Trust Italia S.p.A. Certification Practice Statement

(Pratiche di Certificazione)

Version 3.8

(Questo template corrisponde al VTN CP v2.8.4 e VTN CPS v3.8.5)

Data di entrata in vigore: 24/10/2011

Trust Italia S.p.A.
Via Flaminia, 497
00191 Roma
Tel.: +39.06 332287
Fax: +39.06 3336145
www.trustitalia.it

Trust Italia S.p.A. Certification Practices Statement

Data di pubblicazione:_____

Importante - Avviso di Acquisizione

Il 9 agosto 2010, Symantec Corporation ha completato l'acquisizione della Divisione Autenticazioni di VeriSign Inc.
Di conseguenza Symantec è ora registrata come proprietaria del presente documento *Certificate Practices Statement* (Pratiche di Certificazione) e dei servizi PKI di seguito descritti.
Tuttavia emergeranno in questo documento riferimenti misti "VeriSign" e "Symantec" per praticità operativa durante il lasso di tempo necessario a completare il re-branding delle Certification Authoritiy e dei servizi.
Ogni riferimento a VeriSign come entità giuridica deve essere strettamente considerato un retaggio linguistico che riflette esclusivamente la storia della proprietà.
Symantec può continuare ad usare il marchio "VeriSign".

Informazioni Relative ai Brand Commerciali

Pratiche ed Affari Esterni Trust Italia S.p.A.,
Via Flaminia 497 – 00191 Roma - ITALIA
Att: Sviluppo Pratiche.
Tel: +39. 06 332287
Fax: +39. 06 3336145
E-mail: supporto@trustitalia.it

1. INTRODUZIONE

Si invita a fare riferimento alla comunicazione *Avviso di Acquisizione* (pag. 2) per mettere in relazione le informazioni sulle denominazioni e le proprietà riferite nel presente documento

Questo documento è il Certification Practice Statement ("CPS") di Trust Italia S.p.A.. Il documento specifica le procedure seguite dalle autorità di certificazione ("CA") di Trust Italia S.p.A. per la fornitura di servizi di certificazione, ivi inclusi rilascio, gestione, revoca e rinnovo di certificati in conformità ai requisiti specifici della Policy di Certificazione ("CP") di VeriSign Trust Network.

Il CP è la principale dichiarazione normativa che disciplina il VTN e stabilisce i requisiti commerciali, legali e tecnici per l'approvazione, il rilascio, la gestione, l'utilizzo, la revoca ed il rinnovo di Certificati digitali all'interno del VTN e per la fornitura dei servizi di sicurezza associati. Questi requisiti, denominati "Standard VTN" proteggono la sicurezza e l'integrità del VTN, si applicano a tutti i Partecipanti al VTN e di conseguenza garantiscono uno standard di sicurezza uniforme in tutto il VTN. Ulteriori informazioni sul VTN e sugli Standard VTN sono disponibili nel CP.

Trust Italia S.p.A. ha l'autorità su una porzione del VTN definita "Sottodominio" del VTN. Il Sottodominio di Trust Italia S.p.A. è rappresentato dalla porzione del VTN posta sotto il suo controllo. Il Sottodominio di un Affiliato include tutte le entità ad esso subordinate, quali Clienti, Abbonati e Parti Facenti Affidamento.

Mentre il CP stabilisce i requisiti a cui i Partecipanti al VTN si devono attenere, il CPS descrive come Trust Italia S.p.A. soddisfa tali requisiti nell'ambito del Sottodominio del VTN di competenza di Trust Italia S.p.A.. Più specificamente, tale CPS descrive le procedure seguite da Trust Italia S.p.A. per:

- gestire l'infrastruttura essenziale che supporta il VTN in maniera sicura; e
- rilasciare, gestire, revocare e rinnovare Certificati VTN

nell'ambito del Sottodominio del VTN di Trust Italia S.p.A., in conformità ai requisiti del CP ed ai suoi Standard VTN.

Il presente CPS è conforme alla Internet Engineering Task Force (IETF) RFC 3.647 per la costruzione dei dati relativi al *Certificate Policy* e *Certification Practice Statement* .

1.1 *Panoramica*

Service Center:

Trust Italia S.p.A. è un *Service Center* come descritto nel CP § 1.1.2.1.2 , ciò significa che Trust Italia S.p.A. può approvare o respingere le richieste di certificazione nel caso di Certificati retail o, nel caso di Certificati per aziende e Enti (*Enterprise Customers*), fornire agli Enterprise Customers tramite Processing Center i servizi di back-end del ciclo di vita del Certificato. Gli Affiliati Service Center che forniscono certificati Client (*Client Service Centers*) diventano CA nell'ambito del VTN ma esternalizzano le funzioni di back-end a Symantec o ad un altro Processing Center. Comunque, quando si forniscono i Certificati Server, i Service Center diventano RA nell'ambito del VTN per l' emissione dei certificati per server della CA VeriSign ®. Questi Service Center (Centri di servizio) svolgono funzione di validazione per approvare o respingere le domande di certificazione per i Secure Server ID o i Global Server ID. I Service Center possono anche fornire le Managed PKI per i loro Enterprise Customer (clienti aziendali). Questi Clienti Managed PKI accedono alla Managed PKI con un accordo stipulato con il Service Center, il quale tramite il suo contratto con Trust Italia S.p.A. o un altro Processing Center, fa in modo che il Processing Center fornisca ai Clienti Managed PKI i servizi di back-end del ciclo di vita del certificato.

Processing Center:Trust Italia S.p.A. è un *Processing Center* come descritto nel CP § 1.1.2.1.2, ciò significa che Trust Italia S.p.A. ha istituito un sicuro impianto di alloggiamento, tra le altre cose, i sistemi di CA, tra cui i moduli crittografici su cui risiedono le chiavi private utilizzate per l'emissione di Certificati.

Trsut Italia Spa agisce come una CA nel VTN e svolge tutti i servizi del ciclo di vita del certificato, emissione, gestione, revoca e rinnovo dei Certificati. Ciò inoltre prevede la gestione chiave delle CA e dei servizi del ciclo di vita del certificato per conto dei propri clienti aziendali o dei clienti Enterprise dei Service Center subordinati a Trust Italia S.p.A.. Trust Italia S.p.A. offre anche Certificati in tutte e tre le linee business[1], Consumer (Certificati Client Classe 1 e 2 Retail), Web Site (Secure Server ID e Global Server ID) ed Enterprise (tramite i servizi Managed PKI). Le pratiche relative ai servizi forniti da Trust Italia S.p.A. o da Symantec ai propri Affiliati sono oltre l'ambito di questo CPS.

Il presente CPS si applica specificamente a:

- Le *Public Primary Certification Authorities* di Symantec ("PCA")
- Le CA Infrastrutturali di Trust Italia S.p.A. e le CA Amministrative di Trust Italia S.p.A. che supportano il VeriSign® Trust Network.
- Le CA Pubbliche di Trust Italia S.p.A. e le CA di Clienti Managed PKI, che rilasciano Certificati nell'ambito del Sottodominio di Trust Italia S.p.A. del VTN.

Più in generale, il CPS disciplina inoltre l'utilizzo dei servizi VTN nell'ambito del Sottodominio del VTN di Trust Italia S.p.A. da parte di tutte le persone fisiche e le entità all'interno del Sottodominio di Trust Italia S.p.A. (qui di seguito, collettivamente, i "Partecipanti al Sottodominio di Trust Italia S.p.A."). Le CA private e le gerarchie gestite da Trust Italia S.p.A. sono fuori dall'ambito del presente CPS.

Il VTN include quattro classi di Certificati, Classi 1-4. Il CP è un documento singolo che definisce le policy per certificati, una per ogni Classe e stabilisce lo Standard VTN per ogni Classe.

Trust Italia S.p.A. offre ognuna delle tre Classi di Certificati nell'ambito del proprio Sottodominio del VTN. Il CPS descrive come Trust Italia S.p.A. soddisfa i requisiti del CP per ogni Classe nell'ambito del proprio Sottodominio. Ciò significa che il CPS – come documento singolo – copre le pratiche e procedure riguardanti il rilascio e la gestione di tutte e tre le Classi di Certificati.

Trust Italia S.p.A. può pubblicare Pratiche di Certificazione complementari a questo CPS per soddisfare specifici requisiti governativi o altri standard industriali ed esigenze particolari.

Queste procedure supplementari di certificazione sono a disposizione degli utenti per i certificati rilasciati nel quadro delle linee guida supplementari e le relative parti coinvolte.

Il CPS è soltanto uno di una serie di documenti relativi al sottodominio del VTN di Trust Italia S.p.A..
Tali documenti includono:

Documenti2 accessori e confidenziali sulla sicurezza che integrano il CP e CPS prevedendo requisiti più dettagliati, quali:

- Il Symantec Phisical Security Policy, che enuncia i principi che disciplinano la sicurezza delle infrastrutture VTN,
- Il Symantec Security and Audit Requirements Guide (SAR), che descrive i requisiti dettagliati per Symantec e affiliati in materia di personale, fisica, telecomunicazioni, logica e gestione della chiave di sicurezza crittografica e
- Il Key Ceremony Guide di riferimento che presenta i requisiti dettagliati per la gestione delle chiavi operative.

• Accordi accessori imposti da Trust Italia S.p.A.. Questi accordi legano Clienti, Abbonati e Relative Parti di Trust Italia S.p.A.. Tra le altre cose, gli accordi rientrano negli Standard VTN per questi partecipanti VTN e in alcuni casi, elencano specifiche pratiche per il modo in cui devono soddisfare gli Standard VTN.

---

[1] I certificati relativi alle linee di business Web Site e Enterprise possono essere fornite anche tramite l'attività diretta di Symantec

[2] Anche se questi documenti non sono accessibili al pubblico le loro specifiche sono incluse nel Annual WebTrust di VeriSign per l'audit delle Certification Autority e possono essere messi a disposizione dei clienti previo accordo speciale

In molti casi, il CPS si riferisce a questi documenti accessori per pratiche specifiche e dettagliate sulle implementazioni agli Standard VTN dove anche le specifiche del CPS potrebbe compromettere la sicurezza del Sottodominio del VTN di Trust Italia S.p.A..

1.2 Nome del Documento ed Identificazione

Il presente documento è il *Certification Practice Statement* (Pratiche di Certificazione) di Trust Italia S.p.A.. I Certificati VTN contengono dei valori identificativi di oggetto corrispondenti alla Classe di Certificati VTN applicabile. Di conseguenza, Trust Italia S.p.A. non ha attribuito al presente CPS un valore identificativo di oggetto. Gli Identificatori di Oggetto relativi alla Policy di Certificazione vengono utilizzati in conformità alla Sezione 7.1.6.

1.3 Partecipanti al PKI

1.3.1 Le Certification Authority (Autorità di Certificazione)

Certification Authority (CA) è un termine di natura generale che include tutte le entità che rilasciano Certificati nell'ambito del VTN. Il termine "CA" racchiude una subcategoria di varie entità per il rilascio che si chiamano *Primary Certification Authorities*, Autorità Primarie di Certificazione (PCA). Le PCA funzionano da root per quattro domini[3], una per ogni classe di Certificati. Ogni PCA è una entità Symantec. Sotto alle PCA si trovano le Autorità di Certificazione che rilasciano Certificati di Abbonamento per utenti finali o ad altre CA.

Symantec gestisce anche la "VeriSign® Universal Root Certification Authority" e la "VeriSign® ECC Universal Root Certification Authority". Le Universal Root della CA non sono definite in una classe particolare del certificato e possono emettere qualsiasi classe di CA Subordinata.

I clienti aziendali Trust Italia S.p.A. possono attivare le proprie CA in qualità di CA subordinate ad un PCA di Trust Italia S.p.A.. Tali clienti entrano in un rapporto contrattuale con Trust Italia S.p.A. nel rispetto di tutti i requisiti del VTN CP e del CPS di Trust Italia S.p.A.. Queste CA subordinate possono tuttavia attuare una prassi più restrittiva in base a loro esigenze interne.

Una VTN CA tecnicamente fuori dalle tre gerarchie in ciascuna delle PCA è la *Secure Server Certification Authority*. Questa CA non ha un CA superiore, come una root o una PCA.
Piuttosto, la Secure Server CA agisce come sua propria root e si è rilasciata un certificato root auto-firmato.
La *Secure Server Certification Authority* si rilascia inoltre certificati per Abbonati utenti finali. Così, la gerarchia Secure Server è costituita solo dalla Secure Server CA.
La Secure Server CA rilascia Secure Server ID, che sono considerati Certificati Organizzativi di Classe 3.

La Secure Server CA utilizza pratiche ciclo di vita che sono sostanzialmente simili a quelle delle altre CA di Classe 3 nell'ambito del VTN. Così, Symantec ha approvato e designato la Secure Server Certification Authority come una CA di Classe 3 all'interno del VTN. I certificati che emette sono considerati affidabili e forniscono garanzie al pari di altri Certificati Organizzativi di Classe 3.

1.3.2 Registration Authority (Autorità di Registrazione)

La Registration Authority (RA) è un entità che svolge funzioni front-end riguardo la conferma d' identità, approvazione o rifiuto di Richieste di Certificati, richiesta di revoca di Certificati, nonché approvazione o rifiuto di richieste di rinnovo per conto della CA VTN. Trust Italia S.p.A. può svolgere funzione di CA per certificati che emette.

Le terze parti che entrano in un rapporto contrattuale con Trust Italia S.p.A., possono operare con proprie RA e autorizzare il rilascio di certificati da una CA Trust Italia S.p.A.. Le RA di terze parti devono rispettare tutti i requisiti del CP VTN, del CPS Trust Italia S.p.A. ed i termini dei loro servizi aziendali con Trust Italia S.p.A.. Tuttavia le RA possono implementare procedure più restrittive in base alle loro esigenze interne[4].

---

[3] Attualmente i certificati di Classe 4 non vengono emessi dal VTN

[4] Un esempio di RA terza parte è un cliente dei servizi Managed PKI

1.3.3 Abbonati

Gli abbonati nell'ambito del VTN includono tutti gli utenti finali (comprese le persone giuridiche) dei certificati rilasciati da una CA VTN. L'abbonato è il soggetto nominato come Abbonato utente finale di un certificato. Abbonati utenti finali possono essere individui, organizzazioni o, componenti infrastrutturali, quali firewall, router, server attendibili o altri strumenti utilizzati per proteggere le comunicazioni all'interno di un'Organizzazione.

In alcuni casi i certificati sono rilasciati direttamente a persone fisiche o giuridiche per il loro proprio utilizzo. Tuttavia esistono comunemente altre situazioni in cui la parte che richiede un certificato è diversa dal soggetto a cui si applica la credenziale. Ad esempio, un'organizzazione può richiedere i certificati per i propri dipendenti per permettere loro di rappresentare l'organizzazione nelle transazioni elettroniche/ di business. In tali situazioni il soggetto abbonato per il rilascio di certificati (ad es. effettuando il pagamento per loro o tramite l'iscrizione ad un servizio specifico, o in qualità essa stessa di emittente) è diverso dal soggetto del certificato (in generale, il titolare della credenziale). Due termini diversi sono usati nel presente CPS per distinguere i seguenti due ruoli: "Abbonato", è l'entità che contratta con Trust Italia S.p.A. per il rilascio delle credenziali e, "Soggetto", cioè la persona a cui la credenziale è associata. L'abbonato ha la responsabilità finale per l'utilizzo delle credenziali, ma il soggetto è l'individuo che viene autenticato quando la credenziale viene presentata.

Quando il termine "Oggetto" viene usato è per indicare una distinzione con l' abbonato. Quando "Abbonato" viene usato può significare solo l'abbonato come entità distinta, ma possono anche essere utilizzato il termine per abbracciare i due. Il contesto del suo utilizzo in questo CPS evocherà la corretta comprensione.

Le CA sono tecnicamente anche gli abbonati dei certificati nell'ambito del VTN, sia nel caso che una PCA si rilasci di un Certificato auto firmato, che venga rilasciato alla CA un certificato da una CA superiore. Tuttavia i riferimenti a "fine entità" e "abbonati" in questo CPS, si applicano solo all'abbonato utente finale.

1.3.4 Parti Facenti Affidamento

Una Parte Facente Affidamento è una persona o entità che agisce in virtù di un certificato e / o una firma digitale rilasciati nell'ambito della VTN. Una Parte Facente Affidamento può o meno essere anche un Abbonato all'interno del VTN.

1.3.5 Altri Partecipanti

Non applicabile

1.4 Applicazioni del Certificato

1.4.1 Applicazioni Adeguate del Certificato

Certificati Rilasciatati a Persone

I Certificati individuali sono normalmente utilizzati dalle persone per firmare e crittografare la posta elettronica e per l'autenticazione ad applicazioni (client authentication). Mentre gli utilizzi più comuni per i singoli certificati sono inclusi nella tabella 1, il certificato individuale può essere utilizzato per altri scopi, a condizione che la Parte Facente Affidamento possa ragionevolmente fare affidamento sul certificato e che l'uso non sia altresì proibito dalla legge, dal VTN CP, dal CPS in base al quale il certificato sia stato rilasciato e dagli accordi con gli abbonati.

Classe di Certificazione	Livello di Sicurezza			Utilizzo		
	Basso	Medio	Alto	Firma	Crittografia	Autenticazione Client
Classe 1	✓			✓	✓	✓
Classe 2		✓		✓	✓	✓
Classe 3			✓	✓	✓	✓

Tabella 1. Utilizzo del Certificato Individuale

Certificati Rilasciati ad Organizzazioni

I Certificati Organizzativi sono rilasciati alle organizzazioni dopo aver accertato che l'organizzazione esista legalmente e che altre attribuzioni all' organizzazione incluse nel certificato (ad esclusione di informazioni non verificate sugli abbonati) siano autenticate ad esempio la proprietà di un dominio Internet o e-mail. Non è nell'intento di questo CPS limitare i tipi di uso per i certificati organizzativi. Mentre gli usi più comuni sono inclusi nella tabella 2, il certificato organizzativo può essere utilizzato per altri scopi, a condizione che la Parte Facente Affidamento possa ragionevolmente fare affidamento sul certificato e che l'uso non sia altresì proibito dalla legge, dal VTN CP, dal CPS in base al quale il certificato sia stato rilasciato e dagli accordi con gli abbonati.

Classe di Certificazione	Livello di Sicurezza		Utilizzo			
	Alto	Medio	Code/Content Signing	Secure SSL/ TLS-sessions	Autenticazione	Firma e Crittografia
Classe 3	✓		✓	✓	✓	✓

Tabella 2. Utilizzo del Certificato Organizzativo[5]

Livelli di Sicurezza

Certificati a basso livello di sicurezza sono quei certificati che non dovrebbero essere utilizzati per l'autenticazione o per sostenere il non-ripudio. La firma digitale fornisce modeste garanzie che l'e-mail provenga da un mittente con un determinato indirizzo e-mail. Il certificato, tuttavia, non fornisce alcuna prova dell' identità dell' abbonato. L'uso della crittografia permette ad una Parte Facente Affidamento di utilizzare il certificato per crittografare i messaggi all'abbonato, anche se il la Parte facente affidamento non avrà la certezza che il destinatario sia in realtà la persona indicata nel Certificato.

Certificati con livello medio di sicurezza sono certificati che siano idonei a garantire alcune email inter/ intra-organizzative, commerciali, e personali che richiedono un livello medio di garanzia dell'identità dell'abbonato, in relazione al Classe 1 e 3.

Certificati ad alto livello di sicurezza sono certificati individuali e organizzativi di Classe 3 che assicurano un livello elevato di certezza circa l'identità dell' abbonato a differenza del Classe 1 e 2.

1.4.2 Applicazioni vietate del Certificato

I certificati sono utilizzati solo nella misura in cui l'uso sia conforme alla normativa vigente ed in particolare

[5] "In circostanze limitate i certificati di Classe 2 possono essere rilasciati da un cliente Managed PKI ad una organizzazione affiliata (e non un individuo all'interno dell'organizzazione). Tale certificato può essere utilizzato soltanto per l'autenticazione dell' organizzazione e per la firma. Salvo quanto espressamente autorizzato da Symantec attraverso un Enterprise Service Agreement che impone l'autenticazione e i requisiti delle pratiche coerenti con le norme di sicurezza di questo CPS, agli Abbonati è proibito utilizzare questo certificato per la firma del codice e dei contenuti, per la crittografia SSL e firma S /Mime e quest'utilizzo della chiave verrà disattivato per questi certificati ".

deve essere utilizzato solo nella misura consentita dalle leggi applicabili all'esportazione o all'importazione.

I Certificati Symantec e Trust Italia S.p.A. non sono progettati, destinati o autorizzati per essere utilizzati o rivenduti come
attrezzature di controllo in circostanze rischiose o per usi che richiedono un funzionamento fail-safe (come ad esempio il funzionamento di strutture per l'energia nucleare, la navigazione aerea o i sistemi di comunicazione, i sistemi per il controllo del traffico aereo o per il controllo di armi, la cui avaria potrebbe avere come effetto diretto la morte o il ferimento di persone o un danno ambientale grave). Inoltre, i Certificati di Classe 1 non dovranno essere utilizzati come prova di identità o a sostegno del non-ripudio di un'identità o autorità. I certificati client sono destinati ad applicazioni client e non devono essere utilizzati come Certificati server o organizzativi.

Certificati CA non possono essere utilizzati per le funzioni ad eccezione di funzioni di CA.
Inoltre, Certificati di Abbonamento degli utenti finali non devono essere utilizzati come certificati CA.

Symantec e Trust Italia S.p.A. rinnovano periodicamente i certificati delle CA intermedie. Applicazioni di terze parti o piattaforme che hanno una certificazione intermedia incorporata come un certificato di origine non possono funzionare come previsto dopo che la certificazione intermedia è stata aggiornata. Trust Italia S.p.A. quindi non garantisce l'uso di CA intermedie come certificati di origine e raccomanda che le CA Intermedie non siano integrate nelle applicazioni e/o piattaforme, come i certificati di origine. Trust Italia S.p.A. raccomanda l'utilizzo di PCA radici come i certificati di origine.

1.5 Amministrazione dei Criteri

1.5.1 Organizzazione Amministrativa del Documento

Trust Italia S.p.A.
Via Flaminia, 497
00191 Roma ITALY
All'attenzione di: Pratiche di Sviluppo - CPS
Tel. +39 06 332287
Fax +39 06 3336145

1.5.2 Persona di Contatto

Il Certificato di Policy Manager VeriSign Trust Network Policy Autorità di Gestione
c / o Trust Italia S.p.A.
Via Flaminia, 497
00191 Roma ITALY
All'attenzione di: Pratiche di Sviluppo - CPS
Tel. +39 06 332287
Fax +39 06 3336145
info@trustitalia.it

1.5.3 Persona che Determina l'Idoneità del CP per la Policy

L'organizzazione indicata alla sezione 1.5.2. è tenuta a stabilire se il presente CPS ed altri documenti relativi alla pratiche di certificazione e che integrano o sono subordinati al presente CPS sono idonei ai sensi del CP e del presente CPS.

1.5.4 Procedura di Approvazione del CPS

L' approvazione del presente CPS e le successive modifiche sono effettuate dal PMA. Le modifiche del CPS devono essere sotto forma di documento contenente un modulo di modifica o un avviso di aggiornamento. Le versioni modificate o gli aggiornamenti devono essere collegati alla sezione Pratiche di Aggiornamento e Avvisi della Repository di Trust Italia S.p.A. posta all'indirizzo:
https://www.trustitalia.it/repository/updates.

Gli aggiornamenti sostituiscono le disposizioni designate o in conflitto di cui si fa riferimento alla versione del CPS.

1.6 Definizioni ed Acronimi

Vedere tabella di acronimi e definizioni dell'appendice A

2. Pubblicazione e Responsabilità della Repository

2.1 Repository

Trust Italia S.p.A. è responsabile per quanto riguarda le funzioni di Repository (archivio) per le proprie CA e per le CA sia dei propri Clienti Managed PKI che per il clienti ASB. Trust Italia S.p.A. pubblicherà i Certificati da loro rilasciati nella Repository in conformità con il CPS § 2.6.

Al momento di revoca di un Certificato di Abbonamento per utente finale, Trust Italia S.p.A. pubblica una comunicazione di tale revoca nella Repository. Trust Italia S.p.A. rilascia CRL per le proprie CA e per le CA di Centri di Servizi e di Clienti Managed PKI all'interno del suo Sotto-dominio ai sensi delle disposizioni di questo CPS. Inoltre, per quei Clienti Managed PKI che hanno fatto richiesta di servizi OCSP (protocollo online sullo stato dei Certificati), Trust Italia S.p.A. fornisce servizi OCSP ai sensi delle disposizioni del presente CPS.

2.2 Pubblicazione di Informazioni sul Certificato

Trust Italia S.p.A. mantiene una repository web-based che permette alle Parti Facenti Affidamento di effettuare domande online per quanto concerne la revoca e altre informazioni sullo stato del certificato. Trust Italia S.p.A. fornisce alle Parti Facenti affidamento le informazioni su come trovare le repository appropriate per controllare lo stato del certificato e, se disponibile l' OCSP (Online Certificate Status Protocol), come trovare il giusto responder del OCSP.

Trust Italia S.p.A. pubblica i certificati emessi per conto delle proprie CA e delle CA dei Client Service Centers nei loro sotto-domini. Dopo la revoca di certificato di un abbonato utente finale, Trust Italia S.p.A. pubblica comunicazione della stessa nella repository. Inoltre Trust Italia S.p.A. pubblica la Certificate Revocation Lists (elenco dei certificati revocati - CRL) e, se disponibili, fornire i servizi OCSP (Online Certificate Status Protocol) per le proprie CA e le CA di Service Center all'interno del proprio sotto-dominio.

Trust Italia S.p.A. in ogni momento può pubblicare una versione corrente di:
- Il presente CP VTN
- il proprio CPS,
- Contratti di Abbonamento,
- Accordo delle Parti Facenti Affidamento

Trust Italia S.p.A. è responsabile delle funzioni di archivio per le CA Infrastrutturali, Amministrative di Trust Italia S.p.A., le CA di Trust Italia S.p.A. e le CA dei Clienti Managed PKI nel sotto-dominio del VTN.

Trust Italia S.p.A. pubblica alcune informazioni sulle CA nella sezione Repository del sito web Trust Italia S.p.A. all'indirizzo http://www.trustitalia.it/repository/ come descritto di seguito.

Trust Italia S.p.A. pubblica il CP del VTN, il presente CPS, i Contratti di Abbonamento ed i Contratti per Parti Facenti Affidamento nella sezione archivi del sito web di Trust Italia S.p.A..

Trust Italia S.p.A. pubblica i certificati secondo quanto indicato nella tabella 3 che segue.

Tipo Certificato	*Condizioni di Pubblicazione*
VTN PCA e CA del VTN che emettono Root di Certificazione VTN	Disponibile per Parti Facenti Affidamento mediante l'inserimento nell'attuale software del browser sia come parte di una catena di certificazione che possa essere ottenuta attraverso il Certificato per abbonato utente finale che attraverso funzioni di query descritte di seguito.
Trust Italia S.p.A. Issuing CA Certificates	Disponibile per Parti Facenti attraverso il Certificato per abbonato utente finale attraverso funzioni di query descritte di seguito.
Certificato della CA di Trust Italia S.p.A. che supporta i Certificati Managed PKI Lite e Certificati CA di Clienti Managed PKI	Accessibili mediante query nel directory server LDAP di Trust Italia S.p.A. all'indirizzo: directory.trustitalia.it.
Certificati Symantec OCSP Responder	Accessibili mediante ricerca nel directory server LDAP di Trust Italia S.p.A. all'indirizzo: directory.trustitalia.it.
Certificati di Abbonamento per utenti finali	Accessibili alle Parti Facenti Affidamento mediante funzioni di query nell'archivio di Trust Italia S.p.A. all'indirizzo: • https://digitalid.trustitalia.it/repository Anche accessibili mediante ricerca nel directory server LDAP di Symantec all'indirizzo • directory.verisign.com
Certificati di Abbonamento per utenti finali rilasciati attraverso Clienti Managed PKI	Messi a disposizione mediante le funzioni di query suindicate, salvo il fatto che – a giudizio del Clienti Managed PKI – il Certificato potrebbe essere accessibile soltanto mediante una ricerca in base al numero di serie del Certificato.

Tabella 3 – Condizioni per la Pubblicazione dei Certificati

2.3 Tempo o Frequenza di Pubblicazione

Gli eventuali aggiornamenti al presente CPS sono resi pubblici in accordo al punto 9.12. Eventuali aggiornamenti ai Contratti di Abbonamento sono pubblicati secondo necessità. I Certificati vengono pubblicati al momento del rilascio, mentre le informazioni sullo stato dei Certificati sono rese pubbliche conformemente alle disposizioni del presente CPS.

2.4 Controlli di Accesso sulle Repository

Le informazioni pubblicate nella sezione archivi del sito web di Trust Italia S.p.A. sono informazioni pubblicamente accessibili. L'accesso "in sola lettura" a tali informazioni non è soggetto ad alcun tipo di limitazione. Trust Italia S.p.A. obbliga le persone, che vogliano avere accesso a Certificati, informazioni sullo stato dei Certificati o CRL, di aderire ad un Contratto per Parte Facente Affidamento. Trust Italia S.p.A. ha attuato misure di sicurezza logiche e fisiche al fine di impedire che persone non autorizzate possano aggiungere, cancellare o modificare dati contenuti nella repository.

3. Identificazione ed Autenticazione

3.1 Nomenclatura

Salvo laddove diversamente indicato nel CP del VTN, questo CPS o il contenuto del certificato digitale, i nomi che figurano nei certificati rilasciati sotto il VTN sono autenticati.

3.1.1 Tipi di Nomi

Mentre il VTN è ora di proprietà di Symantec Corporation (vd. la comunicazione di acquisizione a pag.2) i certificati devono continuare ad essere rilasciati indicando "VeriSign Inc." e "VeriSign Trust Network" durante tutto il tempo necessario al processo di re-branding.

I Certificati CA di Trust Italia S.p.A. contengono dei Nomi Distintivi X.501 nei campi Entità di Rilascio e Soggetto. I Nomi Distintivi delle CA di Trust Italia S.p.A. sono composti dagli elementi indicati nella Tabella 4 che segue.

Attributo	***Valore***
Paese (C) =	"IT" o non utilizzato
Organization (O) =	"VeriSign, Inc." o Trust Italia S.p.A. [6] or <organization name>[7]
Organizational Unit (OU) =	I Certificati delle CA di Trust Italia S.p.A. possono contenere vari attributi OU i quali possono specificare uno o più dei dati seguenti: • Nome della CA • VeriSign Trust Network • Riferimento al Contratto per Parte Facente Affidamento applicabile che disciplina le condizioni di utilizzo del Certificato; e • Informazioni sul copyright.
Stato o Provincia (S) =	Non utilizzato.
Località (L) =	Non utilizzato, ad eccezione della CA Symantec Commercial Software Publishers, che indica "Internet."
Common Name (CN) =	Questo attributo include il nome della CA (qualora non fosse specificato in un attributo OU) o non viene utilizzato.

Tabella 4 - Attributi dei Distinguished Name (Nomi Distintivi) nei Certificati delle CA

I Certificati di Abbonamento per utenti finali contengono dei Nomi Distintivi X.501 nel campo Nome Soggetto e sono composti dagli elementi indicati nella Tabella 9 che segue.

Attributo	***Valore***
Paese (C) =	"IT." o non utilizzato.
Organization (O) =	L'attributo Organizzazione si usa come segue: • "Trust Italia S.p.A.." per il Responder OCSP di Trust Italia S.p.A. e per Certificati individuali. • Nome dell'organizzazione dell'Abbonato per Certificati web server e certificati individuali che non abbiano un'affiliazione con organizzazioni
Organizational Unit (OU) =	I Certificati per Abbonati (utenti finali) di Trust Italia S.p.A. possono contenere vari attributi OU i quali possono specificare uno o più dei dati seguenti: • Nome dell'unità organizzativa dell'Abbonato (per Certificati aziendali) • VeriSign Trust Network • Riferimento al Contratto per Parte Facente Affidamento applicabile che disciplina le condizioni di utilizzo del Certificato • informazioni sul copyright • "Autenticato da Trust Italia S.p.A." e "Membro del VeriSign Trust Network" nei Certificati le cui richieste sono state autenticate da Trust Italia S.p.A. • "Persona non convalidata" per Certificati Individuali di Classe 1 • Testo a descrizione del tipo di Certificato.
Stato/ Provincia (S) =	Indica lo Stato dell'Abbonato (non è un campo richiesto per l'emissione di certificati individuali).
Località (L) =	Indica la località dell'Abbonato (non è un campo richiesto per l'emissione di certificati individuali).
Common Name (CN) =	Questo attributo include:

[6] Un'eccezione a questo è il Secure Server CA, che indica "RSA Data Security, Inc.," ma ora è una CA Symantec.

[7] Per una CA dedicata ad un cliente organizzativo, la componente (o =), dovrà essere la denominazione ufficiale dell'organizzazione.

Attributo	*Valore*
	• Il nome del Responder OCSP (per Certificati Responder OCSP) • Nome dominio (per Certificati web server) • Nome dell'organizzazione (per Certificati a firma di codici/oggetti) • Nome (per Certificati individuali).
E-Mail (E) =	Indirizzo e-mail per Certificati individuali di Classe 1 e più in generale per i certificati MPKI

Tabella 5 - Attributi dei Nomi Distintivi nei Certificati di Abbonamento Utente Finale

La componente Common Name (=CN) del nome distintivo del Soggetto nei Certificati di Abbonamento per utenti finali viene autenticata nel caso di Certificati di Classe 2 e 3.

- Il valore autenticato per il common name inserito nei nomi distintivi del Soggetto all'interno di Certificati aziendali è un nome di dominio (nel caso di ID Secure Server o ID Global server) oppure la denominazione sociale dell'organizzazione o dell'unità all'interno dell'organizzazione.

- Il valore del common name autenticato incluso nel soggetto del nome distintivo di un Certificato Organizzativo ASB di Classe 3, tuttavia, è il nome personale generalmente accettato del rappresentante dell'organizzazione autorizzata ad utilizzare la chiave privata dell'organizzazione, e la componente dell'organizzazione (=O) è la il Nome legale della stessa.

- Il valore per il common name comune inserito come nome distintivo del Soggetto in Certificati individuali rappresenta il nome personale generalmente accettato dell'individuo in questione.

3.1.2 I Nomi Devono Essere Significativi

I Certificati per Abbonati di Classe 2 e 3 per utenti finali contengono nomi con una semantica generalmente comprensibile che consente la determinazione dell'identità dell'individuo o dell'organizzazione che è il Soggetto del Certificato.

I certificati CA di Trust Italia S.p.A. contengono nomi dalla semantica comunemente comprensibili al fine di consentire la determinazione dell' identità della CA che è il Soggetto del Certificato.

3.1.3 Anonimato o Pseudonimia degli Abbonati

L'identità degli abbonati individuali con classe 1 non è autenticata. Gli abbonati Classe 1 possono utilizzare pseudonimi. Salvo quando richiesto per legge o da uno Stato o autorità di governo per proteggere l'identità di determinati abbonati utenti finali (ad esempio, minori, o informazioni sensibili di dipendenti pubblici), agli abbonati con Classe 2 e 3, non è permesso usare pseudonimi (altri nomi diversi dal vero nome personale o dell' organizzazione dell'abbonato). Ogni richiesta di anonimato in un certificato sarà valutata nel merito dal PMA e, se consentito, il certificato indicherà che l'identità è stato autenticata ma rimane protetta.

3.1.4 Norme per l'Interpretazione delle varie Forme di Nomi

Nessuna stipulazione

3.1.5 Unicità dei Nomi

Trust Italia S.p.A. garantisce che i Nomi Distintivi dei Soggetti siano unici (nell'ambito del dominio di una specifica CA) grazie agli elementi automatizzati nel processo di iscrizione degli Abbonati. E' possibile per un Abbonato avere due o più certificati con lo stesso Subject Distinguished Name.

3.1.6 Riconoscimento, Autenticazione e Ruolo dei Marchi

Ai Richiedenti di Certificati è vietato usare nomi nelle loro Richieste di Certificati che violino gli altrui Diritti di Proprietà Intellettuale. Trust Italia S.p.A., tuttavia, non controlla se i Diritti di Proprietà Intellettuale per il nome che appare in una Richiesta di Certificato spettino al Richiedente

del Certificato stesso. Trust Italia S.p.A. inoltre non farà da arbitro e mediatore e non si adopererà per risolvere le eventuali controversie riguardo alla proprietà di nomi di dominio, nomi commerciali, marchi commerciali o di servizi. Trust Italia S.p.A. ha la facoltà, senza alcuna responsabilità verso i Richiedenti dei Certificati, di rifiutare o sospendere qualsiasi Richiesta di Certificato in seguito ad una tale controversia.

3.2 Convalida Iniziale d'Identità

3.2.1 Metodo per comprovare il possesso della Chiave Privata

Il Richiedente il certificato deve dimostrare di possedere legittimamente la chiave privata corrispondente alla chiave pubblica per essere elencato nel Certificato. Il metodo per verificare il possesso di una chiave privata dovrà essere PKCS # 10, un'altra prova crittograficamente equivalente o un altro metodo approvato da Trust Italia S.p.A.. Questa prescrizione non si applica quando una coppia di chiavi è generata da una CA per conto di un abbonato, per esempio laddove su smart card sono collocate le chiavi pre-generate.

3.2.2 Autenticazione dell'identità di un'organizzazione

Ogni volta che un certificato contiene il nome di un'organizzazione, l'identità e altre informazioni dell'organizzazione presentate al momento dell' iscrizione dai richiedenti il certificato (ad eccezione delle Informazioni Abbonati Non Verificate) sono confermate in base alle direttive documentate nelle Procedure di Validazione stabilite da Trust Italia S.p.A. e/o Symantec.

Come minimo Trust Italia S.p.A. e/o Symantec dovrà:

- Verificare che la relativa organizzazione esista mediante il coinvolgimento di almeno un servizio o database di comprova dell'identità di terzi o, in alternativa, di documentazione ufficiale presentata all'ente governativo competente la quale conferma l'esistenza dell'organizzazione in questione; e
- Confermare - tramite un idoneo referente aziendale via telefono, posta o procedura paragonabile – determinate informazioni sull'organizzazione stessa, che l'organizzazione abbia autorizzato la Richiesta di Certificato e che la persona che presente la Richiesta di Certificato per conto dell'organizzazione è autorizzata a farlo. Quando un certificato include il nome di un individuo come rappresentante autorizzato dall'Organizzazione, il lavoro di questo individuo e la sua autorità ad agire per conto dell'Organizzazione dovrà allo stesso modo essere confermata.

Quando un nome dominio o un indirizzo e-mail sono inclusi nel certificato Trust Italia S.p.A. e/o Symantec autentica il diritto dell'organizzazione ad usare quel nome dominio sia come Nome Dominio per Esteso (Fully Qualified Domain Name) sia come dominio di posta elettronica.

I controlli supplementari necessari per soddisfare le normative di esportazione degli Stati Uniti e le licenze rilasciate dal Department of Commerce Bureau of Industry and Science ("BIS") degli Stati Uniti sono effettuati da Trust Italia S.p.A. e/o Symantec quando richiesto.

Ulteriori procedure vengono eseguite per specifiche tipologie di Certificati come descritto nella tabella 6 che suegue.

Tipologia di Certificato	***Procedure Aggiuntive***
OFX Server ID	Symantec verifica che l' Organization sia una banca, un istituto di credito oppure sia classificata sotto uno dei seguenti codici SIC: • 60xx Istituti di Deposito • 61xx Istituti di Credito e di non-deposito • 62xx Sicurezza, broker merceologici e servizi • 63xx Compagnie Assicurative • 64xx Agenti assicurativi, broker e servizi • 67xx Holding ed altri fondi d'investimento • 7372 Software preconfezionati • 7373 Progettazione di sistemi integrati per computer • 7374 Data processing ed allestimento

Tipologia di Certificato	*Procedure Aggiuntive*
	• 3661 Apparecchiature telefoniche e telegrafiche • 8721 Contabilità, Revisione dei conti e dei libri contabili.
Hardware Protected SSL Certificate	Symantec verifica che la coppia di chiavi sia generata su hardware certificato FIPS 140.
Managed PKI for Intranet SSL Certificate	Symantec verifica che l' host name o l' indirizzo IP assegnato ad un Device non sia accessibile da internet (accessibile pubblicamente) e sia di prorietà dell' abbonato del certificato.
Authenticated Content Signing Certificate	Prima che Symantec firmi digitalmente contenuti utilizzando ACS si autentica che il contenuto sia l'originale firmato dall' Organization utilizzando un proprio Certificato Code Signing

Tabella 6. Specifiche Procedure di Autenticazione

3.2.3 Autenticazione dell' Identità Individuale

L' autenticazione di identità individuale differisce a seconda della classe di certificazione. Lo standard minimo di autenticazione per ciascuna classe di VTN è spiegata nella tabella 7 qui di seguito.

Classe di Cerificazione	Autenticazione dell' Identità
Classe 1	Nessuna autenticazione dell'identità. E' limitata alla conferma dell'email dell'abbonato richiedendo a quest'ultimo di rispondere ad un' email da quell'email
Classe 2	Si autentica l'identità confrontando l'identità fornita dall'abbonato con: o Informazioni riposte nel database di Trust Italia S.p.A., servizio di prove di identità, come un istituto di credito o altra fonte attendibile che fornisca informazioni, o o informazioni contenute nei documenti aziendali o database di informazioni commerciali (elenchi di dipendenti o clienti) di un RA che approvi i certificati per i propri individui affiliati
Classe 3	L'autenticazione delle Richiesta di Certificati individuali di Classe 3 si basa sulla presenza personale (fisica) del Richiedente il Certificato innanzi ad un rappresentante della CA o della RA o dinnanzi ad un notaio o altro pubblico ufficiale con autorità similare nell'ambito giurisdizionale del Richiedente il Certificato. Il rappresentante, notaio o altro pubblico ufficiale controlla l'identità del Richiedente il Certificato mediante una forma ampiamente riconosciuta di documento identificativo rilasciato da un ente governativo (ad es. passaporto o patente) ed un'altra credenziale identificativa. L'autenticazione dei Certificati da Amministratore Classe 3 certificati è basata sull'autenticazione dell'organizzazione e da una conferma da parte dell'organizzazione sull'identità e sul l'autorizzazione della persona ad agire in qualità di Amministratore. Trust Italia S.p.A. potrebbe trovarsi ad approvare Richieste di Certificazione per propri stessi Amministratori. Gli Amministratori sono "Persone di Fiducia" all'interno dell'organizzazione. In questo caso, l'autenticazione delle loro domande di certificazione si basa sulla conferma della loro identità in relazione alla loro posizione lavorativa o sulla memorizzazione in qualità di contraente indipendente e di procedure di background di controllo.[8]

[8] Trust Italia S.p.A. può dare approvazione che certificati per Amministratore siano associati ad un destinatario non-umano, come un dispositivo o un server. Le richieste di autenticazione di un certificato di Classe 3 per amministratore di destinatari non umani devono comprendere:

• Autenticazione dell'esistenza e dell'identità del servizio denominato come Amministratore nella Richiesta di Certificazione

• Autenticazione che il servizio sia stato implementato in modo sicuro coerentemente con l'oggetto che svolge la funzione Amministrativa

• Conferma dell'identità e autorizzazione della persona che si registra nella Richiesta di Certificato per il certificato di Amministratore nel servizio denominato Amministratore.

Tabella 7. Autenticazione dell' Identità Individuale

3.2.4 Informazioni Non Verificate degli Abbonati

Le informazioni non verificate sugli Abbonati comprendono :

- Organization Unit (OU)
- Nome dell'Abbonato nei certificati di Classe 1
- Qualsiasi altra informazione definita come non-verificata nel certificato.

3.2.5 Validazione dell'Autorità

Ogni volta che il nome di un individuo viene associato al nome di una Organizzazione nell'ambito di un certificato in modo tale da indicare l'affiliazione individuale o l'autorizzazione ad agire per conto dell' Organizzazione, Trust Italia S.p.A. o una RA:

- determina l'esistenza dell' Organizzazione, utilizzando almeno un'entità terza per comprovare l'identità tramite servizio o database, o in alternativa, documentazione organizzativa rilasciata o depositata presso il governo di riferimento che confermi l'esistenza dell'Organizzazione, e
- utilizza le informazioni contenute nei documenti aziendali o banche dati di informazioni commerciali (reperite o da directory del cliente) di una RA per l'approvazione di certificati per i propri affiliati individuali o conferma tramite telefono, posta o procedura analoga per l'Organizzazione, l'assunzione presso l'Organizzazione della persona che presenta domanda di certificazione e, se del caso, la sua autorità ad agire per conto dell'Organizzazione.

3.2.6 Criteri per l' Interoperatività

Trust Italia S.p.A. può fornire servizi di interoperabilità che consentano ad una CA non VTN di essere nelle condizioni di interoperare unilateralmente con la VTN certificando quella CA. Le CA abilitate ad interagire in questo modo dovranno rispettare il CP VTN, integrando le policy supplementari laddove necessario.

Trust Italia S.p.A. può autorizzare l'interoperabilità con la VTN di una CA non VTN soltanto in circostanze in cui la CA, come minimo:

- Entra in un accordo contrattuale con Trust Italia S.p.A.
- Opera nell'ambito del CPS che soddisfi i requisiti VTN per le classi di certificati che rilascia
- Passa una valutazione di conformità prima di poter interoperare
- Passa una valutazione di conformità annuale per l'ammissibilità ad interoperare con continuità.

3.3 Identificazione e Autenticazione per Richieste di Rigenerazione di chiavi

Prima della scadenza di un Certificato di Abbonamento esistente, è necessario che l'Abbonato ottenga un nuovo certificato al fine di mantenere la continuità nell'utilizzo del Certificato. Trust Italia S.p.A. prevede di solito che l'Abbonato generi una nuova coppia di chiavi in sostituzione della coppia che viene a scadere (processo tecnicamente definito "Ricodifica" o "Rekey"). Tuttavia, in alcuni casi (ad es. per certificati web server) Trust Italia S.p.A. permette agli Abbonati di richiedere un nuovo certificato per coppie di chiavi pre-esistenti (processo tecnicamente definito "Rinnovo").

In termini generali, sia la "Ricodifica" che il "Rinnovo" sono comunemente descritti come "Rinnovo di Certificato", poiché ci si concentra sul fatto che il vecchio Certificato viene sostituito da uno nuovo, senza tenere conto se sia stata generata una nuova coppia di chiavi o meno. Per tutte le Classi e tutti i Tipi di Certificati di Trust Italia S.p.A., ad eccezione dei Certificati Server di Classe 3, tale distinzione non è rilevante, in quanto nell'ambito del processo di sostituzione di un Certificato di Abbonamento per utente finale effettuato da Trust Italia S.p.A. viene sempre generata una nuova coppia di chiavi.
Tuttavia per i Certificati Server di Classe 3, poiché la coppia di chiavi dell'Abbonato è generata sul web server e la maggior parte degli strumenti per la generazione di coppie di chiavi per web server permettono la creazione di una nuova Richiesta di Certificato per una coppia di chiavi esistente, vi è una distinzione fra "ricodifica" e "rinnovo".

3.3.1 Identificazione e Autenticazione di routine per la Rigenerazione delle chiavi

Le procedure di Rigenerazione delle chiavi accerta che la persona o l'organizzazione che cerca di rigenerare il Certificato di Abbonamento da utente finale sia di fatto il richiedente il certificato.

Una procedura accettabile prevede l'utilizzo di una Challenge Phrase, "parola d'ordine" (o equivalente), o la prova di possesso della chiave privata. Gli Abbonati scelgono ed inseriscono la Challenge Phrase durante l'immissione dei loro dati di immatricolazione. Al momento del rinnovo del certificato, se l'Abbonato immette correttamente la Challenge Phrase di sottoscrizione (o equivalente) con le informazioni di ri-immatricolazione dell' Abbonato, e le informazioni di iscrizione (comprese le informazioni di contatto aziendale e tecnico) non sono cambiate, il rinnovo del certificato viene rilasciato automaticamente. In alternativa all'utilizzo della Challenge Phrase (o equivalente) Symantec può inviare un messaggio di posta elettronica all'indirizzo e-mail associato al verificato contatto aziendale per il certificato di rinnovo, richiedendo la conferma dell'ordine di rinnovo del certificato e l'autorizzazione a rilasciare il Certificato. Al ricevimento della conferma, che autorizza l'emissione del Certificato, Symantec rilascerà il certificato qualora i dati di iscrizione (incluse le informazioni sul Contatto Tecnico e Aziendale[9]) non siano cambiate.

Dopo la rigenerazione delle chiavi o rinnovo in questo modo, e almeno su ulteriori istanze alternative di riassegnazione delle chiavi o rinnovo seguenti, Trust Italia S.p.A. o la RA riconferma l'identità dell'abbonato in conformità con i requisiti di identificazione e autenticazione di una Richiesta di Certificazione[10].

In particolare, per successive richieste di rigenerazione delle chiavi per la vendita al dettaglio di certificati organizzativi di Classe 3 attraverso il sito www.trustitalia.it, Trust Italia S.p.A. ri-autentica il nome dell'organizzazione e il nome dominio inclusi nel certificato. Nei casi in cui:

- La Challenge Phrase sia utilizzata correttamente per il successivo certificato di rinnovo e:
- Il Distinguished Name del certificato non sia stato modificato, e
- Le informazioni sul contatto Aziendale e Tecnico rimangano invariate da ciò che in precedenza era stato verificato,

Trust Italia S.p.A. non dovrà riconfermare per telefono, posta, o procedura analoga certe informazioni al richiedente il certificato circa l'organizzazione, che la stessa ha autorizzato la Richiesta di Certificato e che la persona che richiede per conto del richiedente sia autorizzata ad agire di conseguenza.

La ricodifica successiva ai 30 giorni dalla scadenza del certificato viene ri-autenticata come una richiesta di Certificato ex-novo e non è rilasciata automaticamente.

3.3.2 Identificazione e Autenticazione per la Rigenerazione di Chiavi dopo la Revoca

La Ricodifica/ Rinnovo dopo la revoca non è ammessa se la revoca è avvenuta in quanto:

- il Certificato (ad eccezione dei Certificati di Classe 1) è stato rilasciato ad una persona diversa da quella nominata come soggetto del certificato, o
- il Certificato (ad eccezione dei Certificati di Classe 1) è stato rilasciato senza l'autorizzazione della persona o l'entità indicata come soggetto di tale certificato, o
- l'ente che approva la Richiesta di Certificato dell'Abbonato scopre o ha motivo di ritenere che un fatto oggettivo nella Richiesta di Certificato sia falso.
- Per qualsiasi altro motivo ritenuto necessario da parte di Symantec o Trust Italia S.p.A. per proteggere la VTN

Fatto salvo per il paragrafo precedente, il rinnovo di un certificato organizzativo o di CA a seguito di revoca del certificato è ammesso a condizione che le procedure di rinnovo accertino che l'organizzazione o la CA

9 Se le informazioni di contatto sono cambiate attraverso una procedura formale di modifica contatto approvata il certificato dovrà essere ancora qualificato come rinnovo automatizzato.

10 L'autenticazione di una richiesta di rigenerazione chiavi / rinnovo di un Certificato Classe 3 ASB, tuttavia, richiede l'uso di una Challenge Phrase così come la stessa identificazione e autenticazione di un Certificato originale.

che chiede il rinnovo sia nei fatti l' abbonato del certificato. I certificati aziendali rinnovati devono contenere lo stesso Distinguished Name come soggetto del certificato organizzativo che è stato rinnovato.

Il rinnovo di un certificato individuale successivo alla revoca deve accertare che la persona che chiede il rinnovo sia effettivamente il richiedente. Una procedura accettabile è considerata l'uso di una Challenge Phrase (o equivalente). In alternativa alla presente procedura o ad altro procedimento approvato da Trust Italia S.p.A., i requisiti per l'identificazione e l'autenticazione di una richiesta di certificazione originale dovranno essere utilizzati per il rinnovo di un Certificato successivo a revoca.

3.4 Identificazione e Autenticazione per Richiesta di Revoca

Prima di revocare un certificato, Trust Italia S.p.A. verifica che la revoca sia stata richiesta dall' Abbonato del certificato, l'ente che ha approvato la Richiesta di Certificato.

Procedure accettabili per autenticare le richieste di revoca di un Abbonato sono:

- Immettere la Challenge Phrase (o il suo equivalente) muniti di sottoscrizione per presentare alcuni tipi di certificati e la revoca del certificato avviene automaticamente se la Challenge Phrase (o l'equivalente) corrisponde con le informazioni.
- Ricevere dal Richiedente un messaggio di richiesta revoca che contenga una firma digitale verificabile con riferimento al certificato da revocare,
- Una comunicazione con la quale il richiedente fornisce garanzie ragionevoli sulla Classe di Certificazione che la persona o organizzazione che chiede la revoca si di fatto il richiedente. Tale comunicazione, a seconda delle circostanze, può essere inclusa tramite uno o più mezzi metodi: telefono, fax, e-mail, posta o corriere.

Gli amministratori di Trust Italia S.p.A. hanno il diritto di richiedere la revoca di un certificato di Abbonamento per utente finale nell'ambito del sottodominio di Trust Italia S.p.A..
Trust Italia S.p.A. autentica l'identità degli amministratori attraverso il controllo di accesso tramite autenticazione SSL e client prima di consentire loro di svolgere le funzioni di revoca, o di altra procedura approvata dal VTN.

Le RA utilizzando un Automated Administration Software Module possono presentare alla rinfusa richieste di revoca a Trust Italia S.p.A.. Tali richieste devono essere autenticate tramite richiesta firmata digitalmente con la chiave privata nell' Automated Administration hardware token delle RA

Le richieste di revoca dei certificati CA devono essere autenticate da Trust Italia S.p.A. per garantire che tale revoca sia stata di fatto richiesta dalla CA stessa.

4. Requisiti Operativi del ciclo di vita di un certificato

4.1 Richiesta di Certificato

4.1.1 Chi può presentare domanda di certificazione?

Di seguito è riportato un elenco di persone che possono presentare domanda di certificazione:

- Qualsiasi individuo che sia il soggetto del certificato,
- Qualsiasi rappresentante autorizzato da un'organizzazione o ente,
- Qualsiasi rappresentante autorizzato da una CA,
- Qualsiasi rappresentante autorizzato da un RA.

4.1.2 Processo di Registrazione e Responsabilità

Utenti finali Richiedenti i Certificati

Tutti gli utente finali richiedenti un certificato devono manifestare il loro assenso al Subscriber Agreement che contiene le dichiarazioni e garanzie descritte nella sezione 9.6.3 e sottoposte ad un processo di registrazione che prevede:

- completare una Richiesta di Certificazione e fornire informazioni veritiere e corrette,

- generare o disporre la generazione di una coppia di chiavi,
- consegnare il proprio/a chiave pubblica, direttamente o tramite una RA, a Trust Italia S.p.A.
- dimostrare il possesso e/o il controllo esclusivo della chiave privata corrispondente alla chiave pubblica consegnata a Trust Italia S.p.A..

Certificati CA e RA

Gli abbonati dei certificati CA ed RA stipulano un contratto con Trust Italia S.p.A.. I richiedenti CA e RA devono fornire le proprie credenziali per dimostrare la loro identità e fornire informazioni di contatto durante il processo di contrattazione. Durante questa trattativa o, al più tardi, prima della Key Generation Ceremony per creare una coppia di chiavi CA o una RA, il richiedente deve cooperare con Trust Italia S.p.A. per determinare il Distinguished Name ed il contenuto dei certificati che devono essere rilasciati al richiedente.

4.2 Processo di Richiesta del Certificato

4.2.1 Attuare le Funzioni di Identificazione ed Autenticazione

Trust Italia S.p.A. o una RA deve eseguire l'identificazione e l'autenticazione di tutte le informazioni dell'Abbonato nei termini della sezione 3.2

4.2.2 Approvazione o Rifiuto delle domande di certificazione

Trust Italia S.p.A. o una RA approverà una domanda di certificazione qualora i seguenti criteri vengano soddisfatti :

- Identificazione e autenticazione di tutte le informazioni dell'Abbonato nei termini della sezione 3.2 avvenute con successo
- pagamento ricevuto

Trust Italia S.p.A. o RA respingerà una richiesta di certificazione se:

- L'Identificazione e l'autenticazione di tutte le informazioni dell'Abbonato nei termini della sezione 3.2 non possano essere completati oppure
- Il richiedente non riesce a fornire la documentazione di supporto, su richiesta, o
- L'abbonato non riesce a rispondere alle comunicazioni entro un tempo determinato, o
- Il pagamento non è stato ricevuto, o
- La RA ritenga che rilasciare il certificato all'abbonato possa discreditare la VTN.

4.2.3 Tempo per processare le Richieste di Certificazione

Trust Italia S.p.A. inizia l'elaborazione delle domande di certificazione entro un termine ragionevole dalla ricezione. Non c'è stipula di tempo per completare il trattamento di una domanda se non diversamente indicato nel relativo Subscriber Agreement, CPS o altri accordi tra i partecipanti delle VTN. Una domanda di certificazione rimane attiva fino a respingimento.

4.3 Rilascio del certificato

4.3.1 Azioni della CA durante l'emissione del Certificato

Un certificato viene generato e rilasciato in seguito all'approvazione di una Richiesta di Certificazione da Trust Italia S.p.A. o su ricezione di richiesta di rilasciare da parte di una RA. Trust Italia S.p.A. genera e rilascia Il certificato al Richiedente sulla base delle informazioni di una Richiesta di Certificazione a seguito dell'approvazione della stessa.

4.3.2 Notifiche all'Abbonato da parte della CA che rilascia il Certificato

Trust Italia S.p.A. deve, direttamente o tramite una RA, informare i Sottoscrittori della creazione di tali Certificati e fornire all'abbonato l'accesso ai Certificati comunicando che i loro certificati sono disponibili. I certificati devono essere messi a disposizione degli abbonati utenti finali, sia permettendo loro di scaricarli da un sito web che tramite un messaggio inviato all'abbonato che contenga il Certificato.

4.4 Accettazione del Certificato

4.4.1 Condotta che costituisce l'Accettazione di un Certificato

Le seguenti condotte implicano l'accettazione del certificato:

- Il download o l'installazione di un certificato in allegato ad un messaggio implica l'accettazione dell'Abbonato del Certificato.
- L'assenza di obiezioni al certificato o al suo contenuto da parte dell' abbonato costituisce l'accettazione del certificato.

4.4.2 Pubblicazione del certificato da parte della CA

Trust Italia S.p.A. pubblica i certificati emessi in una repository accessibile al pubblico.

4.4.3 Notifica di Emissione del Certificato dalla CA ad altri Enti

Le RA possono ricevere la notifica del rilascio dei certificati da loro approvati.

4.5 Coppia di Chiavi ed Utilizzo dei certificati

4.5.1 Chiave Privata dell' Abbonato ed Utilizzo dei Certificati

L'uso della chiave privata corrispondente alla chiave pubblica contenuta nel certificato è consentito soltanto una volta che l 'Abbonato abbia accettato il Subscriber Agreement e accettato il certificato. Il certificato deve essere utilizzato legalmente in conformità con il Subscriber Agreement di Trust Italia S.p.A. entro i termini del CP e di questo CPS della VTN. L'uso del certificato deve essere coerente con le estensioni dei campi dell KeyUsage incluso nel certificato (ad esempio, se la firma digitale non è abilitata, il certificato non deve essere utilizzato per la firma).

I Sottoscrittori devono proteggere le loro chiavi private da un uso non autorizzato e interrompere l'utilizzo della seguente chiave privata dopo la scadenza o la revoca del certificato.

4.5.2 Chiave Pubblica delle Parti Facenti Affidamento ed Utilizzo del Certificato

Le parti facenti affidamento devono basarsi sui termini di contratto applicabili come condizione di riferimento sul certificato.

L' affidamento su un certificato deve essere ragionevole in base alle circostanze. Se le circostanze indicano la necessità di ulteriori garanzie, la Parte Facente Affidamento deve ottenere tali garanzie affinché tale fiducia possa essere considerata ragionevole.

Prima di qualsiasi atto di fiducia, Le parti facenti Affidamento devono valutare in modo indipendente:

- L'opportunità di utilizzare un certificato per un determinato scopo e di stabilire che il certificato sarà nei fatti utilizzato per uno scopo appropriato che non sia vietato o altresì limitato dal presente CPS. Trust Italia S.p.A. non ha responsabile nel valutare l'adeguatezza di utilizzo di un certificato.
- Che il certificato venga utilizzato in conformità con le estensioni dei campi del KeyUsage incluso nel certificato (ad esempio, se la firma digitale non è abilitata, il certificato non può essere evocato per convalidare la firma di un Abbonato).
- Lo stato del certificato e tutte le CA della catena che ha emesso il certificato.
  Se uno dei certificati della catena di certificazione sia stato revocato, la Parte Facente Affidamento è l'unico responsabile della verifica sull' affidamento di una firma digitale eseguita da un Abbonato utente finale del Certificato prima della revoca di un certificato all'interno di una catena di certificazione ragionevole. Ogni affidamento è sotto il rischio esclusivo della relativa parte.

Supponendo che l'utilizzo del certificato sia opportuno, le Parti Facenti Affidamento devono utilizzare il software appropriato e / o l' hardware per eseguire la verifica delle firme digitali o altre operazioni di crittografia che s'intenda svolgere, come condizione di far valere Certificati in relazione a ogni operazione del genere. Tali operazioni includono l' individuazione di una catena di certificazione e la verifica delle firme digitali su tutti i certificati nella Catena di certificazione.

4.6 Rinnovo del Certificato

Il rinnovo rappresenta l'emissione di un nuovo certificato per l'abbonato senza modificare la chiave pubblica o altre informazioni contenute nel certificato. Il rinnovo del certificato per i Classe 3 è supportato laddove la coppia di chiavi viene generata su un web server come la maggioranza degli strumenti su web server per la generazione di chiavi permette la creazione di una nuova richiesta di certificazione per una coppia di chiavi esistente.

4.6.1 Circostanze per il Rinnovo del Certificato

Prima della scadenza di un certificato esistente per abbonato, è necessario rinnovare un nuovo certificato per mantenere la continuità nell' utilizzo dello stesso. Un certificato può anche essere rinnovato dopo la scadenza.

4.6.2 Chi può richiedere il Rinnovo

Il rinnovo del certificato può essere richiesto soltanto dall'abbonato di un certificato individuale o da un rappresentante autorizzato per un certificato organizzativo.

4.6.3 Elaborazione delle Richieste di Rinnovo del Certificato

Le procedure di rinnovo garantiscono che la persona o l'Organizzazione che richiede il rinnovo di un Certificato di Abbonamento per utente finale sia effettivamente il abbonato (o sia da esso autorizzato) del Certificato.

Una procedura accettabile è considerata l'uso di una Challenge Phrase (o equivalente), o la verifica del possesso della chiave privata. Gli abbonati scelgono ed immettono nei loro dati di iscrizione una Challenge Phrase (o equivalente). Nel rinnovo di un certificato, se un abbonato immette correttamente la Challenge Phrase (o equivalente) con le informazioni di re-iscrizione dell'abbonato, e le informazioni di iscrizione (comprese le informazioni di Contatto Organizzativo e Tecnico[11]) non siano cambiate, il rinnovo del certificato viene rilasciato automaticamente. In alternativa all'utilizzo di una Challenge Phrase (o equivalente) Trust Italia S.p.A. può inviare un messaggio di posta elettronica all'indirizzo e-mail associato al contatto aziendale verificato per l'avvenuto rinnovo del certificato, richiedendo la conferma dell'ordine di rinnovo e l'autorizzazione a rilasciare il certificato. Al ricevimento della conferma, che autorizza l'emissione del certificato, Trust Italia S.p.A. rilascerà il certificato se i dati di iscrizione (comprese le informazioni di Contatto Organizzativo e Tecnico[12]) non siano cambiati.

In questo modo dopo il rinnovo, e almeno su istanze alternative di rinnovo successive, Trust Italia S.p.A. o la RA dovranno riconfermare l'identità dell'abbonato in conformità ai requisiti specificati nel presente CPS per l'autenticazione di un Certificato originale.

In particolare, per successive richieste di rigenerazione delle chiavi per la vendita al dettaglio di certificati organizzativi di Classe 3 attraverso il sito www.trustitalia.it , Trust Italia S.p.A. ri-autentica il nome dell'organizzazione e il nome a dominio inclusi nel certificato. Nei casi in cui:

- La Challenge Phrase sia utilizzata correttamente per il successivo rinnovo del certificato e:
- Il Distinguished Name del certificato non sia stato modificato, e
- Le informazioni sul contatto Tecnico e Organizzativo rimangano invariate da quanto in precedenza era stato verificato,

Trust Italia S.p.A. non dovrà riconfermare al Richiedente il certificato per telefono, conferma per posta, o procedura analoga le informazioni circa l'organizzazione, che l'organizzazione abbia autorizzato la il

---

11 Se le informazioni di contatto sono cambiate attraverso una procedura formale di modifica contatto approvata il certificato dovrà essere ancora qualificato come rinnovo automatizzato

12 **Se le informazioni di contatto sono cambiate attraverso una procedura formale di modifica contatto approvata il certificato dovrà essere ancora qualificato come rinnovo automatizzato.**

richiedente il Certificato, e che la persona che presenta la Richiesta di Certificato per conto del richiedente sia autorizzato a farlo.

A differenza della presente procedura o da altra approvata da Trust Italia S.p.A., i requisiti per l'autenticazione di una Richiesta di Certificato originale devono essere utilizzati per rinnovare un Certificato di Abbonamento per utente finale.

4.6.4 Notifica di Emissione per un nuovo certificato di Abbonamento

La notifica di rilascio del rinnovo del certificato di Abbonamento è a norma della sezione 4.3.2

4.6.5 Gestione che costituisce l'accettazione di un certificato di rinnovo

Tale gestione è rinnovata conformemente alla sezione 4.4.1

4.6.6 Pubblicazione del certificato di rinnovo da parte della CA

Il certificato rinnovato viene pubblicato nella repository pubblicamente accessibile di Trust Italia S.p.A..

4.6.7 Notifica di emissione del certificato dalla CA ad altre entità

Le RA possono ricevere la notifica del rilascio dei certificati che loro approvano.

4.7 Ri-generazione delle Chiavi del Certificato

E' la domanda per il rilascio di un nuovo certificato che attesta la nuova chiave pubblica. La rigenerazione delle chiavi è supportata per tutte le classi di certificato.

4.7.1 Condizioni per la Ri-generazione delle Chiavi del Certificato

Prima della scadenza di un certificato esistente per abbonato, è necessario per l' abbonato ri-generare le chiavi del certificato per dare continuità all' utilizzo del Certificato. Un certificato può avere le chiavi ri-generate successivamente alla scadenza.

4.7.2 Chi può richiedere la certificazione di una nuova chiave pubblica

Solo l'abbonato di un certificato individuale o un rappresentante autorizzato per un certificato organizzativo possono chiedere il rinnovo del certificato

4.7.3 Elaborazione Richieste di Ri-generazione Chiavi

Le procedure di Ri-generazione delle chiavi assicurano che la persona o l'ente che richiede il rinnovo di un Certificato di Abbonamento per utente finale sia effettivamente l'abbonato (o che sia autorizzato dall'abbonato) del Certificato.

Una procedura accettabile è considerata l'uso di una Challenge Phrase (o equivalente), o la verifica del possesso della chiave privata. Gli abbonati scelgono ed immettono nei loro dati di iscrizione una Challenge Phrase (o equivalente). Nel rinnovo di un certificato, se un abbonato immette correttamente la Challenge Phrase (o equivalente) con le informazioni di re-iscrizione dell'abbonato, e le informazioni di iscrizione (comprese le informazioni di contatto organizzativo e tecnico[13]) non siano cambiate, il rinnovo del certificato viene rilasciato automaticamente.

---

13 **Se le informazioni di contatto sono cambiate attraverso una procedura formale di modifica contatto approvata il certificato dovrà essere ancora qualificato come rinnovo automatizzato.**

Fatte salve le disposizioni della sezione 3.3.1, successivamente alla ri-generazione delle chiavi e almeno su istanze alternative alle ri-generazioni successive, Trust Italia S.p.A. o la RA dovranno riconfermare l'identità dell'abbonato in conformità ai requisiti specificati nel presente CPS per l'autenticazione di un Certificato originale.

A differenza della presente procedura o da altra approvata da Symantec, i requisiti per l'autenticazione di una Richiesta di Certificato originale devono essere utilizzati per la ri-generazione delle chiavi di un Certificato di Abbonamento per utente finale.

4.7.4 Notifica di Emissione di un nuovo certificato per Abbonato

Tale notifica è conforme alla sezione 4.3.2.

4.7.5 Condotta che costituisce l'accettazione di un certificato con chiavi ri-generate

In conformità con la sezione 4.4.1.

4.7.6 Pubblicazione del certificato con chiavi ri-generate da parte della CA

Tale certificato è pubblicato nella repository di Trust Italia S.p.A. accessibile pubblicamente.

4.7.7 Notifica di emissione del certificato dalla CA ad altre entità

Le RA possono ricevere la notifica del rilascio dei certificati che loro approvano.

4.8 Modifica del Certificato

4.8.1 Condizioni per la Modifica del Certificato

La modifica del certificato è relativa alla domanda per il rilascio di un nuovo certificato a causa di variazioni delle informazioni in un certificato esistente (differisce la chiave pubblica dell'abbonato).

La modifica del certificato è considerata una Richiesta di Certificato nei termini del punto 4.1.

4.8.2 Chi può richiedere la modifica del Certificato

Si veda la Sezione 4.1.1

4.8.3 Elaborazione delle Richieste per la Modifica del Certificate

Trust Italia S.p.A. o una RA devono eseguire l'identificazione e l'autenticazione di tutte le informazioni richieste all'abbonato nei termini del punto 3.2.

4.8.4 Notifica di Emissione di un Nuovo Certificato di Abbonato

Si veda la Sezione 4.3.2.

4.8.5 Condotta che costituisce l'accettazione delle Modifiche ai certificati

Si veda la Sezione 4.4.1.

4.8.6 Pubblicazione da parte della CA del certificato Modificato

Si veda la Sezione 4.4.2.

4.8.7 Notifica di Emissione del Certificato dalla CA ad Altre Entità

Si veda la Sezione 4.4.3.

4.9 Certificato di Revoca e Sospensione

4.9.1 Condizioni per la Revoca

Solo nei casi elencati di seguito, un certificato per Abbonato utente finale sarà revocato da Symantec (o dal abbonato) e pubblicato su un CRL. Su richiesta di un abbonato che non può più usare (o non voglia più usare) un certificato per un motivo diverso da quelli indicati qui di seguito, Symantec spunterà il certificato come inattivo nel suo database, ma non pubblicherà il certificato sul CRL.

Un Certificato di Abbonamento per utente finale viene revocato se:

- Trust Italia S.p.A., un Cliente o un Abbonato ha motivo di ritenere o ha forti sospetti che si sia verificata una Compromissione della chiave privata di un Abbonato,
- Trust Italia S.p.A. o un Cliente ha motivo di ritenere che l'Abbonato abbia violato un obbligo, dichiarazione o garanzia essenziale previsto nel Contratto di Abbonamento applicabile,
- Il Contratto di Abbonamento stipulato con l'Abbonato è stato risolto,
- L'affiliazione tra un Cliente Managed PKI ed un Abbonato è stata risolta o è cessata in altro modo,
- L'affiliazione tra un' Organizzazione che ha sottoscritto un Certificato di Classe 3 Organizzativo ASB ed il rappresentante organizzativo che controlla la chiave privata dell' abbonato è stata risolta o è cessata in altro modo,
- Trust Italia S.p.A. o un Cliente hanno motivo di ritenere che il Certificato sia stato rilasciato in un modo sostanzialmente non conforme alle procedure previste dal CPS applicabile, il Certificato (ad eccezione dei Certificati di Classe 1) sia stato rilasciato ad una persona diversa da quella indicata come Soggetto del Certificato, o il Certificato (ad eccezione dei Certificato di Classe 1) sia stato rilasciato senza l'autorizzazione delle persona indicata come Soggetto del Certificato stesso,
- Trust Italia S.p.A. o un Cliente hanno ragione di ritenere che un dato essenziale della Richiesta di Certificato sia falso
- Trust Italia S.p.A. o un Cliente stabiliscono che un presupposto essenziale per il Rilascio del Certificato non sia stato né soddisfatto né soggetto a rinuncia,
- Nel caso di Certificati aziendali di Classe 3: cambia la denominazione dell'organizzazione dell'Abbonato,
- Le informazioni contenute nel certificato ad eccezione di quelle non verificate sull'abbonato siano incorrette o cambiate, oppure
- L'uso continuativo di questo certificato sia dannoso al VTN

Nel valutare se l'uso del certificato sia dannoso per la VTN, Trust Italia S.p.A. ritiene, tra le altre cose, quanto segue:

- La natura e il numero di reclami ricevuti
- L'identità del denunciante (/i)
- La legislazione in vigore
- Le risposte al presunto uso dannoso da parte dell' Abbonato

Nel valutare se l'uso di un certificato Code Signing sia dannoso per il VTN, Trust Italia S.p.A. ritiene, tra le altre cose, quanto segue:

- Il nome del codice che è stato firmato
- Il comportamento del codice
- Le modalità di distribuzione del codice
- Divulgazioni rivolte ai destinatari del codice
- Qualsiasi accusa supplementare realizzata sul codice

Trust Italia S.p.A. può anche revocare un certificato di amministratore se l'autorità dell'amministratore a d agire come tale sia stato interrotta oppure sia terminata.

I contratti di Abbonamento di Trust Italia S.p.A. richiedono agli Abbonati utenti finali di notificare immediatamente a Trust Italia S.p.A. ogni compromissione appurata o presunta della propria chiave privata.

4.9.2 Chi può Richiedere la Revoca

I singoli abbonati possono richiedere la revoca dei propri certificati individuali. Nel caso di Certificati organizzativi, un rappresentante debitamente autorizzato dall'organizzazione ha il diritto di richiedere la revoca di Certificati rilasciati per l'organizzazione. Un rappresentante debitamente autorizzato da Trust Italia S.p.A. o da una RA ha il diritto di richiedere la revoca di un certificato di amministratore di una RA. L'ente che ha approvato una Richiesta di Certificato dell'Abbonato dovrà avere anche la facoltà di revocare o di richiedere la revoca del Certificato dell'abbonato.
Solo Trust Italia S.p.A. ha il diritto di richiedere o avviare la revoca dei certificati rilasciati dalla propria CA. Le RA hanno diritto, attraverso i loro rappresentanti debitamente autorizzati, di richiedere la revoca dei propri certificati e le loro entità superiori hanno il diritto di richiesta o di avviare la revoca dei loro certificati.

4.9.3 Procedura per la Richiesta di Revoca

Procedura per la Richiesta di Revoca di un Certificato di Abbonamento per utente finale

Un Abbonato utente finale che richiede la revoca è tenuto a comunicare la richiesta a Trust Italia S.p.A. o al Cliente che approva la Richiesta di Certificato dell'Abbonato, che a sua volta avvierà prontamente la revoca del certificato. Per i clienti aziendali, l'Abbonato è tenuto a comunicare la richiesta all' amministratore dell'organizzazione che provvederà a comunicare la richiesta di revoca a Trust Italia S.p.A. per l'elaborazione. Le comunicazioni di richiesta di revoca devono essere conformi al CPS § 3.4.

Quando un cliente aziendale avvia la revoca di un Certificato di Abbonamento per utente finale di propria iniziativa, il Cliente Managed PKI o Cliente ASB incarica Trust Italia S.p.A. a revocare il certificato.

Procedura per la Richiesta di Revoca di un certificato CA o RA

Una richiesta di revoca da parte di una CA o RA d un proprio certificato è necessario che sia comunicata a Trust Italia S.p.A.. Di conseguenza Trust Italia S.p.A. revocherà il certificato. Trust Italia S.p.A. può anche avviare una revoca dei certificati di CA o RA.

4.9.4 Periodo di Grazia per Richiesta di revoca

Le richieste di revoca devono essere presentate il prima possibile entro un lasso di tempo commercialmente ragionevole.

4.9.5 Tempo entro il quale una CA deve elaborare la richiesta di revoca

Trust Italia S.p.A. adotterà le misure commercialmente ragionevoli per elaborare le richieste di revoca senza indugio.

4.9.6 Verifica dei requisiti di revoca per le Parti Facenti Affidamento

Le Parti Facenti Affidamento devono verificare lo stato dei Certificati di cui intendono avvalersi. Un metodo con il quale le Parti Facenti Affidamento possono controllare lo stato del certificato è consultando il CRL più recente dalla CA che ha rilasciato il certificato di cui la Parte Facente Affidamento intende avvalersi. In alternativa, le Parti Facenti Affidamento possono soddisfare tale requisito mediante il controllo di stato del certificato utilizzando il repository applicabile su base web tramite l' OCSP (se disponibile). Le CA possono fornire alle Parti Facente Affidamento informazioni su come trovare il CRL appropriato, la repository su base web, o l'OCSP (laddove disponibile) per verificare lo stato di revoca.

4.9.7 Frequenza di Pubblicazione del CRL

Le CRL per i certificati di Abbonamento degli utenti finali sono rilasciati almeno una volta al giorno. Le CRL per i certificati di CA sono rilasciati con cadenza minima annuale, ma anche ogni volta che un certificato CA viene revocato.

Le CRL per Authenticated Content Signing (ACS) su Root CA sono pubblicate annualmente ed anche ogni

volta che un certificato CA viene revocato.

Se un certificato in lista sulla CRL è in scadenza, esso può essere rimosso dal CRL successivamente alla pubblicazione dopo la scadenza del certificato.

4.9.8 Latenza massima dei CRL

CRL sono inviati al repository entro un tempo commercialmente ragionevole dopo generazione. Questo è generalmente fatto automaticamente in pochi minuti di generazione.

4.9.9 Possibilità di Controlli On-Line su Stato/Revoca

La revoca online ed altre informazioni sullo stato dei Certificati sono disponibili tramite repository su base web e, se disponibile, OCSP. Oltre alla pubblicazione dei CRL, Trust Italia S.p.A. fornisce informazioni sullo stato del certificato tramite le funzioni di query nella repository Trust Italia S.p.A..

informazioni sullo stato dei Certificati sono disponibili attraverso funzioni di ricerca su base web accessibili tramite la repository di Trust Italia S.p.A. Repository su

- https://www.trustitalia.it/repository (per Certificati individuali) e
- https://www.trustitalia.it/repository (per Certificati Server e Developer).

Trust Italia S.p.A. fornisce anche informazioni sullo stato di Certificati OCSP. I Clienti Managed PKI, che stipulano servizi OCSP, potranno controllare lo stato dei Certificati tramite l'utilizzo dell'OCSP. La URL per il relativo Responder OCSP viene comunicata al Cliente Managed PKI.

4.9.10 Requisiti per la Verifica della Revoca On-line

Una Parte Facente Affidamento deve verificare lo stato di un certificato di cui lui / lei / esso intenda avvalersi. Se una Parte Facente Affidamento non controlla lo stato di un certificato di cui intende avvalersi consultando a riguardo il CRL più recente, la Parte Facente Affidamento verifica lo stato dei Certificati consultando la relativa repository o mediante la richiesta di stato del Certificato tramite il risponder OCSP applicabile (OCSP in cui i servizi siano disponibili).

4.9.11 Altre Forme di Pubblicizzazione delle Revoche

Non applicabile.

4.9.12 Condizioni Speciali in Relazione alla Compromissione di Chiavi

Trust Italia S.p.A. userà mezzi commercialmente ragionevoli per informare potenziali Parti Facenti Affidamento nel caso in cui si accorga, o abbia motivo di credere che si sia verificata una Compromissione della chiave privata della loro stessa CA o di una CA all'interno dei loro sotto-domini.

4.9.13 Condizioni per la Sospensione

Non applicabile.

4.9.14 Chi può Richiedere la Sospensione

Non applicabile.

4.9.15 Procedura per la Richiesta di Sospensione

Non applicabile.

4.9.16 Limiti sul Periodo di Sospensione

Non applicabile.

4.10 Servizi sullo Status del Certificato

4.10.1

4.10.2 Caratteristiche Operative

Lo stato dei certificati pubblici è disponibile sul sito Trust Italia S.p.A. tramite CRL, directory LDAP e responder OCSP (laddove disponibile).

4.10.3 Disponibilità del Servizio

I servizi sullo Status dei Certificati sono disponibili 24 x 7, senza interruzioni di linea.

4.10.4 Caratteristiche Opzionali

L' OCSP è una caratteristica opzionale sullo stato del servizio che non è disponibile per tutti i prodotti e deve essere specificamente abilitata per altri prodotti.

4.11 Termine della Sottoscrizione

Un abbonato può terminare una sottoscrizione per un certificato Trust Italia S.p.A. all'avverarsi di una delle seguenti circostanze:

- Lasciare che il proprio certificato arrivi a scadenza senza rinnovo o rigenerazione delle chiavi del certificato
- Revocare il proprio certificato prima della scadenza senza la sostituzione dei certificati.

4.12 Key Escrow e Recovery

Ad eccezione delle imprese in possesso della Managed PKI Key Management Services nessun partecipante VTN può custodire chiavi privati di CA, RA o di Abbonati utenti finali.

I clienti aziendali utilizzando il Managed PKI Key Management Service (KMS) possono custodire copie delle chiavi private degli Abbonati le cui richieste di certificazione vengano approvate. Il cliente Aziendale può utilizzare un KMS gestito al di fuori della società o internamente ai Data Center in sicurezza di Trust Italia S.p.A.. Se gestite al di fuori dell'ambito dell'impresa, Trust Italia S.p.A. non archivierà le copie delle chiavi private degli abbonati, ma giocherà un ruolo importante nel processo di recovery della chiave dell'abbonato.

4.12.1 Key Escrow e Recovery Policy e Pratiche

Ai clienti aziendali che utilizzano il Managed PKI Key Management Service (o un servizio equivalente approvato da Symantec) è consentito custodire la chiave privata degli abbonati utenti finali. Le chiavi private custodite saranno immagazzinate in forma cifrata usando il Managed PKI Key Manager software. A parte i clienti aziendali che usano il Managed PKI Key Manager Service (o un servizio equivalente approvato da Symantec), le chiavi private delle CA o degli abbonati utenti finali non saranno custodite.

Le chiavi private degli abbonati utenti finali saranno recuperate soltanto in circostanze consentite all'interno della Managed PKI Key Management Service Administrator's Guide, secondo cui:

- I clienti aziendali utilizzando il Managed PKI Key Manager devono confermare l'identità di ogni persona che si presenta come Abbonato per garantire che una presunta richiesta di sottoscrizione per chiave privata sia effettivamente dell' Abbonato e non di un impostore,
- I clienti aziendali devono recuperare la chiave privata di un Abbonato senza l'autorizzazione dell' Abbonato solo per i propri fini leciti e legittimi, in conformità con le procedure giudiziarie, amministrative o di un mandato di perquisizione e non per scopi illegali, fraudolenti o altri illeciti e
- Tali clienti aziendali dovranno controllare personalmente al fine di evitare che gli amministratori del Key Management Service ed altre persone abbiano accesso non autorizzato alle chiavi private.

Si raccomanda ai clienti Enterprise che utilizzano il KMS di:

- Informare gli abbonati che le loro chiavi private siano custodite

- Proteggere gli abbonati dalla divulgazione non autorizzata,
- Proteggere tutte le informazioni, comprese le chiavi (e) dell'amministratore che potrebbero essere utilizzate per recuperare le chiavi custodita dagli abbonati.
- Rilasciare le chiavi custodite dell' Abbonato solo previo autenticazione regolamentata e richiesta di recovery autorizzata.
- Revocare la coppia di chiavi dell' Abbonato prima di recuperare la chiave cifrata.
- Non essere tenuti a comunicare ogni informazione relativa ad un recovery all'abbonato, tranne qualora l'abbonato stesso lo richieda espressamente. Non divulgare o permettre che siano divulgate le chiavi custodite o informazioni relative a chiavi custodite, se non richiesto dalla legge, norma di governo, o regolamento; da policy organizzativa aziendale, o per ordine di un tribunale della giurisdizione competente.

4.12.2 Incapsulamento delle Chiavi di Sessione, Policy di Recupero e Pratiche

Le chiavi private vengono memorizzate nel database del Key Manager in forma crittografata. Ciascuna chiave privata di ogni abbonato è individualmente cifrata con la propria chiave simmetrica triple-DES. Viene generato un Key Escrow Record (KER), quindi il la chiave triple-DES viene combinata con una sessione chiave casuale per formare una sessione chiave mascherata. La risultante chiave di sessione mascherata (MSK) viene correttamente inviata e memorizzata nel database della Managed PKI presso Trust Italia S.p.A.. Il KER (contenente la chiave privata dell'utente finale) e la maschera di sessione casuale chiave sono memorizzate nel Key Manager database e tutto il materiale residuo delle chiavi viene distrutto.

Il Managed PKI database è gestito dal Secure Data Center di Trust Italia S.p.A.. Il cliente aziendale può scegliere di utilizzare il Key Manager database sia internamente all' impresa che all'infuori del secure data center di Trust Italia S.p.A..

Il recupero del certificato di chiave privata e digitale richiede che l'amministratore della Managed PKI per accedere in modo sicuro al Managed PKI Control Center, selezioni la coppia di chiavi appropriata da recuperare e faccia click sul collegamento ipertestuale "recupero". Solo dopo il click di approvazione di un amministratore sul link "recupero" viene restituita la MSK per quella coppia di chiavi dal database Managed PKI. Il Key Manager recupera la chiave di sessione dal KMD e la combina con la MSK per rigenerare la chiave triple-DES che è stata originariamente utilizzata per crittografare la chiave privata, consentendo il recupero della chiave privata dell'utente finale. Come ultimo passaggio, viene restituito all'amministratore un file criptato PKCS # 12 ed infine distribuito all' utente finale.

5. Funzioni, Management e Controlli Operativi

5.1 Controlli Fisici

Trust Italia S.p.A. ha implementato la Trust Italia S.p.A. Physical Security Policy, che supporta i requisiti di sicurezza di questo manuale operativo. Il rispetto di tali politiche è incluso nel audit interno a Trust Italia S.p.A. descritto nella Sezione 8. La Trust Italia S.p.A. Physical Security Policy contiene informazioni sensibili per la sicurezza ed è disponibile solo previo accordo con Trust Italia S.p.A.. Una panoramica dei requisiti è descritta di seguito.

5.1.1 Dislocamento del Sito e Costruzioni

Le operazioni di CA e RA di Trust Italia S.p.A. sono svolte all'interno di un ambiente fisicamente protetto che scoraggia, previene e rileva un uso non autorizzato, la divulgazione o l'accesso ad informazioni sensibili ed ai sistemi sia celati che manifesti.

Trust Italia S.p.A. mantiene anche servizi di disaster recovery per le proprie operazioni di CA. I servizi di disaster recovery di Trust Italia S.p.A. sono protetti da più livelli di sicurezza fisica paragonabili a quelli degli ambienti primari di Trust Italia S.p.A..

5.1.2 Accesso Fisico

I sistemi CA di Trust Italia S.p.A. sono protetti mediante quattro livelli di sicurezza fisica. E' necessario ottenere accesso al livello inferiore prima di poter accedere a quello superiore.

I privilegi di accesso fisico progressivamente restrittivi controllano l'accesso ad ogni livello. L'attività operativa sensibile di CA, tutta l'attività relativa al ciclo di vita del processo di certificazione quale l'autenticazione, la verifica e l'emissione, si presentano all'interno di livelli fisici molto restrittivi. L'accesso ad ogni livello richiede l'uso di badge degli impiegati come carta di prossimità. L'accesso fisico è annotato ed il video è registrato automaticamente. I livelli supplementari impongono il controllo specifico di accesso con l'uso dell'autenticazione a due fattori compresa la biometria. Al visitatore, compreso agli impiegati o gli ospiti non autenticati, non è permesso l'accesso in tali zone di sicurezza.

Il sistema di sicurezza fisica include livelli aggiuntivi per la gestione delle chiavi di sicurezza che servono a tutelare sia lo storage online e offline del CSU che il materiali di cifratura. Aree utilizzate per creare e archiviare materiale crittografico richiedono un doppio controllo, ciascuno attraverso l'uso di autenticazione a due fattori tra cui la biometria. I CSU on line sono protetti tramite l'uso di armadi chiusi a chiave. I CSU offline sono protetti tramite l'uso di casseforti chiuse, armadi e container. L'accesso al CSU ed al materiale di cifratura è limitato in conformità con i requisiti degli obblighi di segregazione di Trust Italia S.p.A.. L'apertura e la chiusura di armadi o contenitori in questi livelli si registra per eventuali controlli.

5.1.3 Alimentazione e Climatizzazione

Gli ambienti in sicurezza di Trust Italia S.p.A. sono dotati di primari e di backup:

- sistemi di alimentazione per garantire la continua, l'accesso ininterrotto di energia elettrica e
- riscaldamento/ ventilazione/ aria condizionata a controllo di temperatura e relativa umidità.

5.1.4 Esposizioni all' Acqua

Trust Italia S.p.A. ha preso le precauzioni necessarie per ridurre al minimo l'impatto dell'esposizione all'acqua dei sistemi di Trust Italia S.p.A..

5.1.5 Prevenzione e Protezione dal Fuoco

Trust Italia S.p.A. ha preso le precauzioni necessarie per prevenire e spegnere gli incendi o altri danni da esposizione a fiamme o fumo. Le misure di prevenzione e protezione dal fuoco di Trust Italia S.p.A. sono state progettate per soddisfare le normative locali di sicurezza antincendio.

5.1.6 Media Storage

Tutti i supporti contenenti software di produzione e dei dati, audit, archivio, o informazioni di backup sono memorizzati all'interno delle strutture di Trust Italia S.p.A. o in una struttura sicura di storage off-site con adeguati controlli di accesso fisico e logico volti a limitare l'accesso al personale autorizzato ed a proteggere questi mezzi di comunicazione da danni accidentali (ad esempio, acqua, fuoco ed elettromagnetici).

5.1.7 Smaltimento Rifiuti

Documenti sensibili e materiali sono triturati prima dello smaltimento. Supporti utilizzati per raccogliere o trasmettere informazioni sensibili sono resi illeggibili prima dello smaltimento. Dispositivi crittografici sono fisicamente distrutti o azzerati secondo orientamento dei produttori prima dello smaltimento. Altri tipi di rifiuti vengono smaltiti in conformità con le normali esigenze di smaltimento di Trust Italia S.p.A..

5.1.8 Backup Off-Site

Trust Italia S.p.A. esegue i backup di routine dei dati critici del sistema, i log di audit ed altre informazioni sensibili. I supporti di backup fuori sede vengono memorizzati in modo fisicamente protetto utilizzando un terzo impianto di storage annesso ed un ambiente Trust Italia S.p.A. per il disaster recovery.

5.2 Controlli Procedurali

5.2.1 Ruoli Fiduciari

Tra le Persone Fiduciarie si annoverano tutti gli impiegati, appaltatori e consulenti i quali abbiano accesso a o controllino le operazioni di autenticazione o crittografia che possano avere un impatto rilevante su:

- la convalida delle informazioni contenute nelle Richieste di Certificati;
- l'accettazione, il rigetto o altro esame di Richieste dei Certificati, domande di revoca o di rinnovo o informazioni presentate all'iscrizione;
- il rilascio o la revoca di Certificati, ivi incluso il personale che ha accesso alle parti riservate dell'archivio; oppure
- l'elaborazione di informazioni e domande presentate dagli Abbonati.

Le Persone Fiduciarie includono (a titolo esemplificativo e non esaustivo):

- personale addetto al servizio-clienti,
- personale addetto a servizi ed operazioni crittografici,
- personale addetto alla sicurezza,
- personale addetto all'amministrazione del sistema,
- personale ingegneristico, e
- dirigenti designati a gestire l'affidabilità infrastrutturale.

Trust Italia S.p.A. considera le categorie identificate nel presente paragrafo come Persone Fiduciarie che rivestono una Posizione Fiduciaria. Le persone che desiderano diventare Persone Fiduciarie attraverso l'ottenimento di una Posizione Fiduciaria devono superare lo screening dei requisiti regolamentato in questo CPS.

5.2.2 Numero di Persone Necessarie per ogni Manzione

Trust Italia S.p.A. ha stabilito, si attiene ed applica rigorose procedure di controllo al fine di garantire la delimitazione delle funzioni basata su rispettive responsabilità e di garantire che le persone più attendibili siano tenute a svolgere delicate attività.

Le procedure di policy e controllo sono in atto per garantire la separazione dei compiti in base alle responsabilità di lavoro. I compiti più delicati, come l'accesso e la gestione di hardware crittografico CA (unità di firma crittografica o CSU) e relativo materiale di cifratura, richiedono più persone "Trusted".

Tali procedure interne di controllo sono strutturate in modo tale da garantire che almeno due membri fiduciari del personale abbiano accesso fisico o logico al dispositivo. L'accesso al hardware crittografico CA è controllato da varie Persone Fiduciarie per tutto il ciclo vitale, dal ricevimento ed ispezione iniziale alla distruzione logica e/o fisica finale. Una volta attivato il modulo tramite chiavi operative, si mettono in atto ulteriori controlli di accesso per mantenere un controllo multiplo sull'accesso sia fisico che logico al dispositivo. Le persone che hanno accesso fisico ai moduli non detengono "Parti Segrete" e viceversa.

Altre operazioni, tra cui la convalida ed il rilascio di Certificati di Classe 3, richiedono il coinvolgimento di almeno due Persone Fiduciarie o una combinazione di almeno una persona di fiducia e di una validazione automatica ed un processo di emissione. Un manuale per le operazioni di Key Recovery può opzionalmente richiedere la convalida di due (2) amministratori autorizzati.

5.2.3 Identificazione ed Autenticazione di Ciascun Ruolo

Per tutti i membri del personale che intendano diventare Persone Fiduciarie viene svolta una verifica di identità che prevede la presenza personale (fisica) di tali impiegati dinanzi a Persone Fiduciarie che svolgono funzioni HR o di sicurezza per Trust Italia S.p.A., nonché un controllo di documenti identificati universalmente riconosciuti (ad es. passaporto e patente). L'identità è ulteriormente confermata mediante le procedure di controllo in background come previste al CPS § 5.3.1.

Trust Italia S.p.A. assicura che gli impiegati in questione abbiano ottenuto lo stato di fiduciari e l'approvazione del rispettivo dipartimento prima che a queste persone:

- Siano rilasciati dispositivi di accesso e sia consentito l'accesso alle strutture richieste; personale addetto a servizi ed operazioni crittografici,
- Siano rilasciate credenziali elettroniche per accedere a e svolgere funzioni specifiche sui sistemi CA, RA o altri sistemi informatici di Trust Italia S.p.A..

5.2.4 Ruoli che richiedono Separazione di Compiti

I ruoli che richiedono una separazione delle funzioni comprendono (ma non solo)

- la convalida delle informazioni nelle richieste di Certificato;
- l'accettazione, il rifiuto o altre procedure delle domande, le richieste di Certificato, richieste di revoca, di recupero o di rinnovo, o le informazioni di enrollment;
- il rilascio o la revoca dei certificati, compresi il personale che ha accesso a parti riservate della repository;
- il trattamento delle informazioni o richieste di sottoscrizione
- la generazione, l'emissione o la distruzione di un certificato CA
- il caricamento di un CA in un ambiente di Produzione

5.3 Controlli Relativi al Personale

Il personale che ambisca a diventare Trusted deve mostrare prova dei requisiti, le qualifiche, e l'esperienza necessarie per adempiere alle proprie responsabilità lavorative con competenza e soddisfazione, così come la prova di nulla osta del governo, se del caso, necessari per svolgere i servizi di certificazione in base ai contratti governativi. I controlli di background verranno ripetuti almeno ogni 5 anni sul personale in possesso dei requisiti di attendibilità.

5.3.1 Qualifiche, Esperienza e Requisiti per l' Accesso

Il personale che ambisca a diventare "Trusted" deve dare prova di possedere requisiti, qualifiche, ed esperienza necessari per adempiere alle proprie responsabilità lavorative con competenza e soddisfazione, così come la prova di nulla osta del governo, se del caso, necessari per svolgere i servizi di certificazione in base ai contratti governativi.

5.3.2 Procedure Controllo Background

Prima dell'inizio dell'attività professionale in un Ruolo Fiduciario, Trust Italia S.p.A. svolgerà controlli di background, inclusi gli elementi seguenti:

- conferme dei precedenti rapporti di lavoro,
- controllo delle referenze professionali,
- conferma del diploma formativo più alto o più importante ottenuto dal candidato,
- controllo d ella fedina penale (locale, regionale e nazionale),
- controllo di documentazione di credito/finanziaria,
- controllo sulla patente di guida.

Nella misura in cui uno o più dei requisiti specificati nel presente paragrafo non possano essere soddisfatti per via di un divieto o di una restrizione previsto dalle leggi locali o da altre circostanze, Trust Italia S.p.A. utilizzerà una tecnica di controllo sostitutiva (e permessa ai sensi di legge) che fornisca informazioni sostanzialmente similari, ivi incluso (a titolo esemplificativo e non esaustivo) un controllo di background svolto dall'ente governativo competente.

Gli elementi riscontrati in un controllo di background che potrebbero dare luogo ad un rifiuto dei candidati alle Posizioni Fiduciarie o anche all'adozione di misure contro una Persone Fiduciaria in carica includono quanto segue:

- false dichiarazioni rese dal candidato o dalla Persona Fiduciaria,
- referenze personali altamente sfavorevoli o non affidabili,
- condanne penali accertate, e
- elementi indicanti una mancanza di responsabilità in materia finanziaria.

5.3.3 Requisiti relativi alla Formazione

Trust Italia S.p.A. fornisce al proprio personale dei corsi di formazione al momento dell'assunzione nonché l'addestramento sul posto di lavoro necessario per uno svolgimento competente e soddisfacente delle mansioni del personale. Trust Italia S.p.A. verifica e migliora i propri programmi di formazione periodicamente secondo necessità. I programmi di formazione di Trust Italia S.p.A. sono adattati alle responsabilità del singolo ed includono gli elementi seguenti (nella misura applicabile):

- concetti basilari sul PKI,
- responsabilità professionali,
- policy e procedure di Trust Italia S.p.A. relative alle sicurezza ed alle operazioni,
- utilizzo e funzionamento dell'hardware e software impiegato,
- gestione e relazioni su incidenti e Compromissioni, e
- procedure relative a disaster recovery e continuità di funzionamento.

5.3.4 Frequenza e Requisiti di Aggiornamento

Trust Italia S.p.A. offre corsi di aggiornamento al proprio personale nella misura e con la frequenza necessarie a garantire che il personale stesso mantenga il livello di competenza richiesto per svolgere le responsabilità professionale in modo competente e soddisfacente. Vengono inoltre organizzati dei corsi di formazione sicurezza a scadenze regolari.

5.3.5 Frequenza e Sequenza del Turnover Lavorativo

Non applicabile

5.3.6 Sanzioni per Atti non Autorizzati

In caso di atti non autorizzati o di altre violazioni delle policy e procedure di Trust Italia S.p.A. saranno decise le idonee misure disciplinare, che possono andare fino alla cessazione del rapporto e che saranno commisurate alla frequenza e gravità delle azioni non-autorizzate.

5.3.7 Requisiti per il Personale Esterno

In alcune circostanze limitate potranno essere chiamati collaboratori o consulenti esterni per ricoprire le Posizioni Fiduciarie. Tali collaboratori e consulenti dovranno soddisfare gli stessi criteri funzionali e di sicurezza applicabili agli impiegati di Trust Italia S.p.A. in posizioni analoghe.

I collaboratori e consulenti esterni che non hanno completato le procedure di controllo background come specificato al CPS § 5.3.2 potranno avere accesso alle strutture sicure di Trust Italia S.p.A. soltanto se vengono scortati e direttamente controllati da Persone Fiduciarie.

5.3.8 Documentazione Fornita al Personale

Trust Italia S.p.A. fornisce ai propri dipendenti la necessaria formazione ed altra documentazione necessaria per svolgere il proprio dovere con competenza, responsabilità ed in maniera soddisfacente.

5.4 Procedure di Registrazione degli Audit

5.4.1 Tipi di Eventi Registrati

Trust Italia S.p.A. manualmente o automaticamente registra i seguenti eventi significativi:

- Eventi del ciclo di vita della gestione chiavi CA, tra cui:
  - Creazione di chiavi, backup, archiviazione, recupero, mantenimento e distruzione
  - Eventi di gestione del ciclo di vita del Dispositivo crittografico
- Eventi di gestione del ciclo di vita del certificato CA ed abbonato, tra cui:
  - Richieste di Certificato, rinnovo, ricodifica e revoca
  - Elaborazione di successo o insuccesso delle richieste
  - Generazione e rilascio di certificati e CRL.

- Eventi legati alla sicurezza, tra cui:
  - Successo ed insuccesso nei tentativi di accesso al sistema PKI
  - PKI ed attività di sistema di sicurezza effettuate da personale Trust Italia S.p.A.
  - Sicurezza dei file sensibili o lettura documenti, scritti o cancellati
  - Modifiche al profilo di sicurezza
  - Crash di sistema, guasti hardware ed altre anomalie
  - Firewall e attività del router
  - Accesso agli ambienti CA entrata/ uscita.

Alla voce Log s'includono i seguenti elementi:

- Data e ora d' ingresso
- Numero di serie o sequenza di ingresso, delle voci automatiche giornaliere
- Identità del soggetto che effettua l'iscrizione giornaliera
- Tipo d' accesso.

Le RA e gli Amministratori Aziendali loggano alle informazioni sulle Richieste di Certificazione informazioni, tra cui:

- Tipo di documento di identificazione presentato dal richiedente il certificato
- Registrazione unica dei dati di identificazione, numeri, o una loro combinazione (ad esempio, il certificato del richiedente patente numero) dei documenti di identificazione, se del caso
- Percorso di archiviazione di copie di applicazioni e documenti di identificazione
- Identità del soggetto all'accettazione della domanda
- Metodo utilizzato per convalidare i documenti di identificazione, se del caso
- Nome della CA ricevente o della RA abbonata, se applicabile.

5.4.2 Frequenza dei Processing Log

I registri di controllo vengono esaminati almeno su base settimanale per significativi eventi legati alla sicurezza ed operativi. Inoltre, Trust Italia S.p.A. analizza i propri log di audit per attività sospette o anomale in risposta ad avvisi generati sulla base di irregolarità e incidenti sulla CA e nei sistemi della RA di Trust Italia S.p.A..

L' elaborazione degli audit sui log consiste in una rassegna di log di audit e la documentazione per tutti gli eventi significativi in un sommario del registro di controllo. Le revisioni sul registro di controllo comprendono una verifica che lo stesso non sia stato manomesso, l'ispezione di tutte le voci di registro, ed un'indagine di avvisi o irregolarità nei registri. Le azioni intraprese sulla base dell' audit dei log sono inoltre documentate.

5.4.3 Periodo di Conservazione del Registro di Controllo

Gli Audit log devono essere conservati in loco per almeno due (2) mesi dopo il trattamento e, successivamente archiviati in conformità con la sezione 5.5.2.

5.4.4 Protezione degli Audit Log

I registri di controllo sono protetti con un sistema elettronico di registro di controllo che include meccanismi per proteggere i file di registro da accessi non autorizzati, modifiche, cancellazioni, o altre manomissioni.

5.4.5 Procedure di backup degli Audit Log

I backup incrementali dei registri di controllo vengono creati ogni giorno mentre un backup completo è realizzato settimanalmente.

5.4.6 Sistema Raccolte Audit (Interno ed Esterno)

I dati automatizzati relativi alle verifiche vengono generati e registrati a livello di applicazioni, rete e sistema operativo. I dati sulle verifiche generati manualmente sono registrati dal personale di Trust Italia S.p.A..

5.4.7 Notifica al Soggetto che ha Causato un Evento

Quando il sistema di raccolta delle verifiche registra un evento, non è comunque necessario inviare una comunicazione all'individuo, organizzazione o dispositivo che ha causato l'evento stesso.

5.4.8 Valutazione di Vulnerabilità

Alcuni eventi nell'ambito del processo di verifica vengono registrati per monitorare la vulnerabilità del sistema. A seguito di un esame di tali eventi monitorati saranno svolte, esaminate e riviste delle valutazioni logiche della vulnerabilità del sistema di sicurezza ("LSVA"). Le LSVA si basano sui dati di registrazione automatizzati in tempo reale e saranno svolte giornalmente, mensilmente ed annualmente in conformità ai requisiti stabiliti della Guida ai Requisiti di Sicurezza e Revisione/Verifica. La LSVA annuale serve da input per la Verifica annuale di Conformità.

5.5 Archiviazione delle Registrazioni

5.5.1 Tipi di Eventi Registrati

Trust Italia S.p.A. archivia:

- Tutti i dati di controllo raccolti nei termini della sezione 5.4
- Informazioni sulle richieste di Certificazione
- Documentazione a supporto delle applicazioni del certificato
- Informazioni sul ciclo di vita del Certificato come ad es.: informazioni sulle applicazioni di revoca, ricodifica e rinnovo

5.5.2 Periodo di Conservazione per l'Archivio

Le registrazioni relative ad un determinato Certificato saranno conservate per il lasso di tempo minimo (qui di seguito specificato) a partire dalla data di scadenza o revoca del Certificato:

- Cinque (5) anni per Certificati di Classe 1,
- Dieci (10) anni e sei (6) mesi per Certificati di Classe 2 e Classe 3

5.5.3 Protezione degli Archivi

Trust Italia S.p.A. protegge le proprie registrazioni archiviate in modo tale che soltanto le Persone Fiduciarie abbiano accesso ai dati archiviati. I dati archiviati elettronicamente sono protetti contro la visione, modifica, cancellazione o altra manomissione non autorizzata mediante l'attuazione di controlli di accessi fisici e logici idonei. I supporti contenenti i dati di archivio e le applicazioni necessarie per poter elaborare tali dati vengono mantenuti in modo tale da garantire l'accesso ai dati archiviati per il periodo di tempo stabilito dal presente CPS.

5.5.4 Procedure per il Backup dell' Archivio

Trust Italia S.p.A. realizza un backup incrementale dell'archivio elettronico delle informazioni sui Certificati rilasciati ogni giorno, mentre un backup completo è realizzato settimanalmente. Le copie dei record su supporto cartaceo saranno conservate in altro luogo.

5.5.5 Requisiti per il Time-Stamping (Marca Temporale) delle Registrazioni

Certificati, CRL ed altre registrazioni contenute nei database relativi alle revoche includono informazioni su data ed ora. Tali informazioni temporali non richiedono una base crittografica

5.5.6 Sistema dell' Archivio di Raccolta (Interno o Esterno)

I sistemi di raccolta di repertorio di Trust Italia S.p.A. sono interni, fatta eccezione per i clienti RA aziendali. Trust Italia S.p.A. assiste le proprie RA nel preservare un audit trail. Tale sistema di raccolta archivio è quindi esterno a quello dell' RA aziendale.

5.5.7 Procedure per l' Ottenimento e la Verifica di Informazioni di Archivio

Solo il personale autorizzato di fiducia è in grado di ottenere l'accesso all'archivio. L'integrità delle informazioni si verifica quando viene ripristinato.

5.6 Sostituzione/ Conversione di Chiavi

Alla fine del loro rispettivo periodo massimo di vita le coppie di chiavi CA di Trust Italia S.p.A. vengono ritirate. I Certificati CA di Trust Italia S.p.A. possono essere rinnovati a condizione che il periodo complessivo certificato dalla coppia di chiavi CA non ecceda il limite massimo previsto per le coppie di chiavi CA. Le nuove coppie di chiavi CA saranno generate secondo necessità, ad esempio per sostituire coppie di chiavi CA che sono state ritirate, per integrare quelle coppia di chiavi esistenti ed attive nonché per supportare nuovi servizi.

Prima della scadenza del Certificato CA per una CA Superiore, saranno attuate le procedure di sostituzione/conversione chiavi per facilitare una transizione agevole (per le entità che si trovano nell'ambito gerarchico della CA Superiore) dalla vecchia coppia di chiavi CA Superiore alla/e nuova/e coppia/e di chiavi CA. Il processo per la sostituzione/conversione di chiavi CA di Trust Italia S.p.A. prevede quanto segue:

- Una CA Superiore cessa di rilasciare nuovi Certificati CA Subordinati entro sessanta giorni prima dalla data ("Data di Cessazione Rilasci") alla quale il periodo rimanente di validità della coppia di chiavi CA Superiore equivale al Periodo approvato di Validità del Certificato per il tipo o i tipi specifico/i di Certificati rilasciati dalle CA Subordinate nella gerarchia della CA Superiore.
- A seguito dell'esito positivo della convalida di domande per Certificati CA Subordinate (o di Abbonamento per utenti finali) ricevute dopo la Data di Cessazione Rilasci, i Certificati saranno firmati con una nuova coppia di chiavi.

La CA Superiore continua a rilasciare CRL firmate con la chiave privata CA Superiore originale fino alla data di scadenza dell'ultimo Certificato rilasciato con la coppia di chiavi originale.

5.7 Disaster Recovery e Compromissione Chiavi

5.7.1 Incidenza e Procedure di Gestione Compromissione

I backup delle informazioni sulla CA che seguono devono essere tenute in deposito fuori sede e messo a disposizione in caso di Compromissione o disastro: informazioni sulle Richieste di Certificato, dati di auditing, e record di database per tutti i certificati rilasciati. I Back-up di chiavi private delle CA devono essere generati e mantenuti in conformità con il CP § 6.2.4. Trust Italia S.p.A. mantiene i backup delle informazioni sulle proprie CA, così come per le Ca dei clienti aziendali all'interno del proprio suo sottodominio.

5.7.2 Corruzione di Risorse Computer, Software e/o Dati

Nel caso di una corruzione di risorse computer, software e/o dati, un tale avvenimento dovrà essere riferita al reparto sicurezza di Trust Italia S.p.A. perché possano essere messo in atto le procedure di Trust Italia S.p.A. per la gestione di incidenti. Tali procedure prevedono un'idonea gerarchizzazione, indagini e reazioni all'incidente avvenuto. Se necessario, saranno messe in atto le procedure di Trust Italia S.p.A. relative alla compromissione di chiavi o disaster recovery.

5.7.3 Procedure in caso di Compromissione Chiavi per Entità

A seguito di sospetta o accertata Compromissione di una CA Trust Italia S.p.A., infrastruttura VTN o chiave privata CA di un cliente, le procedure di risposta di Trust Italia S.p.A. sono emanate dal Trust Italia S.p.A. Security Incident Response Team (TISIRT). Questo team, che comprende personale di sicurezza, crittografia, Business Operations, Produzione dei servizi ed altri rappresentanti del management Symantec, valuta la situazione, sviluppa ed implementa il piano d'azione con l'autorizzazione dell'esecutivo di Trust Italia S.p.A..

Se si richiede una revoca di certificato CA, vengono eseguite le seguenti procedure:

- Lo stato di revoca Certificato viene trasmesso alle Parti Facenti Affidamento attraverso la Trust Italia S.p.A. Repository in base al CPS § 4.9.7,

- In termini commerciali sarà fatto un ragionevole sforzo per fornire ulteriore avviso di revoca a tutti i partecipanti interessati al VTN, e
- La CA genera una nuova coppia di chiavi in conformità con il CPS § 5.6, a meno che la CA non sia cessata in base al CPS § 5.8.

5.7.4 Capacità di Business Continuity a seguito di Disastro

Symantec ha realizzato un sito per disaster recovery ad oltre 1.000 chilometri dal principale Centro di Elaborazione sicuro di Symantec. Symantec ha sviluppato, applicato e testato un piano di disaster recovery per mitigare gli effetti di ogni tipo di calamità naturale o provocata dall'uomo. Questo piano è regolarmente testato, verificato e aggiornato per essere operativo in caso di calamità.

Dettagliati piani di disaster recovery sono in atto per affrontare il ripristino dei servizi dei sistemi informativi e delle funzioni aziendali chiave. Il luogo del Disaster Ricovery di Symantec ha attuato le protezioni di sicurezza fisica e controlli operativi richiesti dalla Guida Symantec Security and Audit Requirements (SAR) per fornire una operativa e sicura configurazione di backup.

In caso di catastrofi naturali o provocate dall'uomo che richiedano la cessazione temporanea o permanente delle operazioni dalla sede centrale Symantec, il processo di disaster recovery viene avviato dal Symantec Emergency Response Team (SERT).

Symantec ha le capacità per ristabilire o ripristinare le proprie operazioni entro ventiquattro (24) ore dopo un disastro di modo da poter supportare – quanto meno – le funzioni seguenti:
- rilascio Certificati,
- revoca Certificati,
- pubblicazione di informazioni sulle revoche, e
- fornitura di informazioni sul recupero chiavi per i Clienti Managed PKI che utilizzano il Gestore Chiavi Managed PKI.

Il database per disaster recovery di Symantec è sincronizzato regolarmente con il database di produzione per un periodo di tempo maggiore di quelli stabiliti nella Guida sui Requisiti di Sicurezza e Revisione. Le strutture Symantec per disaster recovery sono protette da sistemi di sicurezza fisica paragonabili ai livelli di sicurezza fisica specificati al CPS § 5.1.1.

Il piano di disaster recovery Symantec è stato progettato per fornire pieno recupero entro una settimana dopo il verificarsi di un disastro presso la struttura primaria di Symantec. Symantec testa il suo equipaggiamento presso il proprio sito primario per supportare non solo le funzioni di tutte le CA / RA, ma una catastrofe che potrebbe rendere inutilizzabile l'intero impianto. I risultati di tali test sono esaminati e tenuti ai fini del controllo e della pianificazione. Dove possibile, le operazioni sono riprese presso il sito principale di Symantec appena possibile a seguito di grave catastrofe.

Symantec gestisce hardware ridondanti e backup del proprio sistema di CA e del software di infrastruttura nel suo stabilimento di disaster recovery. Inoltre, le chiavi private CA sono sostenute e mantenute per il disaster recovery in conformità con CPS § 6.2.4.

Symantec gestisce backup offsite di importanti informazioni di CA per le CA Symantec così come le CA di centri di servizio e clienti aziendali, all'interno del Sottodominio Symantec. Tali informazioni comprendono, e non soltanto: Informazioni di richiesta Certificato, dati di auditing (per sezione 4.5) e record dei database per tutti i certificati rilasciati.

5.8 Cessazione della CA o RA

Nel caso si rendesse necessario per una CA Trust Italia S.p.A. o una CA Cliente Managed PKI di cessare le proprie operazioni, Trust Italia S.p.A. farà quanto commercialmente ragionevole per informare gli Abbonati, le Parti Facenti Affidamento ed altre entità interessate di tale cessazione prima dell'inizio della stessa. Quando si rende necessaria la cessazione di una CA, Trust Italia S.p.A. e, nel caso di una CA Cliente, il relativo Cliente svilupperanno un piano di cessazione per minimizzare le discontinuità rispetto a Clienti, Abbonati e Parti Facenti Affidamento. Nel piano di cessazione possono essere determinati gli elementi seguenti (nella misura applicabile):

- notifica alle parti interessate dalla cessazione – quali Abbonati, Parti Facenti Affidamento e Clienti – con informazioni sullo stato della CA gestione dei costi di tali notifiche,
- revoca del Certificato rilasciato alla CA da parte di Trust Italia S.p.A.,
- mantenimento degli archivi e record della CA per i periodi di tempo stabiliti al CPS § 4.6,
- prosecuzione dei servizi agli Abbonati e di supporto-clienti,
- prosecuzione dei servizi di revoca, tra cui la pubblicazione di CRL o il mantenimento di servizi online per la verifica di stato,
- revoca di Certificati (non scaduti e non revocati) di Abbonati utenti finali e CA subordinate, se necessario,
- pagamento di un compenso (se del caso) a quegli Abbonati i cui Certificati non scaduti e non
- revocati sono revocati secondo quanto stabilito nel piano o procedura di cessazione oppure, in alternativa, rilascio di Certificati sostitutivi da parte di una CA subentrante,
- eliminazione della chiave privata della CA e degli elementi hardware che la contengono, e
- misure necessarie per la transizione dai servizi dalla CA ad una CA subentrante

6. Controlli Tecnici di Sicurezza

6.1 Generazione di Coppia di Chiavi ed Installazione

6.1.1 Generazione Coppia di Chiavi

La generazione di coppie di chiavi CA si realizza per mezzo di varie persone selezionate, addestrate e affidabili che si avvalgono di Sistemi e processi Attendibili a garanzia della sicurezza e della forza crittografica richiesta per le chiavi generate. Per le PCA e le CA Root, i moduli crittografici usati per la generazione di chiavi soddisfano in requisiti stabiliti al FIPS 140-1 livello 3. Per le altre CA (ivi incluse le CA Trust Italia S.p.A. e le CA dei Clienti Managed PKI), i moduli crittografici usati soddisfano per lo meno i requisiti stabiliti al FIPS 140-1 livello 2.
Tutte le coppie di chiavi CA sono generate nell'ambito di Procedure di Generazione Chiavi pre-progettate in conformità alle condizioni stabilite nella Guida di Riferimento per Procedura Chiavi, nella Guida Utente per gli Strumenti di Gestione Chiavi CA e nella Guida ai Requisiti di Sicurezza e Verifica. Le attività svolte nell'ambito di ogni procedura di generazione chiavi vengono registrate, datate e firmate da tutte le persone coinvolte. La relativa documentazione è conservata ai fini di verifica e tracciamento per un lasso di tempo ritenuto idoneo dal management di Trust Italia S.p.A..
In generale, la generazione di coppie di chiavi RA è svolta dalla RA con l'ausilio di un modulo crittografico certificato FIPS 140-1 livello 1 fornito con il software per il browser.
I Clienti Managed PKI generano la coppia di chiavi utilizzata dai loro server di Amministrazione Automatizzata. Trust Italia S.p.A. raccomanda di realizzare la generazione di coppie di chiavi per server di Amministrazione Automatizzata con un modulo crittografico certificato FIPS 140-1 livello 2.
La generazione di coppie di chiavi per Abbonati (utenti finali) viene di norma realizzata dall'Abbonato interessato. Per Certificati di Classe 1, Certificati di Classe 2 e Certificati per firma codice/oggetto di Classe 3, l'Abbonato userà di norma un modulo crittografico certificato FIPS 140- 1 livello 1 fornito con il browser software per la generazione chiavi. Per Certificati server, l'Abbonato di norma utilizzerà il programma per generazione chiavi fornito con il software per il web server.
Per applicazioni ACS IDTrust Italia S.p.A. genera una coppia di chiavi a nome dell'Abbonato utilizzando una semina di numeri casuali generati su un modulo crittografico che sia quanto meno conforme ai requisiti della FIPS 140-1 level 3.

6.1.2 Consegna della Chiave Privata all' Abbonato

Quando l' abbonato (utente finale) si genera la coppia di chiavi, la consegna della chiave privata ad un abbonato non è sostenibile. Per Applicazioni ACS ID, anche la consegna della chiave privata non è applicabile.
Quando Trust Italia S.p.A. pre-genera delle coppie di chiavi per RA o Abbonati (utenti finali) su elementi hardware o smart-card, questi dispositivi sono distribuiti alla RA o all'Abbonato (utente finale) mediante un servizio commerciale di consegna ed un imballaggio che evidenzia eventuali manomissioni. I dati di attivazione necessari per attivare il dispositivo sono comunicati alla RA o all'Abbonato (utente finale) mediante un processo "out of band". La distribuzione dei dispositivi viene annotata da Trust Italia S.p.A..

Qualora la coppia di chiavi dell'abbonato utente finale sia pre-generata da clienti aziendali su token hardware o smart card, tali dispositivi sono distribuiti all' abbonato (utente finale) utilizzando un servizio commerciale di consegna e ed un imballaggio che evidenzia eventuali manomissioni. I dati di attivazione necessari per attivare il dispositivo sono comunicati alla RA o all'Abbonato (utente finale) mediante un processo "out of band". La distribuzione dei dispositivi viene annotata dal cliente aziendale.
Per i Clienti Managed PKI che utilizzano il Gestore Chiavi Managed PKI per i servizi di recupero chiavi, il Cliente potrà generare coppie di chiavi per crittazione (per conto degli Abbonati le cui Richieste di Certificati siano state approvate) e trasmettono tali coppie di chiavi agli Abbonati mediante un file PKCS # 12 protetto da password.

6.1.3 Consegna della Chiave Pubblica all' Ente Certificatore

Gli Abbonati (utenti finali) e le RA sottopongono elettronicamente la loro chiave privata a Trust Italia S.p.A. (per la certificazione) per mezzo di un CSR (domanda di firma Certificato) PKCS#10 o un altro pacchetto a firma digitale nell'ambito di una sessione garantita da Secure Sockets Layer (SSL). Quando le coppie di chiavi CA, RA o Abbonato (utente finale) sono generate da Trust Italia S.p.A., la presente clausola non è applicabile.

6.1.4 Consegna Chiave Pubblica CA agli Utenti

Trust Italia S.p.A. mette i Certificati CA per le proprie PCA e CA Root a disposizione degli Abbonati e delle Parti facenti Affidamento attraverso la loro inclusione nel software di web browser Microsoft e Netscape. Quando si generano nuovi Certificati per PCA e CA Root, Trust Italia S.p.A. fornisce tali nuovi Certificati ai produttori di browser perché possano essere inclusi in nuove versioni e aggiornamenti dei browser.
In generale, al momento del rilascio Trust Italia S.p.A. fornisce l'intera catena di certificazione (ivi incluse la CA di origine e tutte le CA all'interno della catena) all'Abbonato (utente finale). I Certificati CA di Trust Italia S.p.A. possono anche essere scaricati dalla Directory LDAP di Trust Italia S.p.A. all'indirizzo: directory.trustitalia.it

6.1.5 Dimensioni delle Chiavi

Le coppie di chiavi devono essere di lunghezza sufficiente ad impedire ad altri di determinarne la chiave privata utilizzando crittoanalisi durante il periodo di utilizzo previsto di tali coppie di chiavi. La chiave Trust Italia S.p.A. di dimensioni Standard minime è l'utilizzo di coppie di chiavi equivalenti in forza alla RSA di 2048 bit per le PCA e le CA.
Le PCA Symantec (G1 e G2) di prima e seconda generazione hanno una coppia di chiavi a sono 1024 bit RSA mentre quelle di terza e quinta generazione (G3 e G5) sono a 2048 bit. La firma di tutte le Classi di Certificazione Symantec e Trust Italia S.p.A. che utilizzano coppie di chiavi RSA devono transitare sulle root con chiavi a dimensione non inferiore a 2048 bit (o equivalente) entro e non oltre il 31 Dicembre 2013. Symantec raccomanda l'utilizzo di chiavi con lunghezza minima a 2048 bit RSA per le coppie di chiavi delle RA e di utenti finali. Symantec e Trust Italia S.p.A. elimineranno gradualmente tutti i 1024-bit RSA entro il 31 Dicembre 2013.
La PCA di Classe 3 Symantec (ECC Universal Root CA) di quarta generazione (G4) include una chiave a 384 bit ECC.
Tutte le classi di certificati VTN, Trust Italia S.p.A., PCA, CA, RA e certificati di utenti finali utilizzano indistintamente come hash di firma digitale l'algoritmo SHA-1 o SHA-2 mentre alcune versioni del Symantec Processing Center supportano l'utilizzo dello SHA-256 e SHA-384 nei certificati per Abbonati utenti finali
Le dimensioni della chiave per i certificati con EV di Trust Italia S.p.A. sono identificati nell'appendice B2.

6.1.6 Generazione di Parametri per Chiavi Pubbliche e Controllo Qualità

Non applicabile

6.1.7 Finalità dell' Utilizzo della Chiave "Key Usage" (Come da campo X.509 v3)

Fare riferimento alla Sezione 7.1.2.1.

6.2 Protezione della Chiave Privata e Cryptographic Module Engineering Controls

Trust Italia S.p.A. ha messo in atto una combinazione di controlli fisici, logici e procedurali al fine di garantire la sicurezza delle chiavi private Trust Italia S.p.A. - Cliente Managed PKI. Gli abbonati sono contrattualmente obbligati a prendere le precauzioni necessarie per prevenire la perdita, divulgazione, modifica o l'uso non autorizzato delle chiavi private.

6.2.1 Standard per Moduli Crittografici

Per la generazione di coppie di chiavi per PCA e CA Root nonché per la memorizzazione di chiavi private CA, Trust Italia S.p.A. utilizza moduli crittografici hardware che sono certificati per o corrispondono essenzialmente al FIPS 140-1 Livello 3.

6.2.2 Controllo Multi-Persona (n di m) per Chiavi Private

Trust Italia S.p.A. ha messo in atto meccanismi tecnici e procedurali che prevedono la partecipazione di varie persone affidabili per lo svolgimento di operazioni crittografiche CA sensibili. Trust Italia S.p.A. si avvale della Suddivisione Segreta (Secret Sharing) per suddividere i dati di attivazione necessari per l'uso di una chiave privata CA in varie parti separate denominate "Secret Shares" detenute da persone addestrate ed affidabili denominate "Shareholder". Un numero minimo Secret Shares (m) del numero complessivo di Secret Shares create e distribuite per un determinato modulo crittografico (m) è necessario per attivare una chiave privata CA memorizzata nel modulo in questione.
Il numero minimo di parti necessarie a firmare una CA è 3. Si noti che il numero di parti distribuite per elementi di disaster recovery è minore del numero distribuito per elementi operativi, mentre il numero minimo di parti necessarie rimane uguale. Le Secret Shares sono protette secondo quanto previsto dal presente CPS.

6.2.3 Chiavi Private Depositate presso Terzi (Private Key Escrow)

Le chiavi private delle CA non sono depositate presso terzi. La custodia della chiave privata per utenti finali è spiegata in dettaglio nella sezione 4.12.

6.2.4 Backup della Chiave Privata

Trust Italia S.p.A. crea copie di backup delle chiavi private CA ai fini del recupero di routine e del disaster recovery. Tali chiavi sono memorizzate in forma criptata all'interno di moduli crittografici hardware e dei relativi dispositivi di memorizzazione chiavi. I moduli crittografici per la memorizzazione di chiavi private CA corrispondono ai requisiti del presente CPS. Le chiavi private CA sono copiate su moduli crittografici hardware di backup in conformità con questo CPS.
I moduli contenenti copie onsite di backup delle chiavi private CA sono soggetti ai requisiti stabiliti dal CPS. I moduli contenenti copie delle chiavi private CA per disaster recovery sono soggetti ai requisiti stabiliti dal presente CPS.
Trust Italia S.p.A. non memorizza copie delle chiavi private RA. Per quel che riguarda il backup di chiavi private di Abbonati (utenti finali), si veda la Sezione 6.2.3 e 4.12. Per le Applicazioni ID ACS, Trust Italia S.p.A. non conserva copie di chiavi private degli abbonati.

6.2.5 Archiviazione della Chiave Privata

Quando le coppie di chiavi CA di Trust Italia S.p.A. sono giunte alla scadenza del loro periodo di validità, tali coppie di chiavi saranno archiviate per un periodo di almeno 5 anni. Le coppie di chiavi CA archiviate saranno memorizzate in maniera sicura con l'ausilio di moduli crittografici hardware che soddisfano i requisiti del presente CPS. Tali coppie di chiavi CA non dovranno rientrare nell'uso produttivo dopo la scadenza del rispettivo Certificato a meno che il certificato CA non venga rinnovato in conformità al presente CPS.
Trust Italia S.p.A. non archivia copie delle chiavi private RA e di Abbonati.

6.2.6 Trasferimento della Chiave Privata in o da un Modulo Crittografico

Trust Italia S.p.A. genera coppie di chiavi CA sui moduli crittografici hardware nei quali le chiavi saranno utilizzate. Inoltre, Trust Italia S.p.A. realizza delle copie di queste coppie di chiavi CA ai fini del recupero di routine e del disaster recovery. Quando viene creato un backup della coppia di chiavi CA su un altro modulo crittografico hardware, le coppie di chiavi vengono trasportate da un modulo all'altro in forma criptata.

6.2.7 Deposito della Chiave Privata su Modulo Crittografico

Le chiavi private CA o RA devono essere conservate su moduli hardware crittografici in forma criptata.

6.2.8 Metodo di Attivazione della Chiave Privata

Tutti i Partecipanti al Sottodominio di Trust Italia S.p.A. dovranno proteggere i dati di attivazione per le loro chiavi private contro perdita, furto, modifica, divulgazione non autorizzata o uso non autorizzato.

Certificati di Classe 1

Lo Standard per la protezione di chiavi private di Classe 1 prevede che gli Abbonati adottino misure commercialmente ragionevoli per la protezione fisica della workstation dell'Abbonato al fine di prevenire l'utilizzo della workstation stessa e della chiave privata ad essa associata senza l'autorizzazione dell'Abbonato. Inoltre, Trust Italia S.p.A. raccomanda agli Abbonati di utilizzare una password in conformità al CPS § 6.4.1 o una misura egualmente potente per autenticare l'Abbonato prima dell'attivazione della chiave privata – come ad esempio una password necessaria per il funzionamento della chiave privata, una password per Windows log-on o salvaschermo o una password per accesso alla rete.

Certificati di Classe 2

Lo Standard per la protezione di chiavi private di Classe 2 prevede che gli Abbonati:

- usino una password in conformità al CPS § 6.4.1 o una misura egualmente potente per autenticare l'Abbonato prima dell'attivazione della chiave privata – come ad esempio una password necessaria per il funzionamento della chiave privata, una password per Windows log-on o salvaschermo, una password per accesso alla rete o una password in connessione al Servizio Roaming Trust Italia S.p.A.; e
- adottino misure commercialmente ragionevoli per la protezione fisica della workstation dell'Abbonato al fine di prevenire l'utilizzo della workstation stessa e della chiave privata ad essa associata senza l'autorizzazione dell'Abbonato.

Quando le chiavi private sono disattivate, dovranno essere mantenute soltanto in forma criptata.

Certificati di Classe 3 ad eccezione dei certificati di Amministratore

Lo Standard VTN per la protezione di chiavi private di Classe 3 (ad eccezione degli Amministratori) prevede che gli Abbonati:

- usino una smart-card, un altro dispositivo crittografica hardware, un dispositivo di accesso biometrico, una password (in connessione al Servizio Roaming Trust Italia S.p.A.) o una misura egualmente potente per autenticare l'Abbonato prima dell'attivazione della chiave privata; e
- adottino misure commercialmente ragionevoli per la protezione fisica della workstation dell'Abbonato al fine di prevenire l'utilizzo della workstation stessa e della chiave privata ad essa associata senza l'autorizzazione dell'Abbonato.

Si raccomanda l'uso di una password insieme ad una smart-card, un altro dispositivo crittografico hardware o dispositivo di accesso biometrico secondo quanto indicato al punto 6.4.1 Quando le chiavi private sono disattivate, dovranno essere mantenute soltanto in forma criptata.

Chiavi Private degli Amministratori (Classe 3)

Lo Standard per la protezione di chiavi private di Amministratori prevede che questi:

- usino una smart-card, un dispositivo di accesso biometrico o una password in conformità col punto 6.4.1 o una misura egualmente potente per autenticare l'Amministratore prima dell'attivazione della chiave privata – come ad esempio una password necessaria per il funzionamento della chiave privata, una password per Windows log-on o salvaschermo o una password per accesso alla rete; e
- adottino misure commercialmente ragionevoli per la protezione fisica della workstation dell'Amministratore al fine di prevenire l'utilizzo della workstation stessa e della chiave privata ad essa associata senza l'autorizzazione dell'Abbonato.

Si raccomanda l'uso di una password insieme ad una smart-card o un dispositivo di accesso biometrico secondo quanto indicato al punto 6.4.1 per autenticare l'Amministratore prima dell'attivazione della chiave privata.
Quando le chiavi private sono disattivate, dovranno essere mantenute soltanto in forma criptata.

Amministratori Managed PKI che utilizzano un Modulo Crittografico (con Amministrazione Automatizzata o con Servizio Gestore Chiavi Managed PKI)

Lo Standard VTN per la protezione di chiavi private di Amministratori che utilizzano un tale modulo crittografico prevede che questi:

- usino il modulo crittografico insieme ad una password ed in conformità al CPS § 6.4.1 per autenticare l'Amministratore prima dell'attivazione della chiave privata; e
- adottino misure commercialmente ragionevoli per la protezione fisica della workstation che contiene il lettore del modulo crittografico al fine di prevenire l'utilizzo della workstation stessa e della chiave privata ad associata al modulo crittografico senza l'autorizzazione dell'Amministratore.

Chiavi Private Conservate nel Processing Center (Classe 1-3)

Una chiave privata CA online dovrà essere attivata quando un numero minimo prestabilito di Titolari fornisce i rispettivi dati di attivazione (conservata in canali sicuri) come stabilito al punto 6.2.2. Una volta attivata, la chiave privata CA potrà essere attiva per un periodo indefinito fino a che la CA sarà messa offline. Un numero minimo prestabilito di Titolari saranno tenuti a fornire i loro dati di attivazione per attivare una chiave privata CA offline. Una volta attivata, la chiave privata sarà attiva soltanto per una volta.

6.2.9 Metodo per la Disattivazione della Chiave Privata

La chiavi private CA di Trust Italia S.p.A. sono disattivate al momento della loro rimozione dal lettore elementi. Le chiavi private RA di Trust Italia S.p.A. (usate per l'autenticazione della richiesta RA) sono disattivate al momento dello scollegamento del sistema. Le RA di Trust Italia S.p.A. sono tenute a scollegare le loro workstation quando lasciano la loro area di lavoro.
Le chiavi private di Amministratori Clienti, RA ed Abbonati (utenti finali) possono essere disattivate dopo ogni operazione al momento della sconnessione del sistema o della rimozione della smart-card dal suo lettore, a seconda del meccanismo di autenticazione impiegato dall'utente. In tutti i casi gli Abbonati (utenti finali) sono tenuti a proteggere adeguatamente le loro chiavi private in conformità con il presente CPS. La chiave privata associata all'Applicazione ACS ID viene immediatamente cancellata dopo l'utilizzo del code signing.

6.2.10 Metodo di Distruzione della Chiave Privata

Ove richiesto, Trust Italia S.p.A. distruggerà le chiavi private CA in modo tale da garantire in misura ragionevole che non esistano residui della chiave che potrebbero portare ad una ricostruzione della stessa. Trust Italia S.p.A. utilizza la funzione "azzeramento" dei propri moduli crittografici hardware ed altri strumenti idonei a garantire la completa distruzione delle chiavi private CA. Le attività di distruzione chiavi saranno registrate al loro svolgimento. La chiave privata associata all'Applicazione ACS ID viene immediatamente cancellata dopo l'utilizzo del code signing.

6.2.11 Valutazione del Modulo Crittografico

Si veda la Sezione 6.2.1

6.3 Ulteriori Aspetti della Gestione della Coppia di Chiavi

6.3.1 Archiviazione della Chiave Pubblica

I Certificati CA Trust Italia S.p.A., RA e degli Abbonati (utenti finali) saranno copiati in backup ed archiviati nell'ambito delle normali procedure di backup di Trust Italia S.p.A..

6.3.2 Periodi di Utilizzo per le Chiavi Pubbliche e Private

Il Periodo Operativo di un Certificato termina al momento della sua scadenza o revoca. Il Periodo Operativo di una coppia di chiavi è uguale a quello del relativo Certificato, salvo il fatto che la chiavi private potranno ancora essere usate per la decriptazione e le chiavi pubbliche potranno ancora essere usate per la verifica delle firme. I Periodi Operativi massimi per Certificati Trust Italia S.p.A. rilasciati a partire dall'entrata in vigore del presente CPS sono indicati alla Tabella 8 che segue. I certificati per gli utenti finali di rinnovi di certificati esistenti possono avere un periodo di validità più lungo (fino a 3 mesi).

Inoltre, le CA di Trust Italia S.p.A. cessano di rilasciare nuovi Certificati ad una data adeguata precedente alla scadenza del Certificato CA di modo che nessun Certificato rilasciato da una CA Subordinata possa venire a scadenza dopo la scadenza dei Certificati CA Superiori.

Certificato Rilasciato da:	***Periodo di Validità***
PCA self-signed (1024 bit RSA)	Fino a 30 anni
PCA self-signed (2048 bit RSA)	Fino a 50 anni
PCA self-signed (256 bit ECC)	Fino a 30 anni
PCA self-signed (384 bit ECC)	Fino a 30 anni
PCA a CA Intermedia Off-line	Generalmente 10 anni ma fino a 15 anni in seguito a rinnovo
PCA a CA on-line	Generalmente 5 anni ma fino a 10 in seguito a rinnovo[14]
CA Intermedia Off-line a CA On-line	Generalmente 5 ma fino a 10 anni in seguito a rinnovo[15]
CA On-line ad Abbonato individuale utente finale	Di norma fino a 2 anni, ma anche fino a 5 anni alle condizioni di seguito indicate[16]
CA On-line ad Abbonati entità finali organizzative	Di norma fino a 3 anni[17][18]

Tabella 8 - Periodi di Operatività del Certificato

Salvo quanto indicato nel presente paragrafo, i Partecipanti al Sottodominio di Trust Italia S.p.A. porranno fine ad ogni uso delle loro coppie di chiavi dopo la scadenza dei rispettivi periodi di utilizzo.
I Certificati rilasciati dalle CA agli Abbonati (utenti finali) potranno avere Periodi Operativi maggiori ai due anni e fino a cinque anni se ricorrono le condizioni seguenti:

- i Certificati sono Certificati individuali,
- le coppie di chiavi degli Abbonati sono residenti su un elemento hardware (ad es. una smart- card),
- gli Abbonati sono tenuti annualmente a sottoporsi alle procedure di ri-autenticazione almeno ogni 25 mesi come previsto al § 3.2.3,
- gli Abbonati forniranno ogni anno prova del loro possesso della chiave privata corrispondente alla chiave pubblica nel Certificato almeno ogni 25 mesi come previsto al § 3.2.3
- se un Abbonato non è in grado di completare le procedure di ri-autenticazione ai sensi di quanto suddetto con esito positivo, o non è in grado di provare il possesso della chiave privata, la CA revocherà automaticamente il Certificato dell'Abbonato in questione.

Trust Italia S.p.A. gestisce altresì una serie di CA root auto-firmate ed obsolete che fanno parte del VeriSign Trust Network. I Certificati di Abbonamento per utenti finali rilasciati da tali CA soddisfano i requisiti per i Certificati CA a Abbonati (utenti finali) come indicati nella Tabella 18 che precede. I requisiti stabiliti per queste CA sono specificati nella Tabella 8 che segue.

6.4 Attivazione dei Dati

6.4.1 Attivazione Generazione Dati ed Installazione

I dati di attivazione (Secret Shares) impiegati per proteggere gli elementi contenenti le chiavi private di Trust Italia S.p.A. vengono generati in conformità ai requisiti del CPS § 6.2.2 ed alla Key Ceremony Reference Guide. La creazione e distribuzione di Secret Share viene registrata.
Le RA di Symantec sono tenute a scegliere delle password potenti a protezione delle loro chiavi private. Le linee-guida Symantec per la selezione delle password prevede che tali password:

- siano generate dall'utente;

[14] Il certificato CA di Amministratore VeriSign® Onsite di Classe 3 ha validità oltre i 10 anni per supportare sistemi obsolete e verrà revocato secondo opportunità

[15] Se vengono emessi certificati da abbonato utente finale di 5 anni, il periodo operativo della CA sarà di 10 anni senza possibilità di rinnovo. Passati i 5 anni verrà richiesta la ri-generazione delle chiavi.

[16] Se vengono emessi certificati da abbonato utente finale di 5 anni, il periodo operativo della CA sarà di 10 anni senza possibilità di rinnovo. Passati i 5 anni verrà richiesta la ri-generazione delle chiavi.

[17]

[18] I Certificati Organizzativi per entità finali utilizzati esclusivamente per supportare operazioni di una parte del VTN potranno essere emessi con validità di 5 anni e fino ad un Massimo di 10 anni successivamente al rinnovo.

- abbiano almeno otto caratteri;
- abbiano almeno un carattere alfabetico ed uno numerico;
- abbiano almeno un carattere minuscolo;
- non contengano lo stesso carattere troppe volte;
- non siano le stesse del nome-profilo dell'operatore; e
- non contengano una lunga sequenza di caratteri tratta dal nome-profilo dell'utente.

Trust Italia S.p.A. decisamente raccomanda agli Amministratori Managed PKI, alle RA ed agli Abbonati (utenti finali) di scegliere delle password che corrispondano ai requisiti suindicati. Trust Italia S.p.A. raccomanda inoltre l'impiego di meccanismi di autenticazione a due fattori (ad es. contrassegno e password, biometrica e contrassegno o biometrica e password) per l'attivazione delle chiavi private.

6.4.2 Protezione dei Dati di Attivazione

I Titolari di Trust Italia S.p.A. sono tenuti a proteggere le loro Parti Segrete ed a firmare un accordo in cui prendono atto delle loro responsabilità in quanto Titolari.
Le RA di Trust Italia S.p.A. sono tenute a memorizzare le loro chiavi private Amministratore/RA in forma criptata mediante una protezione con password e l'opzione "high security" del loro browser.
Trust Italia S.p.A. decisamente raccomanda agli Amministratori Clienti, alle RA ed agli Abbonati (utenti finali) di memorizzare le loro chiavi private in forma criptata e di proteggerle mediante un contrassegno hardware e/o una potente password. Si incoraggia inoltre l'impiego di meccanismi di autenticazione a due fattori (ad es. contrassegno e password, biometrica e contrassegno o biometrica e password).

6.4.3 Altri aspetti relativi ai Dati di Attivazione

Trasmissione Dati di Attivazione

Nella misura in cui i dati di attivazione per chiavi private vengono trasmessi, i partecipanti al VTN devono proteggere la trasmissione utilizzando metodi contro perdita, furto, modifica, divulgazione non autorizzata o uso non autorizzato di tali chiavi private. Nella misura in Windows o nome di rete di accesso di utente / password combinazione viene utilizzato come dati di attivazione per un utente finale di sottoscrizione, le password trasferiti attraverso una rete devono essere protetti contro l'accesso da parte di utenti non autorizzati.

Distruzione Dati di Attivazione

I dati di attivazione per chiavi private CA sono eliminati con metodi contro perdita, furto, modifica, divulgazione non autorizzata o uso non autorizzato delle chiavi private protette da tali dati di attivazione. Superati i termini di conservazione dati scaduti come da sezione 5.5.2, Trust Italia S.p.A. dovrà disattivare i dati di attivazione tramite sovrascrittura e/o distruzione fisica.

6.5 Controlli di Sicurezza Computer

Trust Italia S.p.A. svolge tutte le funzioni CA e RA mediante Sistemi Attendibili conformi a quanto stabilito dalla Guida Symantec SAR. I Clienti Managed PKI devono utilizzare Sistemi Attendibili.

6.5.1 Requisiti Tecnici Specifici di Sicurezza Computer

Trust Italia S.p.A. assicura che i sistemi contenenti software CA e file-dati sono Sistemi Attendibili garantiti contro un accesso non autorizzato. Inoltre, Trust Italia S.p.A. limita l'accesso ai server di produzione a quelle persone che hanno un valido motivo lavorativo per un tale accesso. I normali utenti delle applicazioni non hanno account sui server di produzione.
La rete di produzione di Trust Italia S.p.A. è separata in maniera logica da altre componenti. Tale separazione impedisce l'accesso alla rete senza le procedure di applicazione pre-definite. Trust Italia S.p.A. utilizza firewall per proteggere la rete di produzione da intrusioni sia interne che esterne e per limitare il tipo e l'origine di attività di rete che possano dare accesso ai sistemi di produzione.
Trust Italia S.p.A. richiede l'uso di password che abbiano un numero minimo di caratteri ed una combinazione di caratteri alfanumerici e speciali. Trust Italia S.p.A. stabilisce che le password siano cambiate regolarmente.

L'accesso diretto ai database di Trust Italia S.p.A. che supportano l'archivio di Trust Italia S.p.A. è limitato alle Persone Fiduciarie facenti parte del gruppo operativo di Trust Italia S.p.A. e che hanno un valido motivo lavorativo per tale accesso.

6.5.2 Classificazione Sicurezza Computer

Una versione del software Symantec's core Processing Center ha soddisfatto i requisiti di garanzia EAL 4 di ISO/IEC 15408-3:1999 - Tecnologica informatica – Tecniche di sicurezza – Criteri di valutazione per la sicurezza di sistemi informatici – Parte Terza: Requisiti garanzia sicurezza, sulla base della valutazione di un ente indipendente (con i Criteri Comuni) del software rispetto all'Obiettivo di Sicurezza del Processing Center Symantec. Symantec potrà di volta in volta valutare le nuove versioni del software per il Processing Center sulla base dei Criteri Comuni.

6.6 Controlli Tecnici di Ciclo Vitale

6.6.1 Controlli Sviluppo Sistema

Le applicazioni sono sviluppate e realizzate da Trust Italia S.p.A. in conformità ai propri standard per sviluppo sistema e gestione variazioni. Trust Italia S.p.A. inoltre fornisce software ai suoi Clienti Managed PKI per lo svolgimento di funzioni RA e di determinate funzioni CA. Tale software è sviluppato in conformità agli standard di Trust Italia S.p.A. per sviluppo sistema.
Al primo caricamento del software sviluppato da Symantec, questo software fornisce un metodo per verificare che venga effettivamente da Symantec o da Trust Italia S.p.A., che non sia stato modificato prima dell'installazione e che si tratti della versione da utilizzare.

6.6.2 Controlli Gestione Sicurezza

Trust Italia S.p.A. ha attuato dei meccanismi e/o delle policy per controllare e monitorare la configurazione dei propri sistemi CA. Trust Italia S.p.A. crea una hash di tutti i pacchetti software Trust Italia S.p.A. e degli aggiornamenti degli stessi, che sarà utilizzata per verificare manualmente l'integrità del software. Trust Italia S.p.A. convalida l'integrità dei propri sistemi CA sia al momento dell'installazione che a intervalli regolari.

6.6.3 Classificazione Sicurezza del Ciclo Vitale

Nessuna pattuizione

6.7 Controlli Sicurezza Rete

Trust Italia S.p.A. esegue tutte le sue funzioni di CA e RA utilizzando reti protette in conformità con la Guida RAS Symantec per prevenire l'accesso non autorizzato e altre attività dannose. Trust Italia S.p.A. protegge le proprie comunicazioni di dati sensibili attraverso l'uso di firme digitali e di cifratura.

6.8 Time-Stamping (Marcatura Temporale)

Certificati, CRL ed altre voci sul database relative alla revoca devono contenere ora e data. Tali indicazioni temporali non devono obbligatoriamente essere su base crittografica.

7. Profilo Certificati e CRL

7.1 Profilo Certificati

Ad eccezione dei Certificati WTLS, i Certificati di Trust Italia S.p.A. sono conformi a (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, Giugno 1997; nonché (b) RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Aprile 2002 ("RFC 3280").

I Certificati X.509 contengono quanto meno i campi di base nonché i valori prescritti o le restrizioni indicate nella Tabella 9 che segue:

Campo	*Valore o Limitazioni di Valore*
Serial Number	Valore unico per DN di emissione
Algoritmo firma	Nome dell'algoritmo usato per firmare il Certificato (vedere CPS § 7.1.3) Object identifier of the algorithm used to sign the certificate (See CP § 7.1.3)
DN di missione	Vedere CPS § 7.1.4
Valido dal	Ora Coordinata Universale sincronizzata sull'orologio dell'Osservatorio Navale Americano. Codificata secondo la RFC 3280.
Valido al	Ora Coordinata Universale sincronizzata sull'orologio dell'Osservatorio Navale Americano. Codificato secondo la RFC 3280.
DN Soggetto	Vedere CPS § 7.1.4
Subject Public Key	Codificata in conformità alla RFC 3280.
Firma	Generata e codificata in conformità alla RFC 3280.

Tabella 9 - Campi Essenziali del Profilo Certificati

7.1.1 Numero/i Versione

I Certificati Trust Italia S.p.A. sono di tipo X.509 Versione 3 sebbene ad alcune Root di certificazione sia permessa la Versione 1 per supportare sistemi ereditati. I certificati CA devono essere X.509 Versione 1 o Versione 3. I certificati per Abbonati utenti finali devono essere X.509 Versione 3.

7.1.2 Estensioni di Certificati

Quando vengono utilizzati Certificati X.509 Version 3, Trust Italia S.p.A. popola i Certificati con le estensioni previste al CPS §§ 7.1.2.1-7.1.2.8. Le estensioni private sono ammesse a condizione che il loro utilizzo sia conforme al CP ed al presente CPS se non specificatamente inclusi mediante riferimento.

Key Usage

I Certificati X.509 Versione 3 sono generalmente popolati in conformità con l' RFC 3280: Internet X.509 Public Key Infrastructure Certificate e CRL Profile, aprile 2002. Le estensioni KeyUsage nei Certificati X.509 Versione 3 sono in genere configurati in modo da impostare e liberare i bit ed il campo di criticità in conformità con la tabella 10. Il campo di criticità dell'estensione KeyUsage è generalmente impostato su VERO per i certificati di CA e può essere impostato su VERO o FALSO per certificati di abbonamento per enti finali.

		CA	*Classe 1 e Classe 2 Abbonati utenti finali*	*Amministrazione Automatizzata dei token e dei Classe 2-3 di Abbonati (utenti finali)*	*Firma a Coppia di Chiavi Duale (Gestore Chiavi Managed PKI)*	*Cifratura a Coppia di Chiavi Duale (Gestore Chiavi Managed PKI)*
Criticità		***VERO***	***FALSO***	***FALSO***	***FALSO***	***FALSO***
0	Firma Digitale	Non Impostato	Impostato	Impostato	Impostato	Non Impostato
1	Non- Ripudio	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato
2	Cifratura Chiavi	Non Impostato	Impostato	Impostato	Non Impostato	Impostato
3	Cifratura Dati	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato
4	Concordanza Chiavi	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato
5	Key CertSign	Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato
6	CRL Sign	Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato
7	Solo Cifratura	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato
8	Solo Decifratura	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato

Tabella 10 - Impostazioni per l' Estensione Key Usage

Nota: Non è necessario impostare il non-ripudio del bit[19] in questi certificati poiché l'industria PKI non ha ancora raggiunto un consenso su ciò che il non ripudio del bit significhi. Fino a quando non si giunga a tale consenso, il non-ripudio del bit non potrà essere significativo per le potenziali Parti Facenti Affidamento.

[19] Il Non-Ripudio del bit può anche riferirsi al Content Commitment nei Certificati Digitali in conformità allo standard X.509.

Inoltre, le applicazioni più comunemente utilizzate non sempre rispettano il non-ripudio del bit. Pertanto, l'impostazione del bit potrebbe non aiutare le Parti Facenti Affidamento a prendere con fiducia una decisione. Di conseguenza questo CPS non richiede che il non-ripudio del bit venga impostato. Esso può essere impostato nel caso di Certificati a doppia coppia di chiavi di firma rilasciati attraverso la Managed PKI Key Manager, o come altrimenti richiesto. Le controversie relative al non ripudio derivanti dall'uso di un certificato digitale riguardano esclusivamente l'Abbonato e il/le Parti Facenti Affidamento. Symantec e Trust Italia S.p.A. non si assumono responsabilità a tale riguardo.

Estensione Policy di Certificazione

I Certificati di Abbonamento per utenti finali Trust Italia S.p.A. X.509 Versione 3 impiegano l'estensione Policy di Certificazione ("Certificate Policies"). Tale estensione è popolata con l'identificatore-oggetto applicabile per il CP VTN in conformità al CP § 7.1.6 ed alle previsioni del CP § 7.1.8. Il campo criticità di questa estensione è impostato su "FALSO".

Subject Alternative Name

L'estensione subjectAltName dei Certificati X.509 Versione 3 sono popolate in conformità con l'RFC 3280. Il campo criticità di questa estensione dovrà essere impostato su FALSO.

Vincoli di Base ("Basic Constraints")

Trust Italia S.p.A. popola i Certificati CA X.509 Versione 3 con un'estensione "BasicConstraints" dove il Tipo Soggetto è impostato su CA. I Certificati di Abbonamento per utenti finali sono anch'essi popolati con un'estensione BasicConstraints dove il Tipo Soggetto è impostato su Entità Finale. La criticità di questa estensione dovrà essere impostata su VERO per i Certificati CA, altrimenti su FALSO.
I Certificati CA X.509 Version 3 di Trust Italia S.p.A. hanno un campo "pathLenConstraint" dell'estensione BasicConstraints impostato sul numero massimo di certificati CA che possono seguire al Certificato stesso in un percorso di certificazione. Certificati CA rilasciati alle CA online di Clienti Managed PKI, che rilasciano Certificati di Abbonamento ad utenti finali, hanno un campo "pathLenConstraint" impostato sul valore "0" il che sta ad indicare che nel percorso di certificazione potrà seguire soltanto il Certificato di Abbonamento per utente finale.

Extended Key Usage

Trust Italia S.p.A. utilizza l'estensione ExtendedKeyUsage per i tipi specifici di Certificati X.509 Versione 3 di Trust Italia S.p.A. elencati alla Tabella 11 che segue. Trust Italia S.p.A. non utilizza l'estensione ExtendedKeyUsage per altri tipi di Certificati.

Tipologia di Certificato	**Tipologia di Certificato**
Certification Authority (CA)	Classe 3 International Server CA
OCSP Responder	Classe 1-3 Public Primary OCSP Responders Secure Server OCSP Responder
Certificati di Classe 3 Web Server	ID Secure Server ID Global Server
Authenticated Content Signing Certificates (ACS)	Authenticated Content Signing Certificates
Individual Certificates	Certificati Individuali di Classe 1 Certificati Individuali di Classe 2

Tabella 11 – Certificati che utilizzano l' Extended Key Usage

Per tali Certificati, Trust Italia S.p.A. popola l'estensione ExtendedKeyUsage come da tabella 12.

	International Server CA Classe 3	**Responder OCSP**	**ID Secure Server**	**ID Global Server**	**Contenuto Certificati di Firma Autenticata**	**Certificati Individuali di Classe 1 e 2**
Criticality	***FALSO***	***FALSO***	***FALSO***	***FALSO***	***FALSO***	***FALSO***
ServerAuth (autenticazione server)	Impostato	Non Impostato	Impostato	Impostato	Non Impostato	Non Impostato
ClientAuth (autenticazione cliente)	Impostato	Non Impostato	Impostato	Impostato	Non Impostato	Impostato
CodeSigning (firma -codice)	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Impostato	Non Impostato

	International Server CA Classe 3	Responder OCSP	ID Secure Server	ID Global Server	Contenuto Certificati di Firma Autenticata	Certificati Individuali di Classe 1 e 2
EmailProtection (protezione e-mail)	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Impostato
ipsecEndSystem	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato
ipsecTunnel	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato
ipsecUser	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato
TimeStamping (Marcatura Temporale)	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato
OCSP Signing (firma OCSP)	Non Impostato	Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato
Microsoft Server Gated Crypto (SGC) OID: 1.3.6.1.4.1.311.10.3.3	Non Impostato	Non Impostato	Non Impostato	Impostato	Non Impostato	Non Impostato
Netscape SGC - OID: 2.16.840.1.113730.4.1	Impostato	Non Impostato	Non Impostato	Impostato	Non Impostato	Non Impostato
Symantec SGC Identifier for CA Certificates – OID: 2.16.840.1.113733.1.8.1	Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato	Non Impostato

Tabella 12 - Impostazioni per Estensione ExtendedKeyUsage

Punti di Distribuzione CRL

La maggior parte dei Certificati X.509 Versione 3 Secure Server ed i Certificati di CA Intermedie utilizzano l'estensione CRL Distribution Points contenente la URL del sito dove una Parte Facente Affidamento può trovare una CRL per verificare lo stato di un Certificato CA. Il campo criticità di questa estensione è impostato su FALSO.

Authority Key Identifier

Trust Italia S.p.A. popola l'estensione "Authority Key Identifier" dei Certificati di Abbonamento per utenti finali X.509 Versione 3 e Certificati di CA Intermedie. L'"Authority Key Identifier" è composta dalla hash SHA-1 a 160-bit della chiave pubblica della CA che ha rilasciato il Certificato. In caso contrario, l' estensione dell' Authority Key Identifier comprende il subject distinguished name e numero seriale della CA emittente. Il campo criticità di questa estensione è impostato su FALSO.

Subject Key Identifier

Quando Trust Italia S.p.A. popola i Certificati VTN X.509 Versione 3 con un'estensione "SubjectKeyIdentifier", viene generato l'identificatore-chiavi in base alla chiave pubblica del Soggetto del Certificato in accordo con uno dei metodi descritti nella RFC 3280. Quando si impiega tale estensione, il campo criticità di questa estensione è impostato su FALSO.

7.1.3 Identificatori Oggetti Algoritmo

I Certificati X.509 di Trust Italia S.p.A. sono firmati con i seguenti algoritmi.

- **sha256withRSAEncryption** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- **ecdsa-with-Sha384** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3}
- **sha-1WithRSAEncryption** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
- **md5WithRSAEncryption** OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}

Le firme sui Certificati prodotte con questi algoritmi devono essere conformi alla RFC 3279. Oppure ***1WithRSAEncryption*** o ***sha256WithRSAEncryption*** saranno usati oltre il ***md5WithRSAEncryption***[20].

7.1.4 Conformazione dei Nomi

Trust Italia S.p.A. popola i Certificati VTN con un Issuer e Subject Distinguished Name in conformità al CPS § 3.1.1.
Inoltre, Trust Italia S.p.A. potrebbe includere all'interno dei Certificati di Abbonamento un ulteriore campo Unità Aziendale contenente un'informazione nella quale si dichiara che le modalità di utilizzo del Certificato sono stabilite in una URL che è un rinvio al Contratto per Parte Facente Affidamento applicabile. Eventuali eccezioni alla clausola precedente saranno ammesse soltanto se le limitazioni di spazio, formattazione o interoperabilità rendono una tale Unità Aziendale impossibile da usare insieme all'applicazione per la quale il Certificato è destinato, o se un rimando al Contratto per Parte Facente Affidamento applicabile viene incluso nella politicy di estensione del certificato.

7.1.5 Restrizioni Relative ai Nomi

Nessuna pattuizione

7.1.6 Identificatore-Oggetto "Certificate Policy"

Quando si utilizza l'estensione "Certificate Policies", i Certificati contengono l'identificatore- oggetto per la Policy di Certificazione corrispondente alla relativa Classe di Certificati come stabilito al CP VTN § 1.2. Per quanto riguarda i Certificati obsoleti rilasciati prima della pubblicazione del CP VTN che includono l'estensione "Certificate Policies", tali Certificati fanno riferimento al CPS VTN.

7.1.7 Utilizzo dell' Estenzione Policy Constraints"

Nessuna pattuizione

7.1.8 Sintassi e Semantica dei Qualificatori di Policy

Trust Italia S.p.A. popola i Certificati VTN X.509 Versione 3 con un qualificatore di policy nell'ambito dell'estensione "CertificatePolicies". In genere, tali Certificati contengono un qualificatore-puntatore CPS che rinvia al Contratto per Parte Facente Affidamento applicabile o al CPS di Trust Italia S.p.A.. Inoltre, alcuni Certificati contengono un Qualificatore Avviso Utente che rinvia al Contratto per Parte Facente Affidamento applicabile.

7.1.9 Semantica di Elaborazione per l' Estensione "Critical Certificate Policies"

Nessuna pattuizione

7.2 Profilo CRL

Le CRL contengono quanto meno i campi e contenuti basilari specificati alla Tabella 13 che segue:

Campo	Valore o Limitazioni di Valore
Versione	Vedere la Sezione 7.2.1.
Algoritmo di Firma	Algoritmo utilizzato per firmare la CRL in conformità con la RFC 3279.
Issuer	Ente che firma e rilascia la CRL.
Data Effettiva	Data di emissione della CRL. Le CRL sono operative previo rilascio.
Aggiornamenti Successivi	Data in cui le successive CRL saranno emesse. La frequenza di emissione delle CRL è in conformità con i requisiti della Sezione 4.4.7.
Certificati Revocati	Lista dei certificate revocati, incluso il Serial Number del certificate revocato e la Data di Revoca.

Tabella 13 – Campi Essenziali del Profilo CRL

20 ***md5WithRSAEncryption*** viene utilizzato solo previo approvazione per preservare la continuità aziendale di applicazioni obsolete.

7.2.1 Numero/i Versione

Trust Italia S.p.A. supporta sia le CRL X.509 Versione 1 e Versione 2. Quest'ultime sono conformi ai requisiti della RFC 5280.

7.2.2 Estensioni CRL e CRL Entry

Nessuna pattuizione

7.3 Profilo OCSP

L' OCSP (Online Certificate Status Protocol) è un modo per ottenere informazioni tempestive sullo stato di revoca di un determinato certificato. Trust Italia S.p.A. convalida:

- Certificati Classe 2 Aziendali attestati OCSP Enterprise conformi alla RFC 2560, e
- Certificati di Classe 2 Aziendali e Certificati di Classe 3 Organizzativi che utilizzano il protocollo di validazione VeriSign ® Trusted Global (TGV), conforme alla RFC 5.019.

7.3.1 Numero Versione(i)

La Versione 1 della specifica dell' OCSP come definito dalla RFC 2560 e dalla RFC 5.019 sono supportate.

7.3.2 Estensioni OCSP

Il Servizio TGV utilizza time-stamp sicuri e periodo di validità per stabilire l' aggiornamento in tempo reale di ogni risposta OCSP. Trust Italia S.p.A. ad oggi non ne fa uso per stabilire l' aggiornamento in tempo reale di ogni risposta OCSP. Invece, i clienti dovrebbero adottare un sistema d'orologio interno per verificare l'aggiornamento in tempo reale di una risposta.

8. Conformità, Audit ed Altre Valutazioni

Un esame WebTrust annuale per Certification Authority (o equivalenti) viene eseguito sui data center operativi e sul key management Trust Italia S.p.A. che supportano i servizi pubblici e Managed PKI inclusi nella VTN Root CA, CA di Classe 3, Classe 2 organizzativi e CA individuali, Classe 1 e CA individuale di cui al punto 1.3.1. Determinate CA del cliente non sono specificamente verificate nell'ambito del controllo delle operazioni Trust Italia S.p.A. se non richiesto dal Cliente. Trust Italia S.p.A. potrebbe pretendere dai clienti Enterprise di sottoporsi ad un controllo di conformità ai sensi del presente CPS e dei programmi di controllo previsti per questa categoria di clienti.
In aggiunta alle verifiche di conformità, Trust Italia S.p.A. ha il diritto di eseguire le revisioni ed altre indagini per assicurare l'affidabilità del Sottodominio Trust Italia S.p.A. del VTN, che include, ma non si limita a:

- Trust Italia S.p.A. ha diritto, unicamente nella propria ed esclusiva discrezione, di effettuare in qualsiasi momento un "Exigent Audit / Investigation" su un cliente nel caso in cui Trust Italia S.p.A. abbia motivo di ritenere che l'ente sottoposto non sia riuscito a soddisfare gli Standard VTN, si sia verificato un incidente o compromissione, abbia agito o mancato di intervenire, in modo che il fallimento dell'ente oggetto della revisione, l'incidente o compromissione, l'atto o l'omissione, costituisca una minaccia reale o potenziale per la sicurezza o l'integrità del VTN.
- Trust Italia S.p.A. ha il diritto di eseguire un " Supplemental Risk Management Reviews " su un cliente in seguito a rilevamenti incompleti o eccezionali in un controllo di conformità o come parte del processo globale di gestione del rischio nel corso del normale svolgimento dell'attività.

Trust Italia S.p.A. ha il diritto di delegare l'esecuzione di tali controlli, recensioni, e le indagini di una società di revisione contabile del partito. Le entità che sono oggetto di una verifica, o indagine ha lo scopo ragionevole collaborazione con Trust Italia S.p.A. e il personale che esegue l', revisione contabile, o le indagini.

8.1 Frequenza e Circostanze di Valutazione

Verifiche di Conformità vengono effettuate almeno su base annuale a spese unicamente del soggetto sottoposto a revisione.

8.2 Identità/ Qualifiche del Valutatore

Le verifiche di conformità sulla CA Trust Italia S.p.A. sono eseguite da uno studio di revisione dei conti pubblici:

- Dimostri competenza in tecnologia di infrastrutture a chiave pubblica, strumenti di sicurezza informatica e tecnica, controlli di sicurezza, funzione di attestazione di terze parti
- È accreditato presso l'Albo dei Revisori Contabili

8.3 Relazioni del Revisore con Enti Valutati

Controlli di Conformità delle attività di Trust Italia S.p.A. vengono eseguiti da uno studio di contabilità pubblica indipendente da Trust Italia S.p.A..

8.4 Argomenti Trattati negli Assessment

Lo scopo del WebTrust annuale di Trust Italia S.p.A. per Certification Authority (o equivalente) di revisione comprende controlli ambientali sulle CA, operazioni di gestione chiavi e controllo Infrastrutture/ Amministrativo delle CA, il ciclo di vita del certificato e divulgazione delle procedure delle CA.

8.5 Azioni Intraprese in Seguito a Mancanze

In merito alle verifiche di conformità delle operazioni Trust Italia S.p.A., significative eccezioni o carenze riscontrate durante il controllo di conformità si tradurranno in una definizione di azioni da intraprendere. Questa determinazione è fatta dal management Trust Italia S.p.A. su input del revisore. Il Management Trust Italia S.p.A. è responsabile della gestione dello sviluppo e dell'attuazione di un piano di azioni correttive. Se Trust Italia S.p.A. stabilisce che tali eccezioni o carenze costituiscono una minaccia immediata alla sicurezza o all'integrità del VTN, un piano di azioni correttive saranno sviluppate entro 30 giorni e attuate entro un lasso di tempo commercialmente ragionevole. Per eccezioni o irregolarità meno gravi, il Management Trust Italia S.p.A. valuterà l'importanza di tali questioni e di determinare il flusso degli interventi del caso.

8.6 Comunicazione dei Risultati

Una copia della relazione di revisione WebTrust Trust Italia S.p.A. per CA (o equivalente) è disponibile all'indirizzo http://www. Trust Italia S.p.A. .com / repository.

9. Altri Aspetti e Questioni Giuridiche

9.1 Commissioni

9.1.1 Commissioni Rilascio o Rinnovo del Certificato

Trust Italia S.p.A. ha il diritto di riscuotere delle somme dagli Abbonati utenti finali per la gestione del rilascio ed il rinnovo dei Certificati.

9.1.2 Commissioni di Accesso al Certificato

Trust Italia S.p.A. ed i Clienti non faranno pagare alcunché quale presupposto per rendere un Certificato disponibile in una repository o renderlo altrimenti disponibile alle Parti Facenti Affidamento.

9.1.3 Commissioni per l'Accesso ad Informazioni relative a Revoca e Stato

Trust Italia S.p.A. non farà pagare alcunché quale presupposto per rendere i CRL previsti al presente CPS disponibili in una repository o renderli altrimenti disponibili alle Parti Facenti Affidamento.
Tuttavia, Trust Italia S.p.A. addebiterà una somma per la fornitura di CRL personalizzati, servizi OCSP o altri servizi di informazioni a valore aggiunto su revoche e stato. Trust Italia S.p.A. non concederà accesso alle informazioni sulle revoche, alle informazioni sullo stato dei Certificati o sul contrassegno datario contenute

nei propri archivi a quei terzi fornitori di prodotti e servizi che utilizzano tali informazioni sullo stato dei Certificati senza il preventivo consenso scritto di Trust Italia S.p.A..

9.1.4 Commissioni per Altri Servizi

Trust Italia S.p.A. non addebiterà nulla per l'accesso al CP o al presente CPS. Qualsiasi utilizzo realizzato per scopi diversi dalla semplice visione del documento (tra cui riproduzione, ridistribuzione, modifica o creazione di opere derivate) è subordinato alla stipula di un contratto di licenza con l'entità che detiene il copyright per il documento.

9.1.5 Politica di Rimborso

All'interno del Sotto-dominio Trust Italia S.p.A., è in vigore la seguente policy relativa ai rimborsi, si veda anche https://www.trustitalia.it

Trust Italia S.p.A. aderisce a e sostiene pratiche e politiche rigorose nelle operazioni di certificazione e nel rilascio di Certificati Server. Tuttavia, qualora – per una qualsiasi ragione – un Abbonato non dovesse essere completamente soddisfatto con i Certificati Server ad esso/a rilasciati, potrà richiedere che Trust Italia S.p.A. revochi il Certificato entro trenta (30) giorni dalla data del rilascio fornendo al contempo un rimborso all'Abbonato. Dopo tale periodo iniziale di trenta (30) giorni, un Abbonato potrà richiedere a Trust Italia S.p.A. di revocare il Certificato ed effettuare un rimborso se Trust Italia S.p.A. ha violato una garanzia o un altro suo obbligo sostanziale ai sensi del presente CPS riguardante l'Abbonato o il Certificato dello stesso. Dopo che il certificato è stato revocato da Trust Italia S.p.A., Trust Italia S.p.A. accrediterà prontamente sul conto di carta di credito dell'Abbonato (nel caso in cui il Certificato sia stato pagato tramite carta di credito), o rimborserà in altro modo all'Abbonato mediante assegno, l'intero importo della tariffa applicabile pagata per il Certificato.
Per richiedere un rimborso è necessario contattare il servizio consumatori al numero +39.06332287. La presente policy di rimborso non rappresenta un rimedio esclusivo e non pone restrizioni ad altre azioni di rimedio a disposizione degli Abbonati.

9.2 Responsabilità Finanziaria

9.2.1 Copertura Assicurativa

I clienti aziendali sono invitati a mantenere un livello commercialmente ragionevole di copertura assicurativa per errori ed omissioni, attraverso un programma di assicurazione per errori ed omissioni con una società assicurativa o mediante una trattenuta di autoassicurazione. Trust Italia S.p.A. è in possesso di tale copertura assicurativa per errori ed omissioni.

9.2.2 Altre Attività

I clienti aziendali devono avere risorse finanziarie sufficienti a mantenere le proprie operazioni e a svolgere i propri compiti e devono essere ragionevolmente in grado di sopportare il rischio di responsabilità per Abbonati e Parti Facenti Affidamento.

Estensione Copertura Garanzia

Il Piano di Protezione **Allianz Global Corporate & Specialty AG** risarcisce il titolare di un ID digitale per perdite finanziarie subite a seguito di compromissioni ed altri rischi specificati, tra cui:

- Compromissione della chiave privata **custodita da Trust Italia**
- Sostituzione di persona a causa di informazioni falsificate
- Ritardo o mancata sospensione o revoca di un ID digitale
- Revoca non-autorizzata di un ID digitale senza giusta causa
- Impossibilità di utilizzo di un ID digitale operativo a seguito di servizi collegati a VeriSign
- Rilascio erroneo di un ID digitale ad una persona sbagliata o non-autorizzata

Il massimale previsto dal Piano di Protezione **Allianz Global Corporate & Specialty AG è pari a € 2.500.000,00**

Il PKI Warranty Program Protection Plan di Trust Italia S.p.A. è un programma di estensione della garanzia che si applica all'interno Sottodominio del VTN Symantec. Laddove applicabile, il Trust Italia S.p.A. PKI Warranty Program Protection fornisce a Trust Italia S.p.A. ed agli abbonati i certificati Code Signing SSL contro perdita o danno dovuti ad una defezione da parte di Trust Italia S.p.A. nell'emissione del certificato o altri illeciti causati da negligenza di Trust Italia S.p.A. o da violazione dei propri obblighi contrattuali, a condizione che il sottoscrittore del certificato abbia adempiuto agli obblighi applicabili derivanti dal contratto di servizio. Per informazioni generali relative al Trust Italia S.p.A. PKI Warranty Program, e per richiedere quali Certificati rientrino in tale copertura, contattare telefonicamente al numero +39.06.332287

9.3 Riservatezza delle Informazioni Aziendali

9.3.1 Ambito di Applicazione delle Informazioni Riservate

I dati successivi relativi agli abbonati, fatta salva la sezione 9.3.2, dovranno rimanere confidenziali e privati ("Informazioni Confidenziali/ Private"):

- Dati sulle applicazioni delle CA, se approvate o non approvate,
- Dati Richieste Certificato,
- Chiavi private conservate da clienti aziendali che utilizzano la Managed PKI e informazioni necessarie per il recupero di tali chiavi private,
- Dati transazionali (sia record completi che la tracciabilità degli audit sulle operazioni),
- Dati di tracciabilità degli audit creati o mantenuti da Symantec o da un cliente,
- Dati degli Audit creati da Trust Italia S.p.A. o da un cliente (nella misura in cui si mantengano tali relazioni), e i loro rispettivi auditor (sia interni che pubblici),
- Piani d'emergenza e piani di disaster recovery
- Misure di sicurezza nel controllare le operazioni hardware e software di Trust Italia S.p.A. e amministrazione dei servizi di certificazione e servizi di iscrizione.

9.3.2 Informazioni Non Incluse tra le Informazioni Riservate

Certificati, revoca del certificato e altre informazioni di stato, repository Trust Italia S.p.A. ed informazioni contenute al loro interno non sono considerate Informazioni Riservate/ Confidenziali. Informazioni non espressamente considerate Riservate/ Confidenziali nella sezione 9.3.1 sono considerate né confidenziali, né private. Questa sezione è soggetta alle leggi sulla privacy.

9.3.3 Responsabilità nella Protezione delle Informazioni Riservate

Trust Italia S.p.A. protegge le informazioni private da compromissioni e divulgazione a terzi.

9.4 Privacy sulle Informazioni Personali

9.4.1 Programmazione della Privacy

Trust Italia S.p.A. ha attuato una politica sulla privacy, rintracciabile all'indirizzo: https://www.trustitalia.it/privacy/index.html, in conformità con CP § 9.4.

9.4.2 Informazioni Considerate Private

Tutte le informazioni sugli abbonati non disponibili al pubblico attraverso il contenuto del certificato rilasciato, directory del certificato e CRL online, sono trattate come private.

9.4.3 Informazioni Non Considerate Private

In rispetto delle leggi locali, tutte le informazioni rese pubbliche in un certificato non vengono considerate private.

9.4.4 Responsabilità nella protezione delle Informazioni Private

I partecipanti al VTN che ricevono informazioni private sono al sicuro dal compromesso e la divulgazione a terzi e dovranno rispettare tutte le leggi locali nella loro giurisdizione sulla privacy.

9.4.5 Comunicazione e Consenso per l'Utilizzo di Informazioni Private

Salvo dove diversamente specificato nel presente CPS, applicabile sulla privacy o da accordo, le informazioni private non saranno utilizzate senza il consenso della parte cui tali informazioni vengono applicate. Questa sezione è soggetta alle leggi sulla privacy

9.4.6 Divulgazione ai sensi di Procedimento Giudiziario o Amministrativo

Trust Italia S.p.A. ha il diritto di rivelare Informazioni Riservate / Confidenziali se, in buona fede, ritenga che:

- La divulgazione sia necessaria in risposta a citazioni e mandati di perquisizione.
- La divulgazione sia necessaria in risposta a procedimenti giudiziari, amministrativi o altro
- Durante lo svolgimento di procedimento legale in una causa civile o amministrativa, quali citazioni, interrogatori, richieste di ammissione e richieste di produzione documentazione.

Questa sezione è soggetta alle leggi sulla privacy.

9.4.7 Altre Circostanze Relative alle Informazioni

Nessuna pattuizione

9.5 Diritti di Proprietà Intellettuale

La ripartizione dei Diritti di Proprietà Intellettuale tra i Partecipanti al Sottodominio di Trust Italia S.p.A. , che non sono Abbonati o Parti Facenti Affidamento, è disciplinata dai contratti stipulati tra tali Partecipanti al Sottodominio di Trust Italia S.p.A.. I seguenti sub-paragrafi del CPS § 9.5 si applicano ai Diritti di Proprietà Intellettuale nei confronti di Abbonati e Parti Facenti Affidamento.

9.5.1 Diritti di Proprietà Relativi alle Informazioni su Certificati e Revoche

Le CA mantengono tutti i Diritti di Proprietà Intellettuale sulle informazioni relative ai Certificati ed alle revoche da esse emesse. Trust Italia S.p.A. e gli Abbonati danno il permesso di riprodurre e distribuire Certificati su base non-esclusiva e senza pagamento di royalties, a condizione che gli stessi siano riprodotti integralmente e che l'utilizzo dei Certificati sia soggetto alle clausole del Contratto per Parte Facente Affidamento a cui si fa riferimento nel Certificato in questione. Trust Italia S.p.A. e gli Abbonati daranno il permesso per l'uso delle informazioni sulle revoche per l'esecuzione delle funzioni di Parte Facente Affidamento ai sensi del CRL Usage Agreement per Parte Facente Affidamento applicabile o di altri accordi applicabili.

9.5.2 Diritti di Proprietà sul CPS

I Partecipanti al VTN danno atto che Trust Italia S.p.A. manterrà tutti i Diritti di Proprietà Intellettuale sul presente CPS.

9.5.3 Diritti di Proprietà sui Nomi

Un Richiedente di Certificato manterrà tutti i propri diritti (se ce ne sono) su qualsiasi marchio commerciale, marchio di servizio o nome commerciale contenuto in una Richiesta di Certificato e distinguished name all'interno di qualsiasi Certificato rilasciato a tale Richiedente.

9.5.4 Diritti di Proprietà su Chiavi e Materiale per Chiavi

Le coppie di chiavi corrispondenti a Certificati di CA ed Abbonati (utenti finali) sono di proprietà delle CA e degli Abbonati utenti finali che risultano essere i rispettivi Soggetti di tali Certificati, subordinatamente ai diritti dei Clienti Managed PKI che utilizzano il Gestore Chiavi Managed PKI ed indipendentemente dal supporto su cui sono immagazzinate e protette, dette persone manterranno tutti i Diritti di Proprietà Intellettuale su tali coppie di chiavi. Nonostante quanto precede, le chiavi pubbliche Root Symantec ed i Certificati Root che le

contengono, incluse tutte le chiavi pubbliche delle PCA ed i Certificati auto-firmati, sono di proprietà Symantec.
Symantec concede delle licenze ai produttori di software e hardware per la riproduzione di tali Certificati root al fine di inserirne delle copie in strutture hardware o software affidabili. Infine, senza limitare la generalità di quanto precede, le Secret Share della chiave privata di una CA sono di proprietà della CA stessa, la quale mantiene tutti i Diritti di Proprietà Intellettuale su queste Secret Share o su CA Symantec.

9.6 Dichiarazioni e Garanzie

9.6.1 Rappresentazioni e Garanzie della CA

Trust Italia S.p.A. garantisce che:

- Non vi siano false dichiarazioni sostanziali nel Certificato che siano conosciute o derivanti dalle entità che approvano la Richiesta di Certificato o che rilasciano il Certificato.
- Non ci siano errori nelle informazioni contenute nel Certificato, che siano state introdotte dalle entità che approvano la Richiesta di Certificato o che rilasciano il Certificato a seguito di una mancata ragionevole cura nella gestione della Richiesta di Certificato o nella reazione del Certificato.
- I loro Certificati soddisfino tutti i requisiti essenziali stabiliti nel presente CPS; e
- I servizi di revoca e l'utilizzo di un archivio siano conformi al presente CPS in tutti gli aspetti essenziali.

I Contratti di Abbonamento possono includere rappresentazioni e garanzie supplementari.

9.6.2 Rappresentazioni e Garanzie delle RA

Le RA garantiscono che:

- Non vi sono false dichiarazioni sostanziali nel Certificato che siano conosciute o derivanti dalle entità che approvano la Richiesta di Certificato o che rilasciano il Certificato.
- Non ci sono errori nelle informazioni contenute nel Certificato, che siano state introdotte dalle entità che approvano la Richiesta di Certificato a seguito di una mancata ragionevole cura nella gestione della Richiesta di Certificato.
- I loro Certificati soddisfano tutti i requisiti essenziali stabiliti nel presente CPS; e
- I servizi di revoca (ove attuabili) e l'utilizzo di una repository sono conformi al presente CPS in tutti gli aspetti essenziali

I Contratti di Abbonamento possono includere rappresentazioni e garanzie supplementari.

9.6.3 Rappresentazioni e Garanzie dell'Abbonato

Gli abbonati garantiscono che:

- Ogni firma digitale creata utilizzando la chiave privata che corrisponde alla chiave pubblica indicata nel Certificato è la firma digitale dell'Abbonato, ed il Certificato è stato accettato e risulta operativo (cioè né scaduto né revocato) al momento della creazione del Certificato.
- Nessuna persona non-autorizzata ha mai avuto accesso alla chiave privata dell'Abbonato.
- Tutte le dichiarazioni rese dell'Abbonato nella Richiesta di Certificato presentata dall'Abbonato stesso no veritiere.
- Tutte le informazioni fornite dall'Abbonato e contenute nel Certificato sono veritiere.
- Il Certificato è utilizzato esclusivamente per scopi leciti e legittimi conformi al presente CPS; e
- L'Abbonato è un Abbonato utente finale e non una CA e non utilizza la chiave privata corrispondente ad una qualsiasi chiave pubblica indicata nel Certificato per firmare digitalmente un Certificato (o un qualsiasi altro formato o chiave pubblica certificata) o CRL in qualità di CA o altro.

I Contratti di Abbonamento possono includere rappresentazioni e garanzie supplementari.

9.6.4 Rappresentazioni e Garanzie della Parte Facente Affidamento

I Contratti per Parti Facenti Affidamento richiedono alle Parti Facenti Affidamento di dare atto che possiedono informazioni sufficienti per poter prendere una decisione informata in merito alla misura in cui intendono fare affidamento sulle informazioni contenute in un Certificato; che sono esclusivamente

responsabili della decisione se fare affidamento su tali informazioni o meno; e che sosterranno tutte le conseguenze legali di una loro eventuale inosservanza degli obblighi stabiliti per la Parti Facenti Affidamento nel presente CPS.
I Contratti per Parti Facenti Affidamento possono includere rappresentazioni e garanzie supplementari.

9.6.5 Rappresentazioni e Garanzie degli Altri Partecipanti

Nessuna stipulazione

9.7 Esclusione di Garanzia

Nella misura concessa dalle leggi applicabili, i Contratti di Abbonamento e i Contratti per Parti Facenti Affidamento di Trust Italia S.p.A. disconoscono possibili ulteriori garanzie di Trust Italia S.p.A., ivi incluse garanzie di commerciabilità o idoneità ad un determinato scopo.

9.8 Limitazioni di Responsabilità

Nella misura concessa dalle leggi applicabili, i Contratti di Abbonamento ed i Contratti per Parti Facenti Affidamento di Trust Italia S.p.A. limitano – e gli altri Contratti di Abbonamento dovranno limitare – la responsabilità di Trust Italia S.p.A.. Le limitazioni di responsabilità includono la previsione che tutti i danni indiretti, speciali, emergenti e conseguenti siano esclusi. Esse potrebbero contenere dei tetti limiti relativi a danni di Trust Italia S.p.A. riguardanti uno specifico certificato:

Classe	Maegini di Responsabilità
Classe 1	Cento Dollari U.S.A. ($ 100.00 US)
Classe 2	Cinquemila Dollari U.S.A. ($ 5,000.00 US)
Classe 3	Centomila Dollari U.S.A. ($ 100,000.00 US)

Tabella 14 – Margini di Responsabilità

La responsabilità (e/o la sua limitazione) degli Abbonati devono essere come stabilito dagli accordi applicabili di sottoscrizione.
La responsabilità (e/o la sua limitazione) delle RA aziendali e le relative CA sono definiti nel contratto(i) tra di loro.
La responsabilità (e/o la sua limitazione) di far valere le Parti Facenti Affidamento deve essere quella enunciata negli accordi applicabili.

9.9 Indennità

9.9.1 Risarcimento per l' Abbonato

Nella misura concessa dalle leggi applicabili, gli Abbonati dovranno risarcire Trust Italia S.p.A per quanto segue:

- Dichiarazione falsa o fuorviante da parte dell'Abbonato nella sua Richiesta di Certificato;
- Mancata informazione da parte dell'Abbonato nella Richiesta di Certificato su un fatto essenziale, nel caso in cui tale falsa dichiarazione o omissione sia stata fatta in negligenza o con l'intenzione di raggirare una delle parti;
- Mancata protezione da parte dell'Abbonato della propria chiave privata, mancato utilizzo di un Sistema Attendibile o altrimenti mancata adozione delle precauzioni necessarie per evitare compromissione, perdita, divulgazione, modifica o utilizzo non-autorizzato della chiave privata dell'Abbonato; o
- Utilizzo da parte dell'Abbonato di un nome (inclusi, a titolo esemplificativo e non esaustivo, common name, nomi dominio o indirizzi e-mail) che violi i Diritti di Proprietà Intellettuale di terzi.

Il Contratto di Abbonamento applicabile può comprendere obblighi di indennizzo aggiuntivo.

9.9.2 Risarcimento per Parti Facenti Affidamento

Nella misura concessa dalle leggi applicabili, i Contratti di Abbonamento obbligano le Parti Facenti Affidamento a risarcire Trust Italia S.p.A per quanto segue:

- Mancata osservanza della Parte Facente Affidamento dei suoi obblighi in quanto tale;
- Affidamento della Parte Facente Affidamento su un Certificato in una maniera non ragionevole nelle circostanze; oppure
- Mancato controllo della Parte Facente Affidamento sullo stato del Certificato in questione per verificare se lo stesso sia scaduto o revocato.

Il contratto per Parte Facente Affidamento applicabile può includere obblighi di indennizzo aggiuntivo.

9.10 Durata e Risoluzione

9.10.1 Durata

Il CPS entra in vigore alla pubblicazione nella repository di Trust Italia S.p.A.. Aggiornamenti al presente CPS entrano in vigore al momento della pubblicazione nella repository di Trust Italia S.p.A..

9.10.2 Terminazione

Il presente CPS modificato di volta in volta rimarrà in vigore fino a quando non verrà sostituito da una nuova versione.

9.10.3 Effetti della Risoluzione e Sopravvivenza

Una volta scaduto il presente CPS, i partecipanti al sotto-dominio Trust Italia S.p.A. sono tuttavia vincolati dalle sue condizioni per tutti i certificati rilasciati durante il periodi di validità di tali certificati.

9.11 Avvisi Individuali e Comunicazioni con i Partecipanti

Salvo diversamente specificato da un accordo tra le parti, i partecipanti al sotto-dominio Trust Italia S.p.A. dovranno utilizzare metodi commercialmente ragionevoli per comunicare tra loro, tenendo conto della criticità e dell'oggetto della comunicazione.

9.12 Modifiche

9.12.1 Procedure di Modifica

Le modifiche al presente CPS possono essere effettuate mediante la Policy Management Authority (PMA) di Trust Italia S.p.A.. Le modifiche devono essere sotto forma di documento contenente una versione modificata del CPS o un aggiornamento. Le versioni modificate o aggiornamenti devono essere collegati alla sezione Practices Updates e Notices, e della Repository Trust Italia S.p.A. reperibile all'indirizzo: https://www.trustitalia.it/archivio/repository/updates. Gli aggiornamenti sostituiscono le disposizioni designate o in conflitto con la versione del CPS cui si fa riferimento. Il PMA deve determinare se le modifiche al CPS richiedono un cambiamento degli identificatori delle Policy di certificazione corrispondenti a ciascuna classe di certificazione.

9.12.2 Meccanismo di Notifica e Periodo

Trust Italia S.p.A. e PMA si riservano il diritto senza preavviso di effettuare modifiche al CPS che non siano sostanziali, incluse, senza limitazione, correzioni di errori tipografici, modifiche alle URL e modifiche alle informazioni di contatto. La decisione del PMA di determinare modifiche come materiali o non materiali sarà ad esclusiva discrezione del PMA.
Proposte di modifica del CPS dovranno figurare nella sezione Aggiornamenti delle Procedure ed Avvisi Trust Italia S.p.A. che si trova all'indirizzo: https://www.trustitalia.it/archivio/repository/updates.
Nonostante eventuali previsioni contrastanti contenute nel presente CPS, se la PMA ritiene che modifiche sostanziali al CPS si rendano immediatamente necessarie per mettere fine o prevenire una violazione della sicurezza del VTN, o di qualsiasi porzione di esso, di Trust Italia S.p.A. e della PMA, avrà il diritto di effettuare tali modifiche mediante pubblicazione nella Repository Trust Italia S.p.A.. Tali modifiche entreranno in vigore immediatamente al momento della pubblicazione. Entro un lasso di tempo ragionevole

dalla pubblicazione, Trust Italia S.p.A. dovrà notificare tali modifiche ai partecipanti del proprio Sotto-dominio.

Periodo Stabilito per le Osservazioni

Salvo quanto diversamente indicato, il periodo per l'invio di osservazioni riguardanti eventuali modifiche sostanziali al CPS sarà di quindici (15) giorni a partire dalla data in cui le modifiche stesse sono state pubblicate nella Repository Trust Italia S.p.A.. Ogni Partecipante al Subdomonio di Trust Italia S.p.A. avrà la facoltà di inviare osservazioni alla PMA fino alla scadenza del periodo indicato.

Meccanismo per la Gestione delle Osservazioni

La PMA terrà conto di tutte le osservazioni giunte sulle modifiche proposte. La PMA avrà tre alternative: (a) permettere che le modifiche proposte entrino in vigore senza cambiamenti, (b) cambiare le modifiche proposte e ripubblicarle come nuove modifiche qualora richiesto, oppure (c) ritirare le modifiche proposte. La PMA ha la facoltà di ritirare le modifiche proposte dandone avviso nella sezione Aggiornamenti ed Avvisi Pratiche della repository Trust Italia S.p.A.. A meno che le modifiche proposte non siano cambiate o ritirate, tali modifiche entreranno in vigore allo scadere dei termini previsti per le osservazioni.

9.12.3 Circostanze che Richiedono Modifiche nella Policy di Certificazione OID

Se la PMA determina che un cambiamento è necessaria nell'identificatore di oggetto corrispondente ad una policy di certificazione, tale modifica deve contenere nuovi identificatori di oggetto per le politiche certificato corrispondente a ciascuna classe di certificazione. In caso contrario, le modifiche non richiederanno un cambiamento all' identificatore di oggetto per le politiche certificato.

9.13 Disposizioni su Risoluzioni di Controversie

9.13.1 Controversie tra Symantec, Affiliati e Clienti

Le controversie tra partecipanti al sotto-dominio di Trust Italia S.p.A. saranno risolte ai sensi delle disposizioni applicabili negli accordi tra le parti.

9.13.2 Controversie con Abbonati "utenti finali" o Parti Facenti Affidamento

Nella misura consentita dalle leggi applicabili, i Contratti di Abbonamento ed i Contratti per Parti Facenti Affidamento di Trust Italia S.p.A. devono contenere una clausola di risoluzione delle controversie. Controversie che coinvolgono Trust Italia S.p.A. prevedono un periodo iniziale di negoziazione di sessanta (60) giorni, seguiti da contenzioso presentato innanzi al Tribunale di Roma, nel caso di richiedenti che siano residenti in Italia o, nel caso di tutti gli altri aventi diritto, l'arbitrato amministrato dalla Camera di Commercio Internazionale ("ICC") in conformità con il Regolamento ICC di Conciliazione e Arbitrato.

9.14 Leggi

Salvo restrizioni previste dalle leggi applicabili, l'attuazione, interpretazione e validità del presente CPS saranno disciplinate dalle leggi italiane, indipendentemente dalle previsioni contrattuali o di altre scelte rispetto alle leggi applicabili e senza che vi sia la necessità di stabilire una sede commerciale in Italia. La presente scelta di legge applicabile viene fatta per assicurare procedure ed interpretazioni univoche per tutti i Partecipanti al Sottodominio di Trust Italia S.p.A. indipendentemente dal luogo della loro sede.
La presente clausola sulla legge applicabile riguarda soltanto il presente CPS. Altri contratti, nei quali il CPS è incorporato mediante riferimento, potranno avere clausole autonome in merito alla legge applicabile, a condizione che CPS § 9.14 disciplini l'attuazione, interpretazione e validità dei termini del CPS separatamente dalle rimanenti clausole di tali contratti e subordinatamente alle eventuali limitazioni stabilite dalle leggi vigenti.
Il presente CPS è soggetto a tutte le leggi, norme, regolamenti, ordinanze, decreti ed ordinamenti nazionali, statali, locali e stranieri applicabili, ivi incluse, a titolo esemplificativo e non esaustivo, eventuali limitazioni sull'import-export di software, hardware ed informazioni tecniche.

9.15 Conformità con le Leggi Vigenti

Il presente CPS è soggetto a tutte le leggi, norme, regolamenti, ordinanze, decreti ed ordinamenti nazionali, statali, locali e stranieri applicabili, ivi incluse, a titolo esemplificativo e non esaustivo, eventuali limitazioni sull'import-export di software, hardware ed informazioni tecniche.

9.16 Disposizioni Varie

9.16.1 Contratto Completo

Non applicabile

9.16.2 Assegnazione

Non applicabile

9.16.3 Divisibilità

Nel caso in cui una clausola o una disposizione del presente CPS sia ritenuta inapplicabile da un tribunale o da un altro tribunale avente autorità, il resto delle disposizioni del CPS resteranno valide.

9.16.4 Imposizione (Spese Legali e Rinuncia dei Diritti)

Non applicabile

9.16.5 Forza Maggiore

Nella misura consentita dalla legge applicabile, i Contratti di Abbonamento ed i Contratti per Parti Facenti Affidamento devono includere una clausola di forza maggiore a protezione di Symantec.

9.17 Altre Disposizioni

Non applicabile

Appendice A. Tavola delle Sigle e Definizioni

Tabella degli Acronimi

Termini	Definizioni
ANSI	The American National Standards Institute.
ACS	Authenticated Content Signing.
BIS	The United States Bureau of Industry and Science of the United States Department of Commerce.
CA	Certification Authority.
CP	Certificate Policy.
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
EAL	Evaluation assurance level (pursuant to the Common Criteria).
FIPS	United State Federal Information Processing Standards.
ICC	International Chamber of Commerce.
KRB	Key Recovery Block.
LSVA	Logical security vulnerability assessment.
OCSP	Online Certificate Status Protocol.
PCA	Primary Certification Authority.
PIN	Personal identification number.
PKCS	Public-Key Cryptography Standard.
PKI	Public Key Infrastructure.
PMA	Policy Management Authority.
RA	Registration Authority.
RFC	Request for comment.
SAR	Security and Audit Requirements
SAS	Statement on Auditing Standards (promulgated by the American Institute of Certified Public Accountants).
S/MIME	Secure multipurpose Internet mail extensions.
SSL	Secure Sockets Layer.
VTN	VeriSign Trust Network.

Definizioni

Termini	Definizioni
Amministratore	Una Persona Fiduciaria all'interno dell'organizzazione di un Processing Center, Centro Servizi, Cliente Managed PKI o cliente Gateway,che esegue funzioni di convalida ed altre funzioni CA o RA.
Certificato Amministratore	Un Certificato rilasciato ad un Amministratore che può essere utilizzato soltanto per eseguire funzioni CA o RA.
Affiliato	Una terza parte fiduciaria, leader ad esempio nel ramo tecnologico, delle telecomunicazioni o dei servizi finanziari, che ha stipulato un contratto con Symantec per diventare un canale di distribuzione VTN e di servizi in un territorio specifico.
Affiliate Practices Legal Requirements Guidebook (Guida Programma di Verifica Affiliati)	Un documento Symantec contenente i requisiti per i CPS degli Affiliati, gli accordi, le procedure di validazione e le policy sulla privacy, inclusi altre prerogative cui gli Affiliati devono attenersi.
Individuo Affiliato	Una persona fisica collegata ad un cliente MPKI, MPKI Lite o Gateway, quale funzionario, direttore, impiegato, partner, contraente, intero, o altro nell'ambito dell' ente, quale membro registrato ad una comunità d'interessi di Symantec, oppure (iii) quale persona che mantiene una relazione con tale entità e quest'ultima possiede documenti economici o di altro tipo che forniscono garanzie adeguate circa l'identità di tale persona.
Amministrazione Automatizzata	Una procedura mediante la quale le Richieste di Certificati vengono approvate automaticamente, se le informazioni di iscrizione corrispondono a quelle contenute in un database.
Modulo Software per Amministrazione Automatizzata	Software fornito da Symantecche svolge l'Amministrazione Automatizzata.
Certificato	Un messaggio che indica per lo meno un nome o identifica la CA, identifica l'Abbonato, contiene la chiave pubblica dell'Abbonato, identifica il Periodo di Validità del Certificato, contiene il numero di serie del Certificato ed è firmato digitalmente dalla CA.
Richiedente un Certificato	Un individuo o un'organizzazione che richiede il rilascio di un Certificato da parte di una CA.
Richiesta di Certificato	Una richiesta da parte di un Richiedente (o di un rappresentante autorizzato del Richiedente) alla CA per il rilascio di un Certificato.

Termini	Definizioni
Catena di Certificazione	Una lista ordinata di Certificati contenente il Certificato Abbonato di un utente finale ed i Certificati CA e che termina con un Certificato "Root". An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
Obiettivi di Controllo di Gestione Certificati	Criteri che un'entità deve soddisfare al fine di un esito positivo della Revisione di Conformità.
Policy di Certificazione (CP)	Il documento denominato "VeriSign Trust Network Certificate Policies" che è la dichiarazione primaria della policy che disciplina il VTN.
Certificate Revocation List (CRL)	Una lista pubblicata periodicamente (o secondo necessità) e firmata digitalmente da una CA, di quei Certificati identificati che sono stati revocati prima della loro data di scadenza come da CP § 3.4 . In genere, la lista indica il nome di chi stila la CRL, la data di redazione, la data prevista per la prossima lista, i numeri di serie dei Certificati revocati, nonché i tempi e le cause specifiche della revoca.
Certificate Signing Request (CSR)	Un messaggio contenente una richiesta di rilascio Certificato.
Certification Authority (CA)	Un'entità autorizzata al rilascio, alla gestione e revoca ed al rinnovo di Certificati nel VTN.
Certification Practice Statement (CPS)	Una dichiarazione delle pratiche seguite da Symantec o da un Affiliato per l'approvazione o il rifiuto di Richieste di Certificati, nonché per il rilascio, la gestione e la revoca di Certificati (pratiche alle quali anche i relativi Clienti Managed PKI e Gateway dovranno attenersi).
Challenge Phrase	Una frase segreta scelta da un Richiedente un Certificato durante l'iscrizione per il Certificato. Al momento del rilascio del Certificato, il Richiedente diventa un Abbonato, e una CA o RA può usare la Challenge Phrase per identificare l'Abbonato quando questo vuole revocare o rinnovare il proprio Certificato.
Classe	Un livello specifico di sicurezza come definito nel CP. Vedi CP § 1.1.1.
Client Service Center	Un Centro Servizi, che è un Affiliato, il quale fornisce Certificati per clienti nel Impostatotore Consumatori o Imprese.
Verifica di Conformità	Una verifica periodica di un Processing Center, Centro di Servizi, Cliente Managed PKI o Gateway, per verificare la sua conformità agli Standard VTN applicabili.
Compromissione	Una violazione (o sospetta violazione) di una policy di sicurezza, per cui può essersi verificata la divulgazione non autorizzata o la perdita di controllo su informazioni sensibili. Per quanto riguarda le chiavi private, una Compromissione è una perdita, furto, divulgazione, modifica, uso non autorizzato o altra compromissione della sicurezza di tale chiave privata.
Informazioni Confidenziali/ Private	Informazioni che devono essere mantenute riservate e private secondo il CPS § 2.8.1.
Contratto di Utilizzo CRL	Un contratto che specifica i termini e le modalità di utilizzo di un CRL o delle informazioni ivi contenute.
Cliente	Un' organizzazione che sia un cliente MPKI, Gateway o ASB.
Impresa, come Service Centerper le Imprese	Un Impostatotore in cui un Affiliato si attiva per fornire servizi MPKI a clienti MPKI.
Audit/Indagine Esigente	Una revisione o indagine da parte di Symantec, nel caso in cui Symantec abbia motivo di ritenere che un'entità non si sia attenuta agli Standard VTN o che si sia verificato un incidente o Compromissione nell'entità o una minaccia effettiva o potenziale alla sicurezza del VTN per mezzo dell'entità.
Diritti di Proprietà Intellettuale	Diritti riguardanti uno o più dei seguenti ambiti: ciascun copyright, brevetto, segreto commerciale, marchio commerciale, nonché ogni altro diritto di proprietà intellettuale.
Autorità di Certificazione Intermedia (CA Intermedia)	Un'Autorità di Certificazione il cui Certificato si trova all'interno di una Catena di Certificazione tra il Certificato della Root CA ed il Certificato di quell'Autorità di Certificazione, che ha rilasciato il Certificato Abbonato dell'utente finale.
Generazione della Key Ceremony	Una procedura mediante la quale si genera la coppia di chiavi di una CA o RA, la sua chiave privata è trasferita in un modulo crittografico, si crea un backup della sua chiave privata e/o la sua chiave pubblica è certificata.
Amministratore Gestore Chiavi	Un Amministratore che svolge funzioni di generazione e recupero chiavi per un Cliente Managed PKI utilizzando un Gestore Chiavi Managed PKI.
Blocco Recupero Chiavi (KRB) (Key Recovery Block - KRB)	Una struttura dati contenente la chiave privata di un Abbonato che viene criptata mediante una chiave di crittazione. I KRB vengono generati utilizzando il software Gestore Chiavi Managed PKI.
Key Recovery Service	Un servizio Symantec che offre le chiavi di crittazione necessarie per recuperare un Blocco Recupero Chiavi nell'ambito dell'utilizzo da parte di un Cliente Managed PKI del Gestore Chiavi Managed PKI per il recupero della chiave privata di un Abbonato.
Managed PKI	Il servizio PKI di Symantec completamente integrato che permette ai Clienti aziendali Symantec e dei suoi Affiliati di distribuire Certificati ad individui, quali impiegati, soci, fornitori e clienti, nonché impianti, quali server, router e firewall. Il Managed PKI permette alle imprese di proteggere applicazioni di messaggi, intranet, extranet, rete virtuale privata e commercio elettronico.

Termini	Definizioni
Amministratore Managed PKI	Un Amministratore che svolge funzioni di convalida o altre funzioni RA per un Cliente Managed PKI.
Managed PKI Control Center	Un'interfaccia su base Web che permette agli Amministratori Managed PKI di effettuare l'Autenticazione Manuale di Richieste di Certificati.
Gestore Chiavi Managed PKI	Una soluzione per il recupero di chiavi per quei Clienti Managed PKI che scelgono di effettuare il recupero chiavi secondo uno speciale Contratto Managed PKI. A key recovery solution for those Managed PKI Customers choosing to implement key recovery under a special Managed PKI Agreement.
Guida per gli Amministratori del Servizio di Gestione Chiavi Managed PKI	Un documento che specifica i requisiti operativi e le pratiche relative ai Clienti Managed PKI che utilizzano un Gestore Chiavi Managed PKI.
Autenticazione Manuale	Una procedura mediante la quale le Richieste di Certificati vengono esaminate ed approvate manualmente una per una da un Amministratore che utilizza un'interfaccia su base web. A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface.
NetSure Protection Plan	Un programma di estenzione garanzia descritto al CPS § 9.2.3.
Informazioni Abbonato Non Verificate	Informazioni presentate da un Richiedente di Certificato ad una CA o RA, ed incluse in un Certificato, che non sono state verificate dalla CA o RA e per le quali la relativa CA o RA non fornisce alcuna garanzia oltre al fatto che tali informazioni sono state fornite dal Richiedente il Certificato.
Non Ripudio	Attributo di una comunicazione che fornisce protezione contro una parte che nega ingannevolmente l'origine della comunicazione, il fatto che sia stata inviata o la sua ricezione. La negazione di origine include la negazione del fatto che una comunicazione proviene dalla stessa fonte come uno o più messaggi precedenti, anche qualora l'identità associata al mittente sia sconosciuta. Nota: soltanto la sentenza di un tribunale, di una commissione arbitrale o di un'altra autorità giudiziaria potrà evitare il ripudio in maniera definitiva. A titolo esemplificativo, una firma digitale verificata in relazione ad un Certificato VTN può costituire prova a sostegno della determinazione del Non Ripudio da parte del tribunale, ma in sé stessa non costituisce un Non Ripudio.
CA Off-Line	PCA VTN, Root CA che rilasciano Root ed altre CA intermedie designate che sono mantenute off-line per motivi di sicurezza al fine di proteggerle da possibili attacchi di intrusi per mezzo del network. Queste CA non sono firmate direttamente da Certificati di Abbonati utenti finali
CA On- Line	CA che firmano Certificati di Abbonati utenti finali sono mantenute on-line per fornire un servizio di firma continuo.
Online Certificate Status Protocol (OCSP)	Un protocollo per fornire informazioni sullo stato dei Certificati in tempo reale alle Parti Facenti Affidamento.
Periodo di Validità	Il periodo decorrente dalla data ed ora in cui un Certificato viene rilasciato (o da una data ed ora successiva se così indicato nel Certificato) e che termina alla data ed ora in cui il Certificato scade o è anticipatamente revocato.
PKCS #10	Standard di Crittografia per Chiave Pubblica #10, sviluppato da RSA Security Inc., che definisce una struttura per una Richiesta di Firma Certificato (CSR)
PKCS #12	Standard di Crittografia per Chiave Pubblica #12, sviluppato da RSA Security Inc., che definisce una modalità sicura per il trasferimento di chiavi private.
Policy Management Authority (PMA)	L'organizzazione interna a Symantec che è responsabile della diffusione di questa policy in tutto il VTN.
Primary Certification Authority (PCA)	Una CA che funge da CA root per una specifica Classe di Certificati e che rilascia Certificati a CA ad essa subordinate.
Processing Center	Un'organizzazione (Symanteco determinati Affiliati) che crea una struttura sicura, la quale contiene tra l'altro i moduli crittografici impiegati per il rilascio di Certificati. Nei Impostatotori Consumatori e Siti Web, i Centri di Elaborazione fungono da CA nell'ambito del VTN e svolgono tutti i servizi nel ciclo vitale dei Certificati (rilascio, gestione, revoca e rinnovo di Certificati). Nel Impostatotore Imprese, i Centri di Elaborazione forniscono servizi di ciclo vitale per conto dei loro Clienti Managed PKI o dei Clienti Managed PKI dei Centri di Elaborazione ed essi subordinati.
Public Key Infrastructure (PKI)	L'architettura ed organizzazione, le tecniche, pratiche e procedure che nel loro insieme supportano la realizzazione ed il funzionamento di un sistema crittografico a chiave pubblica basato su Certificati. Il PKI del VTN consta di sistemi che collaborano al fine di fornire ed attuare il VTN.
Registration Authority (RA)	Un'entità approvata da una CA per fornire assistenza ai Richiedenti nella loro Richieste di Certificati e per approvare o rifiutare Richieste di Certificati, revocare Certificati o rinnovarli.
Relying Party (Parte Facente Affidamento)	Un individuo o un'organizzazione che agisce facendo affidamento su un certificato e/o su una firma digitale.
Relying Party Agreement (Contratto per Parte Facente Affidamento)	Un contratto utilizzato da una CA nel quale si stabiliscono i termini e le condizioni alle quali un individuo o un'organizzazione agisce in qualità di Parte Facente Affidamento.
Retail Certificate	Un Certificato rilasciato daSymantec o da un Affiliato, che agisce da CA, ad individui o organizzazioni che ne fanno richiesta singolarmente a Symantec sul suo sito web.

Termini	Definizioni
RSA	Sistema crittografico per chiave pubblica inventato da Rivest, Shamir e Adelman.A public key cryptographic system invented by Rivest, Shamir, and Adelman.
RSA Secure Server CA	L'Autorità di Certificazione che rilascia ID Secure Server.
Gerarchi RSA Secure Server	La gerarchia PKI comprensiva dell'Autorità di Certificazione RSA Secure Server.
Secret Share	Una porzione di una chiave privata CA o una porzione dei dati di attivazione necessari al funzionamento di una chiave privata CA ai sensi di un accordo di Suddivisione Segreta (Secret Sharing).
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under CP § 6.2.2.
Secure Server ID	Un Certificato organizzativo di Classe 3 utilizzato per supportare sessioni SSL tra browser web e server web.
Secure Sockets Layer (SSL)	La metodologia standard del Impostatotore per proteggere comunicazioni web, sviluppata da Netscape Communications Corporation. Il protocollo di sicurezza SSL fornisce criptazione dati, au tenticazione server, integrità messaggi ed autenticazione opzionale clienti per un collegamento Protocollo Controllo Trasmissione / Protocollo Internet.
Security and Audit Requirements (SAR) Guide (Guida ai Requisiti di Sicurezza e Revisione)	Un documento Symantec che specifica i requisiti e le pratiche di sicurezza e di revisione per Processing Centers ed iService Centers.
Esame di Sicurezza e Pratiche	L'esame di un Affiliato da parte di Symantec prima che tale Affiliato possa diventare operativo.
Service Center	Un Affiliato che non possiede unità di firma Certificati per il rilascio di Certificati in vista del rilascio di Certificati di uno specifico tipo o Classe, ma si rivolge ad un Processing Center per l'effettuazione di rilascio, gestione, revoca e rinnovo dei Certificati stessi.
Sub-domain (Sottodominio)	La porzione del VTN che si trova sotto il controllo di un'entità nonché tutte le ulteriori entità ad essa subordinate nell'ambito della gerarchia VTN.
Subject (Soggetto)	Il possessore di una chiave privata corrispondente ad una chiave pubblica. Nel caso di un Certificato aziendale, il termine "Soggetto" può riferirsi all'apparecchiatura o al dispositivo che custodisce una chiave privata. Al Soggetto viene assegnato un nome inequivocabile collegato alla chiave pubblica contenuta nel Certificato del Soggetto stesso.
Abbonato (Subscriber)	Nel caso di un Certificato individuale, la persona che è il Soggetto di ed alla quale è stato rilasciato un Certificato. Nel caso di un Certificato aziendale, l'organizzazione (azienda) che possiede l'apparecchiatura o il dispositivo che è il Soggetto di ed al quale è stato rilasciato un Certificato. Un Abbonato è in grado di utilizzare, ed è stato autorizzato a farlo, la chiave privata corrispondente alla chiave pubblica indicata nel Certificato.
Subscriber Agreement (Contratto di Abbonamento)	Un contratto utilizzato d a una CA o RA che specifica i termini e le modalità alle quali un individuo o un'organizzazione agisce in qualità di Abbonato.
Superior Entity (Entità Superiore)	Un'entità al di sopra di una determinata entità nell'ambito di una gerarchia VTN (la gerarchia di Classe 1, 2 o 3).
Supplemental Risk Management Review (Esame Supplementare Gestione Rischi)	L'esame di un'entità da parte di Symantec a seguito di risultati incompleti o insoliti durante una Revisione di Conformità dell'entità stessa, oppure nell'ambito del generale processo di gestione rischi durante la normale conduzione dell'attività.
Reseller	Un'entità che commercializza servizi per conto di Symantec o di un Affiliato in determinati mercati.
Symantec	S' intende, nel rispetto di ciascuna parte pertinente del presente CPS, Symantec Corp. e/o ciascuna succursale interamente acquisita da Symantec responsabile per specifiche operazione di emissione.
Symantec Digital Notarization Service (Servizi Notarili Digitali)	Un servizio offerto a Clienti Managed PKI, che fornisce un'affermazione a firma digitale (Ricevuta Digitale) secondo cui un determinato documento o una serie di dati esisteva ad un preciso momento.
Trusted Person (Persona Fiduciaria)	Un impiegato, appaltatore o consulente di un'entità all'interno del VTN che è responsabile della gestione dell'attendibilità infrastrutturale dell'entità, dei suoi prodotti e servizi, delle sue strutture e/o pratiche come definito in dettaglio al CPS § 5.2.1.
Trusted Position (Posizione Fiduciaria)	Le posizioni in una entità VTN che devono essere ricoperte da Persone Fiduciarie (Trusted Person).
Trustworthy System (Sistema Attendibile)	Hardware, software e procedimenti di computer che sono ragionevolmente sicuri e protetti da intrusioni e abusi; che forniscono un livello ragionevole di disponibilità, affidabilità e funzionamento corretto; che sono ragionevolmente adatti allo svolgimento delle funzioni previste e che attuano la policy di sicurezza applicabile. Un sistema attendibile non è necessariamente un "sistema fiduciario" come individuato dalla terminologia governativa classificata.
VeriSign® Repository	Il database di Symantec per Certificati ed altre informazioni attinenti al VeriSign® Trust Network accessibile on-line.
VeriSign® Trust Network (VTN)	L'Infrastruttura di Chiave Pubblica basata su Certificati e disciplinata dalla Policy di Certificazione del VeriSign Trust Network, che permette lo spiegamento e l'utilizzo di Certificati su scala mondiale da parte di Symantec e dei suoi Affiliati nonché dei loro rispettivi Clienti, Abbonati e Parti Facenti Affidamento.
VTN Participant	Un individuo o un'organizzazione che rientra in una o più delle categorie seguenti nell'ambito del

Termini	Definizioni
(Partecipante)	VTN: Symantec, un Affiliato, un Cliente, un Reseller, un Abbonato o una Parte FacenteAffidamento.
VTN Standards	I requisiti commerciali, legali e tecnici stabiliti per il rilascio, la gestione, la revoca, il rinnovo e l'utilizzo di Certificati nell'ambito del VTN.