastruttura a Chiave Pubblica Internet - Protocollo per lo Stato dei Certificati Online (OCSP).