Policy dei certificati

CA firma personale con firma cloud

(ETSI 102 042 e ETSI 101 456)

21/10/2014 (versione tradotta in italiano)

DBD Protezione e sottoscrizione della firma personale ETSI CP v 1.3

CA firma personale con firma cloud

(ETSI 102 042 e ETSI 101 456 e ETSI 319 411-1&2)

Versione	1.3	**Pagine**	77
Stato	□ Bozza	□ Finale	
Autore	Emmanuel Montacutelli	OpenTrust	

Lista di distribuzione	Esterna	Interna
Stato	Pubblica	Tutti gli impiegati

Storico

Data	Versione	Autore	Commenti	Verificato da
24/10/2013	1.0	EM	Creazione della versione 1.0	JYF
21/10/2014	1.1	EM	Integrazione del certificato di rinnovo regole per i sottoscrittori	JYF
15/02/2016	1.2	EM		

CONTENUTI

1 INTRODUZIONE

1.1 Riepilogo

Presente policy dei certificati (CP) definisce i requisiti applicabili alla gestione del ciclo di vita dei certificati digitali dei sottoscrittori forniti dal servizio di Protect and Sign (firma personale).

I certificati dei sottoscrittori vengono firmati dalle Certification Authority subordinate (Sub-CA) di proprietà della DOCUSIGN FRANCE o da un cliente della DOCUSIGN FRANCE (in conformità con [PSMP]).

I certificati elettronici emessi e gestiti in conformità con presente policy dei certificati, nel seguito chiamati "certificati dei sottoscrittori", vengono forniti agli utenti (nel seguito chiamati sottoscrittori) dei clienti Protect and Sign (firma personale) che utilizzano il servizio Protect and Sign (firma personale).

La PKI ha istituito un dominio sicuro che consiste in:

- Una Root Certification Authority (RCA, chiamata anche "Root CA"): utilizzata come trust anchor che firma i certificati CA intermedi e le Authority Revocation List associate (ARL). Per questa PKI, la RCA viene gestita da Adobe e viene chiamata "Adobe Root CA".

- CA intermedia (ICA): utilizzata per firmare le Sub-CA e le Authority Revocation List associate (ARL). Per questa PKI, la ICA viene gestita da DOCUSIGN FRANCE e viene chiamata "KEYNECTIS CDS CA".

- CA subordinate (Sub-CA), utilizzate per firmare i certificati dei sottoscrittori e le CRL. Per questa PKI è possibile avere 2 tipi di Sub-CA:

  - DOCUSIGN FRANCE Sub-CA: questa Sub-CA viene chiamata "CA firma personale con firma cloud".

  - Sub-CA cliente: questo tipo di Sub-CA è sempre ospitata da DOCUSIGN FRANCE nel suo centro dati e deve soddisfare i requisiti della presente CP. DOCUSIGN FRANCE deve approvare questo tipo di Sub-CA.

Questa CP si basa su:
- RFC 3647 « Policy dei certificati e struttura delle pratiche di certificazione » emessa dalla Internet Engineering Task Force (IETF).

- [ETSI 101 456]: Requisiti del ETSI 101 456 solo per i certificati qualificati. « Firme elettroniche e infrastrutture (ESI); requisiti policy per l'autorità di certificazione che emette i certificati qualificati », ETSI TS 101 456, v 1.4.3 (2007- 05).
- [Cert]: « X.509 V.3 profilo certificato per i certificati emessi per persone fisiche », ETSI TS 102 280 V1.1.1 (2004-03).
- [Qual cert]: « Profilo certificato qualificato », ETSI TS 101 862 V1.3.3 (2006-01).
- [ETSI 102 042]: "Requisiti della ETSI 102 042 (LCP) per il certificato rispetto solamente a questo standard. ETSI TS 102 042 V2.3.1 (2012-11), specifica tecnica firme elettroniche e infrastrutture (ESI); requisiti policy per le autorità di certificazione che emettono i certificati a chiave pubblica".
- [CRYPTO]: "ETSI TS 102 176-1 V2.0.0 (2007-11), specifica tecnica, firme elettroniche e infrastrutture (ESI); algoritmi e parametri per le firme elettroniche sicure; parte 1: Funzioni hash e algoritmi asimmetrici".
- [PSMP]: Firma attestata e policy di gestione, minimo versione 6.
- [Adobe CP per CDS]: "Adobe Systems Incorporated, policy dei certificati CDS ottobre 2005, revisione #14".
- [PSM SSCD]: "Secure Information Technology Center – Austria, CONFERMA IN FORZA DEL § 18 PARA. 5 SIGG, dispositivo di creazione della firma sicura, firma personale Protect & Sign, versione 4.1, conferma emessa il: 2015-12-03, numero di riferimento: A-SIT-1.117".

1.2 Nome documento e identificazione

Emessi con numeri OID indicati nella tabella sotto riportata con il link a [PSMP]:

PSMP (anche chiamato PSGP in francese) v6 OID	CP OID	Livello di fiducia
1.3.6.1.4.1.22234.2.4.6.1.8	1.3.6.1.4.1.22234.2.8.3.7	Certificato qualificato senza SSCD Certificato da un verificatore esterno
1.3.6.1.4.1.22234.2.4.6.1.7	1.3.6.1.4.1.22234.2.8.3.9	ETSI 102 042 (LCP) Certificato da un verificatore esterno
1.3.6.1.4.1.22234.2.4.6.1.15	1.3.6.1.4.1.22234.2.8.3.20	Certificato qualificato con SSCD Certificato da un verificatore esterno

Questa CP copre tutte queste 3 OID in un solo documento. Quando ci sono delle normative dedicate e particolari che possono essere descritte in una sezione della CP, l'OID viene utilizzato per identificare una sub-sezione nella CP, per poter identificare in modo chiaro le normative applicate per il livello menzionato in particolare.

1.3 Componenti PKI

DOCUSIGN FRANCE ha costituito una autorità di gestione della policy (PMA) per gestire i componenti PKI e i servizi. La PKI è composta da componenti descritti di seguito e supporta seguenti servizi (servizi PKI):

- generazione di una coppia di chiavi Sub-CA: genera le coppie di chiavi sub-CA e i CSR associati durante le cerimonie delle chiavi.

- registrazione dei sottoscrittori: consiste nel raccogliere e verificare l'identità dei sottoscrittori e le loro informazioni, che verranno utilizzate per costruire le richieste di certificato e/o verranno incluse nei certificati tecnici.

- generazione della coppia di chiavi per i sottoscrittori: consiste nel generare una coppia di chiavi per un sottoscrittore.

- generazione del certificato sottoscrittori: genera i certificati dei sottoscrittori.

- autenticazione della richiesta di revoca dei sottoscrittori (solo per casi di emergenza, in accordo con il contratto firmato tra la DocuSign France e il cliente): consiste nella raccolta delle informazioni, per autenticare una richiesta di revoca e trasmettere una richiesta di revoca alla CA.

- revoca dei certificati dei sottoscrittori (solo per certificato in corso di validità): se il link tra un sottoscrittore e la chiave pubblica inclusa nel suo certificato non viene più considerata valida, la CA revoca il certificato del sottoscrittore.

- generazione del percorso log: genera log che vengono usati per la verifica o per essere analizzati per risolvere un incidente.

- pubblicazione di un CRL: un CRL viene emesso dalla CA per il certificato sottoscrittori. Questo CRL è sempre vuoto perché non c'è un servizio di revoca per i sottoscrittori.

- servizi OCSP: La CA consegna le informazioni sullo stato OCSP per il certificato sottoscrittori.

- servizi pubblicazione: pubblicazione del certificato Sub-CA e di tutte le informazioni rilevanti relative all'utilizzo dei servizi Sub-CA e del certificato sottoscrittori.

Questa CP fornisce i requisiti di sicurezza applicabili a tutti i servizi, mentre il Certification Practice Statement (CPS) associato darà maggiori dettagli relativi alle pratiche attuate da ogni componente che partecipa alle attività della PKI.

1.3.1 Autorità di gestione della policy (PMA)

La PMA è l'autorità che conduce la PKI ed è gestita da DOCUSIGN FRANCE.

La PMA approva la CP e il Certification Practice Statement (CPS) utilizzato a supporto dei servizi di certificazione della PKI.

La PMA definisce l'organizzazione dei componenti e dei servizi della PKI, è competente per la nomina dei componenti della PKI e per la verifica che i servizi che forniscono osservino le sezioni applicabili di questa CP e la sua CPS corrispondente.

La missione principale PMA minima è seguente:

- Approva i servizi e i prezzi della PKI che devono essere forniti dall'infrastruttura PKI.

- Approva le policy dei certificati.

- Approva la creazione e la revoca della CA.

- Approva la scelta della RCA e della ICA utilizzate per firmare la Sub-CA.

- Approva la specifica crittografica (algoritmi utilizzati per la firma, la codifica, l'autenticazione, funzioni hash e la lunghezza delle chiavi, la durata operativa) dei sistemi PKI e i cambiamenti relativi.

- Approva le specifiche dei token crittografici che generano le chiavi e ospitano i certificati dei sottoscrittori

- Approva gli standard delle applicazioni della PKI. Questo assicura il livello richiesto di interoperabilità e l'accettazione da parte della RCA.

- Approva la conformità tra i documenti sulla pratica di sicurezza e le policy relative (per esempio CPS/CP).

- Approva il report annuale finale di verifica interna di tutti i componenti PKI.

- Approva il report di verifica esterna della RA eseguita da DocuSign France.

- Gestisce la verifica esterna della RA.

- Approva il protocollo di approvazione selezionato, definito con DocuSign France.

- Approva le procedure definite dal cliente per la gestione dei sottoscrittori.

- Garantisce la validità e l'integrità delle informazioni pubblicate dalla PKI.

- Assicura che abbia luogo un processo adeguato per gestire gli incidenti di sicurezza all'interno dei servizi della PKI e dei componenti PKI.

- Arbitra le controversie relative ai servizi della PKI e l'utilizzo dei certificati e assicura che venga pubblicata la deliberazione di tali controversie.

1.3.2 Certification Authority subordinata (Sub-CA)

La Sub-CA è di proprietà della DOCUSIGN FRANCE o di un cliente, e viene operata dalla DOCUSIGN FRANCE.

La Sub-CA supporta i seguenti servizi della PKI:

- generazione delle coppie di chiavi Sub-CA.

- generazione del certificato sottoscrittori.

- revoca dei certificati sottoscrittori (in accordo con il contratto tra DocuSign France e il cliente)

- pubblicazione di una CRL.

- generazione di un percorso log.

Una Sub-CA opera i suoi servizi in accordo con presente CP e la corrispondente CPS. Una Sub-CA non può iniziare a operare senza una preventiva approvazione della PMA.

1.3.3 Autorità di registrazione (RA)

La RA è di proprietà del cliente e viene operata dall'entità designata dal cliente.

La RA supporta i seguenti servizi della PKI:

- autenticazione della richiesta di revoca del sottoscrittore.

- registrazione del sottoscrittore.

- generazione di un percorso log.

La RA è designata e autorizzata dalla Sub-CA, in base a un contratto. Di conseguenza, la RA documenta e attua le procedure per l'identificazione delle entità legali e gli individui privati, in accordo con le regole da lei definite in base alle sue esigenze, in particolare nel protocollo di approvazione. Il suo ruolo è quello di provare che il richiedente corrisponda all'identità e alle caratteristiche indicati nel certificato. Queste procedure di identificazione variano a seconda del livello di fiducia che la RA decida di applicare su questa verifica.

La RA è responsabile della definizione delle procedure che si riferiscono specialmente alle sezioni 3, 4, 5, 6, 8 e 9 della presente CP che si riferisce alla RA. Se il cliente designa un'entità legale che differisce dal cliente, deve essere stipulato un contratto o documento legale conforme al link tra il cliente e l'entità legale designata dal cliente. Questo contratto deve essere stipulato tra il cliente e l'entità legale designata dal cliente, per poter coprire i servizi della RA interessati dall'entità designata.

Le procedure per gestire i sottoscrittori, definite dalla RA, vengono eseguite da un operatore RA. La RA è responsabile della istituzione e del mantenimento di una lista di operatori RA che contiene tutti gli operatori RA che sono autorizzati a iscrivere i sottoscrittori.

La CPS fornisce i dettagli sul come una RA è organizzata ed esegue le sue operazioni, conformemente al tipo di certificato da fornire a un sottoscrittore.

Una RA opera i suoi servizi in accordo con presente CP e la corrispondente CPS. Una RA non può iniziare a operare senza una preventiva approvazione della PMA.

1.3.4 Autorità operativa (OA)

L'autorità operativa (OA) è l'entità che ospita e gestisce tutto il software, il hardware e il HSM utilizzato per supportare i servizi della PKI. L'OA è l'entità che configura e realizza tutte le operazioni per i servizi della PKI. La CPS fornisce i dettagli sul come ogni sevizio viene fornito a ogni componente PKI.

I componenti PKI sono operati da:

– DOCUSIGN FRANCE che è l'OA per la Sub-CA e il PS.

– il cliente che è l'OA per la RA.

La OA opera i suoi servizi in accordo con presente CP e la corrispondente CPS. La OA non può iniziare a operare senza una preventiva approvazione della PMA.

1.3.5 Servizio di pubblicazione (PS)

Il PS è di proprietà della DOCUSIGN FRANCE, e viene operata dalla DOCUSIGN FRANCE.

Il servizio di pubblicazione (PS) è l'archivio DOCUSIGN FRANCE (vedi capitolo 2 in basso) che fornisce seguenti servizi della PKI:

- servizi di pubblicazione (vedi sezione 2 in basso).

- generazione di un percorso log.

1.3.6 Sottoscrittori

Un sottoscrittore è una persona fisica la cui identità risulta come soggetto in un certificato sottoscrittori e che firma un documento utilizzando il servizio Protect and Sign (firma personale). La generazione della coppia di chiavi e del certificato del sottoscrittore è collegata all'operazione di firma eseguita dal sottoscrittore conformemente a [PSMP] e ai regolamenti del cliente, descritti nei documenti del cliente, attuati tecnicamente nel protocollo di approvazione.

I sottoscrittori tengono fede al presente CP e alle procedure ad essa associate, così come sono descritte nella documentazione RA.

1.3.7 Altri partecipanti

1.3.7.1 Il cliente

Il cliente è una entità legale che stipula un contratto con la DOCUSIGN FRANCE per utilizzare il servizio Protect and Sign (Firma personale). Il cliente designa una entità che è la RA. Nel contratto tra il cliente e DOCUSIGN FRANCE, tutti gli obblighi della RA sono inclusi. Il cliente definisce le regole di iscrizione che la RA deve applicare, seleziona il livello di fiducia per il certificato sottoscrittori e seleziona e definisce il protocollo di approvazione.

Il protocollo di approvazione deve richiedere ai sottoscrittori l'uso di dati di attivazione tecnica. La RA deve essere verificata conformemente ai regolamenti definiti nella sezione 8 in basso.

1.3.7.2 Utilizzatori

Gli utilizzatori sono le entità che agiscono affidandosi sulla validità del legame dell'identità dei sottoscrittori con una chiave pubblica. Un utilizzatore del certificato è responsabile di decidere sul come controllare la validità di un certificato sottoscrittori, almeno controllando le informazioni appropriate sullo stato del certificato (utilizzando risposte CRL e ARL o OCSP) per i certificati sottoscrittori, Sub-CA, ICA e Root CA. Un utilizzatore del certificato può utilizzare le informazioni sul certificato (come gli identificatori della policy dei certificati) per appurare l'idoneità del certificato per un utilizzo particolare.

1.4 Utilizzo del certificato

1.4.1 Utilizzo appropriato del certificato

1.4.1.1 Certificato Sub-CA

Un certificato Sub-CA viene utilizzato per convalidare i certificati dei sottoscrittori e CRL, oltre al certificato OCSP che ha fornito.

Ogni chiave privata Sub-CA può firmare i seguenti tipi di certificati:

- CSR Sub-CA.

- certificato sottoscrittori.

1.4.1.2 Sottoscrittori

La chiave privata viene utilizzata in seguenti modi:

- per firmare documenti elettronici conformemente al protocollo di approvazione (con una dati di attivazione tecnici) e alla policy di firma del cliente.

- per firmare CSR (formato Pkcs#10).

Il certificato viene utilizzato in seguenti modi:

- per verificare la firma elettronica applicata su un documento che utilizza il servizio Protect and Sign (Firma personale).

1.4.2 Utilizzo vietato del certificato

Presente CP non copre un utilizzo diverso da quelli indicati nella sezione 1.4.1 in alto riportata.

La DocuSign France non è responsabile per l'uso diverso da quelli indicati in presente CP.

1.5 Gestione della policy

1.5.1 Organizzazione che gestisce il documento

La PMA è responsabile di tutti gli aspetti di presente CP e la CPS associata.

1.5.2 Persona di riferimento

La persona da contattare è:

– DocuSign France;

– Mr. Thibault de Valroger;

– Contatto: Direttore, Sviluppo Aziendale;

– DocuSign France – 175, rue Jean-Jacques Rousseau - 92131 Issy-les-Moulineaux Cedex – Francia;

– E-mail: PMA-DocuSignFrance@docusign.fr;

– Telefono: (+33) (0)1 53 94 22 00;

– Fax: (+33) (0)1 53 94 22 01.

1.5.3 Persona che appura l'adeguatezza del CPS alla policy

Il PMA approva il CPS. La PKI viene verificata periodicamente per verificare l'osservanza delle linee guida e degli standard PMA approvati dalla PMA. La verifica garantisce che la CPS è applicata correttamente e che è conforme alla CP. Inoltre, la PMA si riserva il diritto di verificare la PKI come indicato nella sezione 8 di presente CP.

In ogni caso, la determinazione dell'osservanza si basa su verifiche indipendenti.

1.5.4 Procedure di approvazione CPS

Le modifiche devono avvenire in forma di una nuova CPS (con una somma delle modifiche) o una notifica di aggiornamento che contiene le modifiche e i riferimento nella CPS precedente. La creazione o modifica della CPS esistente rimane a discrezione della PMA. Una nuova CPS sostituisce automaticamente la precedente e diventa operativa appena la PMA l'ha approvata. Le nuove CPS o gli aggiornamenti della CPS esistente devono essere conformi alla presente CP, prima dell'approvazione.

1.6 Definizioni e acronimi

1.6.1 Definizioni

Termine	Definizione
Accreditamento	Dichiarazione formale da una Approving Authority designata che un sistema informativo è stato approvato a operare in una particolare modalità di sicurezza, utilizzando un pacchetto di misure di salvaguardia prescritto, a un livello accettabile di rischio.
Dati di attivazione	Dati segreti (per es.: password, codice PIN, certificato o OTP) utilizzati per eseguire delle operazioni crittografate, utilizzando una chiave privata.
Verifica	Una revisione e ispezione indipendente di documentazioni, record e attività per accedere all'adeguatezza dei controlli di sistema, per assicurare l'osservanza delle policy e delle procedure operative stabilite, e per consigliare le modifiche necessarie nei controlli, nelle policy o nelle procedure.
Autenticazione	Il processo ove una parte ha presentato una identità e rivendicazioni di essere tale identità, e la seconda parte conferma che questa asserzione di identità è vera.
Dati di autenticazione	Dati di attivazione tecnici particolara>BD.9 85.944 57.48 reW*nBT/F3 9e8563 acti) Dad)3.85 405.1299 E3 eW*n50 1 P /MCID Tf1 0 0 1 56.64 371.091Tm0 36[(A)4(ute)-7(n)4(p)-9(

Lavorazione del certificato	Il processo dell'accettazione di una chiave pubblica e delle informazioni identificative da un sottoscrittore autorizzato, che produce un certificato digitale che contiene queste e altre informazioni pertinenti e che firma digitalmente il certificato.
Policy dei certificati (CP)	Un pacchetto denominato di regolamenti che indica l'applicabilità di un certificato a una comunità particolare e/o classe di applicazioni con requisiti comuni di sicurezza.
Richiesta di certificato	Un messaggio inviato da un cliente a una Sub-CA, per richiedere un certificato digitale. La richiesta di certificato contiene le informazioni che identificano il sottoscrittore a volte i dati di attivazione.
Certificate Revocation List (CRL)	Una lista dei certificati revocati che viene creata e firmata da una CA. Un certificato viene aggiunto alla lista se è revocato (per es. a causa di una sospetta compromissione della chiave, per la modifica del nome distinto (DN)), che poi viene rimosso dalla lista quando ha raggiunto la fine del periodo di validità del certificato. In alcuni casi, la CA potrebbe scegliere di suddividere la CRL in una serie di CRL più piccole. Se un sottoscrittore sceglie di accettare un certificato, l'accordo per l'utilizzatore del certificato richiede che questo utilizzatore del certificato controlli che il certificato non sia elencato sull'ultima CRL emessa.
Periodo di validità del certificato	Il periodo di validità del certificato è l'intervallo di tempo durante il quale la CA garantisce che manterrà le informazioni sullo stato del certificato. [RFC 3280].
Percorso di certificazione (anche detto percorso sicuro o catena di certificazioni sicure)	Una catena di certificati multipli necessari per validare un certificato che contiene la chiave pubblica richiesta. Una catena di certificati consiste in un certificato RCA (anchor), un certificato CA e i certificati dei sottoscrittori firmati dalla CA.
Certification Practice Statement (CPS)	Una dichiarazione di pratiche che un CA esegue nell'emettere e revocare i certificati, e nel fornire l'accesso ai certificati. La CPS definisce l'equipaggiamento e le procedure che la CA utilizza per soddisfare e requisiti specificati nella CP e che sono supportati da essa.
Criteri comuni	I criteri comuni per la valutazione della sicurezza della tecnologia delle informazioni sono uno standard internazionale (ISO/IEC 15408) per la certificazione della sicurezza della tecnologia delle informazioni.
Compromissione	Una violazione (o violazione sospetta) di una policy di sicurezza, in cui può essersi verificata una divulgazione non autorizzata di informazioni sensibili, o la perdita del controllo sulle informazioni sensibili. In riferimento alle chiavi private, una compromissione è una perdita, un furto, una divulgazione, una modifica, un utilizzo non autorizzato o un'altra compromissione della sicurezza di una tale chiave privata.
Riservatezza	La caratteristica che le informazioni non vengono rese disponibili o diffuse a individui, entità o processi non autorizzati [ISO/IEC 13335-1:2004].
Dominio crittografato (per HSM)	Ambiente sicuro che contiene una o più chiavi e che viene gestito con dati di attivazione dedicati. Questo ambiente sicuro è utilizzato in un Hardware Security Module (HSM), per attivare e utilizzare le chiavi.
Protocollo di approvazione	Documento in cui il cliente specifica tutti i regolamenti da seguire da una determinata applicazione di un cliente che utilizza il servizio Protect and Sign (Firma personale), inclusi: (i) la definizione delle azioni che devono essere eseguite dai sottoscrittori per firmare il documento proposto dal cliente, (ii) i termini e le condizioni dei sottoscrittori, (iii) i metodi utilizzati dal servizio Protect and Sign (Firma personale) per autenticare i

	sottoscrittori all'operazione di firma e quindi alla generazione della coppia di chiavi e del certificato dei sottoscrittori, e (iv) il tipo di file presentato dal cliente e che deve essere firmato (XML/PDF…).
Firma digitale	Il risultato della trasformazione di un messaggio ai sensi di un sistema crittografato che utilizza chiavi che possono essere determinate da una persona che ha ricevuto un messaggio firmato digitalmente: Se la trasformazione è stata creata utilizzando la chiave di firma privata che corrisponde alla chiave di verifica pubblica del firmatario. Se il messaggio è stato alterato dal momento che è stata fatta la trasformazione.
Directory	Un sistema di directory che è conforme alla serie di raccomandazioni ITU-T X.500.
Piano di ripristino in caso di disastro	Un piano definito dalla CA per recuperare in parte o totalmente i suoi servizi della PKI, dopo che sono stati distrutti in seguito a un disastro, in un rinvio definito nella CP/CPS.
Nome distinto	Uno string creato durante il processo di certificazione e incluso nel certificato che identifica in modo univoco il sottoscrittore all'interno di un dominio CA.
Coppia di chiavi di codifica	Una coppia di chiavi pubblica e privata per criptare e decriptare i dati.
Standard di lavorazione delle informazioni federali (FIPS)	Standard federali che descrivono dei requisiti di performance specifici, pratiche, formati, protocolli di comunicazione, ecc. per operazioni di telecomunicazioni, dati, software, hardware, ecc. Le agenzie federali americane sono obbligate ad applicare questi standard come specificato, a meno che non sia stata accordata una deroga in accordo con le procedure di deroga dell'agenzia.
Hardware Security Module (HSM)	Un HSM è un dispositivo di hardware utilizzare per generare coppie di chiavi crittografate, tenere sicura la chiave privata e generare firme digitali. È utilizzato per tenere al sicuro le chiavi CA, e in alcuni casi le chiavi di alcune applicazioni (sottoscrittori).
Hardware Token	Un dispositivo hardware che può tenere chiavi private, certificati digitali, o altre informazioni elettroniche che possono essere utilizzati per l'autenticazione o l'autorizzazione. Smart card e USB token sono degli esempi di hardware token.
Funzione hash	Una funzione che mappa le string dei bit a delle string di bit a lunghezza fissa, che soddisfano seguenti due caratteristiche: - Dal punto di vista informatico è impossibile trovare un input per un output dato che possa mappare per arrivare a questo output; - Dal punto di vista informatico è impossibile trovare un secondo input per un input dato che possa mappare per arrivare allo stesso output [ISO/IEC 10118-1].
Internet Engineering Task Force (IETF)	La Internet Engineering Task Force è una grande comunità internazionale aperta per network designer, operatori, venditori e ricercatori, occupati con lo sviluppo dell'architettura di internet e regolare funzionamento di internet.
Integrità	Si riferisce alla correttezza delle informazioni, del mittente delle informazioni e il funzionamento del sistema che le processa.
Interoperabilità	Implica che l'equipaggiamento e le procedure in uso da una o più entità son compatibili e quindi che è possibile intraprendere delle attività comuni o relative.
Cerimonia delle chiavi (KC)	Una cerimonia delle chiavi (KC) è una operazione che abilita la gestione (generazione e distruzione) delle coppie di chiavi crittografate e il ciclo di vita CA (firma del certificato e

	revoca). Una cerimonia delle chiavi richiede un numero minimo di impiegati fidati che rappresentano il proprietario della PKI.
Generazione chiavi	Il processo di creare una chiave privata e una coppia di chiavi pubbliche.
Identificatore di oggetti (OID)	Un identificatore di oggetti è una sequenza di numeri formattata in modo speciale, registrata con una organizzazione di standard riconosciuti a livello internazionale.
OCSP	Protocollo utile nell'appurare lo stato attuale di un certificato digitale, senza la richiesta di CRL.
Periodo operativo di un certificato	Il periodo operativo di un certificato è il periodo della sua validità. Di norma inizia con la data in cui è stato emesso il certificato (o una data successiva specificata nel certificato) e termina con la data e l'ora in cui scade, come indicato sul certificato o precedentemente, se revocato.
Organizzazione	Direzione, agenzia, partnership, trust, joint-venture o un'altra associazione.
PIN	Numero Personale di Identificazione. Vedi i dati di attivazione per la definizione
PKCS #10	Standard crittografia chiave pubblica #10, sviluppato da RSA Security Inc., che definisce una struttura per una richiesta di firma del certificato.
Dichiarazione di divulgazione PKI (PDS)	Definita dal RFC 3647 della IETF come "Uno strumento che integra una CP o CPS divulgando informazioni critiche sulle policy e le pratiche di una CA/PKI. Una PDS è un veicolo per divulgare ed enfatizzare le informazioni che normalmente sono coperte nel dettaglio dai documenti CP e/o CPS associati. Di conseguenza, una PDS non ha lo scopo di sostituire una CP o CPS.
PKIX	Gruppo di lavoro IETF ufficialmente costituito per sviluppare delle specifiche tecniche per componenti PKI basate su certificati X.509 versione 3.
Chiave privata	La chiave privata di una coppia di chiavi utilizzata per eseguire la crittografia della chiave pubblica. Questa chiave deve essere tenuta segreta.
Chiave pubblica	La chiave pubblica di una coppia di chiavi utilizzata per eseguire la crittografia della chiave pubblica. La chiave pubblica è disponibile liberamente da chiunque la richieda. La chiave pubblica viene normalmente fornita tramite un certificato emesso da una Certification Authority ed è spesso ottenuta accedendo a un archivio.
Infrastruttura a chiave pubblica (PKI)	Una serie di policy, processi, piattaforme server, software e postazioni di lavoro utilizzati per gestire i certificati e le coppie di chiavi pubbliche-private, inclusa la capacità di emettere, mantenere e revocare i certificati a chiave pubblica.
Coppia di chiavi pubbliche/private (anche chiamata coppia di chiavi)	Due chiavi relazionate matematicamente, che hanno caratteristiche che (i) una chiave può essere utilizzata per criptare dati che possono essere decriptati solo utilizzando un'altra chiave, e (ii) conoscendo una delle chiavi ce è chiamata chiave pubblica, è impossibile dal punto di vista informatico scoprire l'altra chiave che è chiamata chiave privata.
Spazio dominio Sub-CA	Lo spazio dominio Sub-CA è il pacchetto di tutti i certificati forniti dalla Sub-CA.
Registrazione	Il processo con cui l'utente si rivolge alla Certification Authority per avere un certificato digitale.

Archivio	Servizio di pubblicazione che fornisce le informazioni necessarie per assicurare l'operazione desiderata per i certificati digitali emessi (per es.: CRL, codifica certificati, certificati CA).
Revoca	Porre fine prematuramente il periodo operativo di un certificato da una data specificata in poi.
RFC3647	Documento pubblicato dalla IETF, che rappresenta il quadro per assistere gli scrittori di policy dei certificati o le certification practice statement per i partecipanti all'interno delle infrastruttura a chiave pubblica, come le certification authority, le policy authority e le comunità interessate che desiderano affidarsi ai certificati. In particolare, il quadro fornisce una lista completa di argomenti che necessitano potenzialmente (a discrezione dello scrittore) di essere coperte da una policy dei certificati o da una certification practice statement.
RSA	Un sistema crittografato a chiave pubblica inventato da Rivest, Shamir e Adelman.
Coppia di chiavi per firma	Una coppia di chiavi pubbliche e private utilizzata per firmare digitalmente i documenti elettronici e per verificare le firme digitali.
Ruoli di fiducia	Quegli individui che eseguono un ruolo di sicurezza che è critico per l'operazione o l'integrità di presente PKI.
Sistema affidabile	Hardware computer, software, e/o procedure che: (a) sono ragionevolmente sicuri contro intrusioni e abusi; (b) forniscono un livello ragionevole di disponibilità, affidabilità e operazione corretta; (c) sono ragionevolmente adatti all'esecuzione delle loro funzioni previste e (d) aderiscono alle procedure di sicurezza generalmente accettate.
Certificato valido	Un certificato che (1) è stato emesso da una Certification Authority, (2) è stato accettato dai sottoscrittori che vi sono elencati, (3) non è scaduto e (4) non è stato revocato. Così, un certificato non è "valido" finché non è stato sia emesso da una CA sia accettato dai sottoscrittori.

1.6.2 Acronimi

Acronimo	Significato
AES	Advanced Encryption Standard (standard di codifica avanzato)
ARL	Authority Revocation List (lista di revoca dell'autorità)
CA	Certification Authority (autorità di certificazione)
CDS	Adobe Certified Document Services (servizi per i documenti certificati Adobe)
CP	Certificate Policy (policy dei certificati)
CPS	Certification Practice Statement (dichiarazione della pratica di certificazione)
CRL	Certification Revocation List (lista di revoca della certificazione)

CSR	Certificate Signing Request (richiesta di firma del certificato)
DES	Data Encryption Standard (standard di codifica dei dati)
DN	Distinguished Name (nome distinto)
EAL	Evaluation assurance level (livello di assicurazione della valutazione), normativa ISO 15408 (criteri comuni) per la certificazione dei prodotti di sicurezza
FIPS	United States of America, Federal Information Processing Standards (standard di lavorazione delle informazioni federali degli Stati Uniti d'America)
HTTP	Hypertext Transport Protocol (protocollo di trasporto degli ipertesti)
IP	Internet Protocol (protocollo internet)
ISO	International Organization for Standardization (organizzazione internazionale per la standardizzazione)
LDAP	Lightweight Directory Access Protocol (protocollo di accesso alle directory rapido e snello)
MBUN	"Meaningless But Unique Number" un numero che viene assegnato dalla PKI per aiutare i sottoscrittori nella differenziazione rispetto a caratteristiche altrimenti similari.
MofN	M out of N (schema soglia) (M di N)
O	Organization (organizzazione)
OCSP	Online Certificate Status Protocol (protocollo dello stato del certificato online)
OID	Object Identifier (identificatore degli oggetti)
OU	Organizational Unit (unità organizzativa)
PIN	Personal Identification Number (numero personale di identificazione)
PKCS	Public-Key Cryptography Standard (standard della crittografia della chiave pubblica)
PKI	Public Key Infrastructure (infrastruttura a chiave pubblica)
PS	Publication Service (servizio di pubblicazione)
RCA	Root Certification Authority (autorità di certificazione del root)
RFC	Request For Comment (richiesta di commento)
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm (algoritmo del hash sicuro)
SSL	Secure Socket Layer (sistema di accesso sicuro)
SSCD	Secure Signature Creation Device (dispositivo di creazione di una firma sicura)
Sub-CA	Subordinate CA (CA subordinata)

TDES	Triple DES
TLS	Transport Layer Security (sicurezza del sistema di trasporto)

2 RESPONSABILITÀ PUBBLICAZIONE E ARCHIVIO

2.1 Archivi

Il servizio di pubblicazione è responsabile di rendere disponibile qualsiasi informazione pubblica relativa ai servizi Sub-CA.

Il PS deve essere così utilizzato per fornire degli elevati livelli di affidabilità (24 ore su 24, 7 giorni su 7)

2.2 Pubblicazione delle informazioni sulla certificazione

Il PS pubblica i seguenti dati:

- CP: http://www.OpenTrustdtm.com/

- certificato Sub-CA OPENTRUST: http://www.OpenTrustdtm.com/

- certificato Sub-CA del cliente: pubblicato dal cliente quando la CA è di proprietà del cliente e dal DOCUSIGN FRANCE quando la CA è di proprietà della DOCUSIGN FRANCE.

- CRL: vedi sezione 10 in basso.

La CA assicura che i termini e le condizioni sono rese disponibili ai sottoscrittori e all'utilizzatore del certificato come segue:

– Sottoscrittori: i termini e le condizioni mostrati ai sottoscrittori durante il protocollo di approvazione e firmati dai sottoscrittori durante il protocollo di approvazione.

– Utilizzatore del certificato: i termini e le condizioni e le informazioni che la ETSI richiede essere pubblicati per l'utilizzatore del certificato sono già contenuti nel presente CP nelle sezioni; 1.4, 4.5.2, 5.5, 9, 9.6, 9.7, e 9.8.

– Il cliente è responsabile per la istituzione e la disponibilità dei termini e delle condizioni particolari per il completamento dei requisiti ETSI per l'utilizzatore del certificato e i sottoscrittori.

2.3 Data o frequenza della pubblicazione

Le informazioni identificate nella sezione 2.2 in alto vengono rese disponibili:

- CP:

o Prima di iniziare il servizio per la CP iniziale.

o Non più tardi di 48 ore successivamente a qualsiasi aggiornamento o sostituzione della CP approvati dalla PMA.

- certificato Sub-CA:

o Prima di iniziare il servizio per la Sub-CA iniziale ed entro 48 ore dalla generazione dei certificati Sub-CA successivi a un rinnovo o a una ricreazione di una chiave.

2.4 Controlli di accesso agli archivi

Il PS è responsabile per il pacchetto di policy di sicurezza che concede l'accesso alle informazioni pubblicate.

L'accesso per leggere le informazioni è disponibile a livello pubblico e internazionale tramite internet, in linguaggio comprensibile, per le seguenti informazioni per il certificato CP e Sub-CA.

3 IDENTIFICAZIONE E AUTENTICAZIONE

3.1 Denominazione

3.1.1 Tipi di nomi

I campi attributo "Nome emittente" e "Soggetto" devono essere conformi alla RFC 5280. I dettagli relativi al tipo di codifica da usare sono riportati in basso.

3.1.1.1 Sub-CA

Il contenuto del DN per i certificati Sub-CA viene dettagliato nella sezione 10 in basso.

3.1.1.2 Sottoscrittori

Il contenuto del DN per i certificati dei sottoscrittori viene dettagliato nella sezione 10 in basso.

3.1.2 Necessità di avere nomi significativi

I certificati emessi in base a presente CP sono significativi solo se i nomi che appaiono sui certificati possono essere capiti e usati dagli utilizzatori. I nomi utilizzati nei certificati devono identificare la persona a cui vengono assegnati in modo significativo e devono essere in linea con la carta d'identità del sottoscrittore

3.1.2.1 Sub-CA

Una coppia di chiavi può essere connessa solo con un CN univoco per ogni certificato Sub-CA.

3.1.2.2 Sottoscrittori

La RA è l'unica responsabile per la definizione dell'identità dei sottoscrittori da indicare nel certificato sottoscrittori.

Solo i certificati dei sottoscrittori con il nome della RA nel campo "OU" possono essere emessi (vedi sezione 10.3 e 10.4 in basso) dalla Sub-CA.

3.1.3 Anonimità o pseudonimo del certificato

Presente policy non consente certificati anonimi. Tutti i certificati devono contenere le informazioni dalla directory aziendale o inserite manualmente dalla RA.

3.1.4 Regole per l'interpretazione di varie forme di nomi

3.1.4.1 Sub-CA

Gli utilizzatori devono utilizzare il nome del soggetto contenuto nel certificato (vedi sezione 3.1.1) per identificare la Sub-CA.

3.1.4.2 Sottoscrittori

I certificati dei sottoscrittori possono essere identificati utilizzando il campo CN contenuto nel DN e gli indirizzi e-mail dei sottoscrittori contenuti nell'estensione "Nome alternativo del soggetto" e il campo E contenuto nel DN. Non è garantito che il campo CN sia univoco.

3.1.5 Unicità dei nomi

3.1.5.1 Sub-CA

I nomi contenuti nei certificati Sub-CA (vedi sezione 3.1.1 in alto) devono essere univoci nel dominio sicuro ICA, e tutti i nomi devono essere forniti all'entità che fornisce i servizi ICA, per essere inclusi negli appropriati valori vincolanti il nome del certificato Sub-CA.

3.1.5.2 Sottoscrittori

L'unicità di un certificato si basa su l'unicità del suo numero di serie all'interno del dominio della CA.

La RA deve essere responsabile della sicurezza dell'unicità del DN nei certificati emessi dalla Sub-CA e della gestione dei conflitti relativi al DN. Per fare ciò, la RA deve creare un TransNUM univoco per ogni sottoscrittore e documento firmato da inserire da parte della CA nel DN del certificato sottoscrittori.

3.1.6 Riconoscimento, autenticazione e funzione dei marchi

Nessuna stipulazione.

3.2 Validazione iniziale dell'identità

3.2.1 Metodo per comprovare il possesso della chiave privata

3.2.1.1 Sub-CA

Le coppie di chiavi Sub-CA devono essere generate, archiviate, attivate, utilizzate e distrutte dalla OA in un modo che dimostra alla PMA che ogni Sub-CA possiede la chiave privata corrispondente alla chiave pubblica contenuta nel suo certificato Sub-CA.

3.2.1.2 Sottoscrittori

Per i certificati dei sottoscrittori, la prova della proprietà della chiave privata corrispondente al certificato sottoscrittori utilizzato per firmare, viene fornita dalle risorse tecniche e organizzatrici definite nel protocollo di approvazione, scelto dal cliente, utilizzato e applicato come parte del servizio Protect and Sign (Firma personale) quando viene fatta la richiesta di certificato.

3.2.2 Autenticazione dell'identità dell'organizzazione

Lì dove il sottoscrittore è una persona che è l'identificatore in associazione con una persona legale o un'altra entità organizzativa, deve essere presentata una dimostrazione verificata dalla RA, di:

– Il nome completo e lo stato legale della persona legale associata o dell'altra entità organizzativa.

– Qualsiasi informazioni di registrazione rilevante esistente (per es. la registrazione della società) della persona legale associata o dell'altra entità organizzativa.

– Dimostrazione che il oggetto è associato alla persona legale o all'entità organizzativa.

3.2.3 Autenticazione dell'identità della persona fisica

3.2.3.1 Sottoscrittori

La RA è responsabile anche della raccolta e la conservazione delle informazioni richieste, per poter fornire una prova dell'identità dei sottoscrittori indicata nel certificato.

L'iscrizione di un utente prima dell'emissione del certificato sottoscrittori viene eseguita direttamente dalla RA.

I regolamenti di verifica dell'identità dei sottoscrittori sono a discrezione della RA, che è competente per la gestione dei sottoscrittori.

La procedura per l'identificazione, autenticazione e validazione di una richiesta di emissione di un certificato viene descritta nella policy di gestione della prova e nel protocollo di approvazione utilizzati per ogni cliente che utilizza i certificati dei sottoscrittori, e viene completata da una procedura specifica per la linea commerciale della RA definita dal cliente.

Il metodo di assegnazione di questa identità è quindi definita dal cliente, che iscrive tutti i suoi utenti con i loro dati di identificazione.

I regolamenti particolari devono essere applicati dal cliente conformemente alla sua scelta di OID.

3.2.3.1.1 OID: 1.3.6.1.4.1.22234.2.8.3.7 e 1.3.6.1.4.1.22234.2.8.3.20

La RA, al momento della registrazione, deve verificare con mezzi appropriati e in conformità con la legge nazionale, l'identità e, se applicabile, qualsiasi caratteristica specifica della persona alla quale viene emesso un certificato qualificato. La prova dell'identità deve essere verificata con una persona fisica direttamente, oppure deve essere controllata indirettamente utilizzando dei mezzi che forniscono una sicurezza equivalente alla presenza fisica. La prova inoltrata può essere in forma cartacea o in forma di documentazione elettronica.

Per i sottoscrittori, è necessario che venga fornita la prova di:

– Il nome completo (incluso il cognome e i nomi, in conformità con la legge applicabile e le pratiche di identificazione nazionale).

– La data e il luogo di nascita, il numero di identità riconosciuto a livello nazionale, o gli altri attributi che possono essere utilizzati, in quanto possibile, per distinguere la persona dalle altre persone con lo stesso nome.

Si consiglia di indicare il luogo in accordo con la convenzione nazione per le nascite registrate.

Nota: Un esempio di prova controllata indirettamente sulla persona fisica è la documentazione presentata per la registrazione, che è stata acquisita come risultato di una domanda che richiede la presenza fisica.

3.2.3.1.2 OID: 1.3.6.1.4.1.22234.2.8.3.9

La RA deve raccogliere la prova diretta o l'attestazione da una fonte appropriata e autorizzata, dell'identità (per es. nome) e, se applicabile, di qualsiasi caratteristica specifica dei sottoscrittori al quale è stato emesso un certificato.

La prova inoltrata può essere in forma cartacea o in forma di documentazione elettronica. La verifica dell'identità del sottoscrittore deve avvenire al momento della registrazione, tramite mezzi appropriati e in accordo con la legge nazionale.

Per i sottoscrittori, è necessario che venga fornita la prova di:

– Il nome completo (incluso il cognome e i nomi, in conformità con la legge applicabile e le pratiche di identificazione nazionale).

– La data e il luogo di nascita, il numero di identità riconosciuto a livello nazionale, o gli altri attributi che possono essere utilizzati, in quanto possibile, per distinguere la persona dalle altre persone con lo stesso nome.

Si consiglia di indicare il luogo in accordo con la convenzione nazione per le nascite registrate.

3.2.4 Validazione dell'autorità

L'autenticazione e l'identificazione dell'autorità di un sottoscrittore vengono eseguite dalla RA utilizzando e verificando le informazioni richieste nella sezione 3.2.2 in alto.

Qualsiasi certificato emesso da una CA che contiene una affiliazione esplicita o implicita di entità del sottoscrittore deve essere emesso solo in base alle clausole della sezione 3.2.2 in alto.

3.2.5 Informazioni sui sottoscrittori non verificati

Non esistono informazioni non verificate utilizzate dalla RA per compilare il certificato.

3.2.6 Criteri per l'interoperabilità

I certificati forniti dai componenti PKI vengono gestiti conformemente ai regolamenti e ai requisiti indicati dalla CA e dal cliente. Conformemente al OID, il certificato è conforme a:

– 1.3.6.1.4.1.22234.2.8.3.7: è conforme a ETSI 101 456 QCP Public (OID 0.4.0.1456.1.2).

– 1.3.6.1.4.1.22234.2.8.3.20: è conforme a ETSI 101 456 QCP Public + SSCD (OID 0.4.0.1456.1.1) e ETSI EN 319 411-2 QCwithQSCD.

– 1.3.6.1.4.1.22234.2.8.3.9: è conforme a ETIS 102 042 LCP (OID 0.4.0.2042.1.3) e ETSI EN 319 411-1 LCP.

3.3 Identificazione e autenticazione per le richieste di ricreare le chiavi

3.3.1 Identificazione e autenticazione per la ricreazione routinaria delle chiavi

3.3.1.1 Sub-CA

Vengono applicate alcune procedure descritte nella sezione 3.2 in alto.

3.3.1.2 Sottoscrittori

Per questa sezione, il sottoscrittore è già registrato dalla RA ed è stato emessi con successo un primo certificato.

Allora, la RA può definire un processo per la nuova emissione di altri certificati per il sottoscrittore. Ma in questo caso, possono rimanere valide come informazioni più importanti, le informazioni utilizzate inizialmente per registrare il sottoscrittore, dato che la RA potrebbe voler evitare di registrare nuovamente e completamente il sottoscrittore come nella sezione 3.2 in alto.

Questa sezione si occupa di un nuovo certificato con una nuova coppia di chiavi per il sottoscrittore (vedi sezione 4.7).

La RA è responsabile anche dell'aggiornamento, della raccolta e la conservazione delle informazioni richieste, per poter fornire una prova dell'identità dei sottoscrittori indicata nel certificato, durante l'operazione di rinnovo.

L'iscrizione per il rinnovo di un utente prima dell'emissione del certificato sottoscrittori viene eseguita direttamente dalla RA.

I regolamenti di verifica dell'identità dei sottoscrittori sono a discrezione della RA, che è competente per la gestione dei sottoscrittori per l'operazione di rinnovo.

La procedura per l'identificazione, autenticazione e validazione di una richiesta di emissione di un nuovo certificato viene descritta nella policy di gestione della prova e nel protocollo di approvazione utilizzati per ogni cliente che utilizza i certificati dei sottoscrittori, e viene completata da una procedura specifica per la linea commerciale della RA definita dal cliente.

Il metodo di assegnazione di questa identità per un certificato nuovo è quindi definita dal cliente, che iscrive tutti i suoi utenti con i loro dati di identificazione e i dati di autenticazione.

I regolamenti particolari devono essere applicati dal cliente conformemente alla sua scelta di OID.

La RA deve controllare l'esistenza e la validità del certificato (non revocato) da rinnovare e che le informazioni utilizzate per verificare l'identità e le caratteristiche del sottoscrittore siano ancora valide.

Se una parte dei termini e delle condizioni CA è stata modificata, essa deve essere comunicata al sottoscrittore e il sottoscrittore deve firmare i nuovi termini e condizioni (vedi sezione 4.1.2 in basso).

Se qualsiasi informazione del sottoscrittore da indicare nel certificato sottoscrittori (vedi sezione 3.1.1 in alto) è cambiata, la registrazione deve essere eseguita in base alle procedure definite nella sezione 3.2 in alto, almeno per ciò che riguarda le informazioni che sono state modificate.

Le informazioni utilizzate per autenticare i sottoscrittori durante il protocollo di approvazione (come l'indirizzo e-mail e il numero di telefono) possono essere modificate dal sottoscrittore solo dopo la verifica eseguita dalla RA, per essere sicuri che le informazioni aggiornate siano collegate al sottoscrittore per il protocollo di approvazione.

3.3.2 Identificazione e autenticazione per la ricreazione delle chiavi in seguito a revoca

3.3.2.1 RCA, ICA e CA

Vengono applicate alcune procedure descritte nella sezione 3.2 in alto.

3.3.2.2 Sottoscrittori

Vengono applicate alcune procedure descritte nella sezione 3.2 in alto.

La RA deve documentare i suoi regolamenti per la ricreazione delle chiavi per cause dipendenti dal tipo di revoca.

3.4 Identificazione e autenticazione per le richieste di revoca

3.4.1.1 Sub-CA

La richiesta di revoca Sub-CA deve essere autorizzata solo dai membri PMA.

3.4.1.2 Sottoscrittori

Per i sottoscrittori, l'autenticazione viene eseguita conformemente alle procedure RA approvate dalla DOCUSIGN FRANCE.

4 REQUISITI OPERATIVI PER IL CICLO DI VITA DEL CERTIFICATO

4.1 Domanda di certificato

Le sezioni 4.1, 4.2, 4.3 e 4.4 specificano i requisiti per una domanda iniziale per il rilascio del certificato.

Le sezioni 4.6, 4.7 e 4.8 specificano i requisiti per il rinnovo del certificato.

4.1.1 Chi può inoltrare una domanda di certificato

4.1.1.1 Sub-CA

Il rappresentante autorizzato della Sub-CA deve presentare la richiesta di certificato indirizzata alla PMA.

4.1.1.2 Sottoscrittori

La richiesta di certificato è sotto la responsabilità della RA.

4.1.2 Processo di iscrizione e responsabilità

4.1.2.1 Sub-CA

I certificati Sub-CA devono essere autorizzati dalla PMA prima del rilascio. Il processo di rilascio include la documentazione delle seguenti informazioni:

- Identità da indicare nel certificato (vedi sezione 3.1.1 in alto).

- Dati di identificazione dell'entità legale, in particolare il nome completo e lo stato della persona legale associata o dell'altra entità organizzativa e qualsiasi informazione di registrazione rilevante esistente (per es. la registrazione della società) della persona legale associata o dell'altra entità organizzativa.

- La CSR associata alla coppia di chiavi generata (vedi sezione 6.1.1). La CSR deve essere inclusa nella domanda.

- Informazioni del rappresentante autorizzato:

o Nome completo, incluso il cognome e il nome/i nomi del rappresentante.

o Nome completo e stato legale del datore di lavoro del rappresentante autorizzato.

o Indirizzo fisico operativo della sede o un altro metodo di contatto adatto relativo al rappresentante autorizzato.

4.1.2.2 Sottoscrittori

La richiesta di certificato deve contenere seguenti informazioni:

– Il sottoscrittore deve fornire un indirizzo fisico o un'altra caratteristica che descrive come il sottoscrittore può essere contattato.

– Il nome completo (incluso il cognome e i nomi, in conformità con la legge applicabile e le pratiche di identificazione nazionale)

– Se il sottoscrittore è una persona che è l'identificatore in associazione con una persona legale o un'altra entità organizzativa, deve essere presentata una dimostrazione di seguenti punti:

o Nome completo e lo stato legale della persona legale associata o dell'altra entità organizzativa.

o Qualsiasi informazioni di registrazione rilevante esistente (per es. la registrazione della società) della persona legale associata o dell'altra entità organizzativa.

o Dimostrazione che il oggetto è associato alla persona legale o all'entità organizzativa

– La RA deve raccogliere l'accordo firmato con il sottoscrittore, incluso:

o Accordo sugli obblighi del sottoscrittore come definito nella sezione 9 di presente CP.

o Consenso alla CA di tenere la documentazione delle informazioni utilizzate per la registrazione, il fatto che non c'è possibilità di revoca di questo certificato, l'identità di qualsiasi caratteristica specifica posizionata nel certificato, e il passaggio di queste informazioni a terzi alle stesse condizioni richieste da presente policy in caso la CA o la RA dovessero terminare i servizi.

o Il fatto che i certificati sottoscrittori non vengono pubblicati e sono solo contenuti nel documento firmato, e quindi vengono resi disponibili dal cliente, nel documento firmato.

o Conferma che le informazioni contenute nel certificato siano corrette.

– La data e il luogo di nascita, il numero di identità riconosciuto a livello nazionale, o gli altri attributi che possono essere utilizzati, in quanto possibile, per distinguere la persona dalle altre persone con lo stesso nome.

4.1.2.2.1 OID: 1.3.6.1.4.1.22234.2.8.3.7

In aggiunta, la richiesta di certificato deve contenere seguenti informazioni:

- Cognome e nome della RA.

- Localizzazione della RA.

4.1.2.2.2 OID: 1.3.6.1.4.1.22234.2.8.3.20

In aggiunta, la richiesta di certificato deve contenere seguenti informazioni:

- Cognome e nome della RA.

- Localizzazione della RA.

- Numero di cellulare del sottoscrittore.

4.2 Lavorazione della domanda di certificato

4.2.1 Esecuzione delle funzioni di identificazione e autenticazione

4.2.1.1 Sub-CA

Le richieste vengono presentate da un rappresentante autorizzato a discrezione della PMA prima del rilascio. La PMA è responsabile della autenticazione del rappresentante autorizzato come descritto nella

sezione 3.2 in alto, e di verificare che le informazioni presenti nella richiesta di certificato siano accurate, per quanto riguarda la CA.

4.2.1.2 Sottoscrittori

La RA è responsabile di verificare che le informazioni presenti nella richiesta di certificato siano accurate, per quanto riguarda la persona fisica (vedi sezioni 3.2.2 e 3.2.5 in alto).

La verifica dell'identità dei sottoscrittori avviene durante l'incontro faccia a faccia tra la RA e il sottoscrittore.

4.2.2 Approvazione o rigetto delle domande di certificato

4.2.2.1 Sub-CA

La PMA deve essere responsabile dell'approvazione o del rigetto della domanda di certificati Sud-CA.

4.2.2.2 Sottoscrittori

La RA deve essere responsabile dell'approvazione o del rigetto della domanda di certificati dei sottoscrittori.

4.3 Rilascio del certificato

4.3.1 Azioni CA durante il rilascio del certificato

4.3.1.1 Sub-CA

La PMA deve trasmettere la richiesta di certificato alla OA e alla Root CA. La OA deve autenticare la richiesta di certificato prima della generazione della coppia di chiavi Sub-CA e della CSR. La trasmissione della richiesta di certificato e della CSR deve essere eseguita in modo da assicurare l'integrità delle informazioni.

Le seguenti azioni devono verificarsi durante una cerimonia delle chiavi Sub-CA, testimoniate da un testimone PMA della DOCUSIGN FRANCE:

- Rilascio di chiavi Sub-CA
- Backup della chiave privata Sub-CA
- Generazione della CSR Sub-CA (la CSR deve includere la chiave pubblica della Sub-CA)

La cerimonia delle chiavi deve essere documentata e una copia deve essere fornita alla PMA della DOCUSIGN FRANCE.

Le seguenti azioni devono verificarsi durante una cerimonie delle chiavi ICA:

- Generazione di un certificato Sub-CA.
- Utilizzo di una ICA chiave privata per firmare il certificato Sub-CA.

4.3.1.2 Sottoscrittori

Il sottoscrittore utilizza i dati di attivazione conformemente al protocollo di approvazione scelto dal cliente (vedi sezione 6.4 in basso). Durante il protocollo di approvazione, il cliente deve dare a disposizione dei

sottoscrittori tutte le informazioni utilizzate per costruire l'identità del sottoscrittore nel DN (vedi sezione 3.1 in alto), per consentire la validazione.

La CA autentica il sottoscrittore utilizzando i dati di attivazione.

La CA genera il certificato sottoscrittori del sottoscrittore.

Il servizio Protect and Sign (Firma personale) firma il documento trasmesso dal cliente e include il certificato sottoscrittori nel documento.

Dopo la firma del documento, la coppia di chiavi del sottoscrittore viene distrutta.

Il servizio Protect and Sign (Firma personale) trasmette il documento alla RA.

4.3.1.2.1 OID: 1.3.6.1.4.1.22234.2.8.3.7 e 1.3.6.1.4.1.22234.2.8.3.20

Se il sottoscrittore accetta di firmare il documento, conferma la sua scelta di far utilizzare alla RA le procedure RA (clicca sullo schermo …) e i mezzi RA durante l'incontro faccia a faccia (vedi sezione 4.2 in alto).

4.3.1.2.2 OID: 1.3.6.1.4.1.22234.2.8.3.9

Se il sottoscrittore accetta di firmare il documento, conferma la sua scelta di far utilizzare alla RA le procedure RA (clicca sullo schermo …) e i mezzi informatici.

4.3.2 Notifica del rilascio del certificato al sottoscrittore da parte del CA

Non applicabile

4.4 Accettazione del certificato

4.4.1 Svolgimento dell'accettazione del certificato

4.4.1.1 Sub-CA

L'accettazione del certificato Sub-CA deve essere eseguito dalla PMA. La Sub-CA non deve emettere i certificati e neanche firmare le CRL, finché non è stato accettato il certificato Sub-CA.

4.4.1.2 Sottoscrittori

Se è presente un errore nel certificato sottoscrittori, la RA deve essere avvertita dalla persona (RA o sottoscrittore) che esegue la verifica.

4.4.1.2.1 OID: 1.3.6.1.4.1.22234.2.8.3.7 e 1.3.6.1.4.1.22234.2.8.3.20

L'accettazione del certificato viene realizzata dalla RA che verifica con il sottoscrittore il contenuto del documento firmato e la firma.

4.4.1.2.2 OID: 1.3.6.1.4.1.22234.2.8.3.9

L'accettazione del certificato viene realizzata dal sottoscrittore che verifica il contenuto del documento firmato e la firma.

4.4.2 Pubblicazione del certificato da parte del PS

Il certificato sottoscrittori è contenuto nel documento firmato, firmato durante il protocollo di approvazione. Quindi, il cliente deve rendere disponibile il documento firmato per rendere disponibile il certificato. La RA raccoglie il consenso del sottoscrittore relativo alla gestione del certificato sottoscrittori durante la raccolta dell'accordo firmato, come specificato nella sezione 4.1 in alto.

Per l'utilizzatore del certificato, il certificato sottoscrittori di un particolare sottoscrittore è contenuto anche esso nel documento associato firmato e quindi sarà disponibile per un utilizzatore del certificato se l'utilizzatore del certificato ha il documento firmato.

L'utilizzatore del certificato può testare il certificato utilizzando informazioni pubblicate dalla CA (vedi sezione 2.2 in alto).

4.4.3 Notifica del rilascio del certificato da parte del CA alle altre entità

Il cliente e la RA vengono informati del rilascio del certificato dalla CA, conformemente ai servizi Protect and Sign (Firma personale).

4.5 Coppia di chiavi e utilizzo del certificato

4.5.1 Chiave privata e utilizzo del certificato

I sottoscrittori e la Sub-CA devono usare le loro chiavi private per gli scopi indicati nella sezione 1.4 in alto.

L'utilizzo di una coppia di chiavi e il certificato associato devono anche essi essere eseguiti come indicato nel certificato stesso, tramite estensioni relative all'utilizzo della coppia di chiavi (vedi sezione 6.1.7 in basso).

4.5.2 Chiave pubblica dell'utilizzatore del certificato e utilizzo del certificato

Gli utilizzatori usano il percorso della certificazione sicura e le chiavi pubbliche associate per scopi vincolati dalle estensioni dei certificati (come l'utilizzo della chiave, l'utilizzo esteso della chiave, le policy dei certificati, ecc.) e per autenticare l'identità comune sicura dei certificati dei sottoscrittori.

Gli utilizzatori devono essere a conoscenza dei regolamenti di sicurezza da utilizzare nella transazione elettronica del cliente per l'utilizzo di un certificato sottoscrittori. un certificato sottoscrittori viene utilizzato per identificare, per esempio il sottoscrittore come una persona fisica che a volte appartiene a una entità esterna. L'utilizzatore del certificato deve controllare le informazioni aggiuntive (utilizzo della chiave, policy OID ...) per poter accettare e utilizzare il corretto certificato sottoscrittori nella transazione elettronica. L'utilizzatore del certificato deve utilizzare tutte le informazioni richieste nel certificato (DN come descritto nella sezione 3.1.1 in alto, estensioni ...) per poter essere sicuro di accettare il sottoscrittore corretto.

Un certificato sottoscrittori non può essere utilizzato senza un preventivo controllo da parte dell'utilizzatore del certificato, come per esempio il percorso sicuro, le informazioni aggiuntive conosciute solo dal sottoscrittore e dall'utilizzatore del certificato (per poter registrare il certificato del sottoscrittore) e le informazioni del cliente relative alla iscrizione del sottoscrittore e l'uso del documento firmato verificabile utilizzando il certificato sottoscrittori.

4.6 Rinnovo del certificato

Conformemente alla RFC 3647, il rinnovo del certificato è un processo in cui vengono modificati solo il periodo di validità del certificato e il numero di serie del certificato (né la chiave pubblica né qualsiasi altra informazione nel certificato vengono modificate).

Questa pratica non è ammessa per i certificati Sub-CA e i certificati dei sottoscrittori. Se viene creato un certificato nuovo, viene creata una coppia di chiavi nuova.

4.7 Ricreazione delle chiavi del certificato

La ricreazione delle chiavi deve essere eseguita quando una coppia di chiavi raggiunge la fine della sua durata (vedi sezione 6.3.2 in basso), la fine del suo utilizzo operativo o quando la chiave pubblica è compromessa. Una nuova coppia di chiavi deve essere garantita in ogni caso.

4.7.1 Sub-CA

Le stesse procedure di quelle applicate per la generazione iniziale devono essere applicate per un nuovo certificato Sub-CA e la generazione della coppia di chiavi associata (vedi sezioni 4.1.1, 4.1.2, 4.2.1, 4.2.2, 4.2.3**Errore ! Fonte del rinvio**

introvabile., 4.3.1, 4.4.1 e 4.4.2 in alto).

4.7.2 Sottoscrittori

vedi sezione 4.1.1, 4.1.2, 4.2.1, 4.2.2, 4.2.3**Errore ! Fonte del rinvio introvabile.**, 4.3.1, 4.4.1 e 4.4.2 in alto, ma per l'autenticazione deve essere applicata la sezione 3.3.

4.8 Modifica del certificato

Conformemente alla RFC 3647, la modifica del certificato è il processo di generazione di certificati nuovi utilizzando la stessa coppia di chiavi.

Questa pratica non è ammessa per i certificati Sub-CA e i certificati dei sottoscrittori. Se viene creato un certificato nuovo, viene creata una coppia di chiavi nuova.

4.9 Revoca e sospensione del certificato

4.9.1 Circostanze per una revoca

Un certificato deve essere revocato se il legame tra il certificato e la chiave pubblica che contiene non viene più considerato valido. Esempi di circostanze che rendono non valido il legame:

- La RCA o ICA emettente la CA nella catena viene revocata o cessa l'attività.

- Il sottoscrittore non osserva gli obblighi necessari e i regolamenti di sicurezza nella CP o CPS.

- Il sottoscrittore cessa di operare, o non è più associato in altro modo all'organizzazione emittente.

- Quando si sospetta che la chiave privata sia compromessa o è compromessa o si sospetti sia stata compromessa.

- Modifica della policy come indicato dalla PMA, inclusi i requisiti di lunghezza delle chiavi, l'algoritmo, la data di validità o altre caratteristiche del certificato.

- Altre ragioni come indicato dalla PMA.

4.9.1.1 Sub-CA

La revoca del certificato Sub-CA può essere gestita solamente dalla PMA. In aggiunta a quanto sopra, un certificato Sub-CA può essere revocato quando:

- La PMA decide che la Sub-CA deve cessare di operare.

- Se la Sub-CA perde la sua licenza di emissione di certificati.

- La Sub-CA viola presente CP o la propria CP interna, a discrezione della PMA.

- L'entità proprietaria della Sub-CA cessa di operare o finisce i suoi servizi Sub-CA verso la DOCUSIGN FRANCE.

4.9.1.2 Sottoscrittori

Un certificato viene revocato se il legame tra il certificato e la chiave pubblica che contiene viene considerato non più valido. Le circostanze in cui una persona fisica rende invalido il legame sono:

- La CA è revocata.

- Le informazioni DN sono compilate in modo errato.

- La persona fisica o la RA non osserva gli obblighi necessari e i regolamenti di sicurezza nella CP e CPS.

- Il certificato corrispondente alla chiave privata è andato perso o è compromesso o sospettato di essere compromesso.

- Qualsiasi altra ragione indicata dalla PMA.

4.9.2 Chi può richiedere una revoca

4.9.2.1 Sub-CA

Solo la PMA ha l'autorità di richiedere la revoca di un certificato Sub-CA.

4.9.2.2 Sottoscrittori

La persona fisica può presentare una richiesta di revoca nei seguenti casi:

- Le informazioni DN sono compilate in modo errato.

- Il certificato corrispondente alla chiave privata è andato perso o è compromesso o sospettato di essere compromesso.

La RA può presentare una richiesta di revoca nei seguenti casi:

- Le informazioni DN sono compilate in modo errato.

- Il certificato corrispondente alla chiave privata è andato perso o è compromesso o sospettato di essere compromesso.

La PMA può presentare una richiesta di revoca nei seguenti casi:

- La CA è revocata.

- La persona fisica o la RA non osserva gli obblighi necessari e i regolamenti di sicurezza nella CP e CPS.

- Il certificato corrispondente alla chiave privata è andato perso o è compromesso o sospettato di essere compromesso.

- Qualsiasi altra ragione indicata dalla PMA

4.9.3 Procedimento di richiesta della revoca

4.9.3.1 Sub-CA

La revoca di un certificato Sub-CA deve richiedere l'autorizzazione della PMA. La PMA deve dirigere la revoca rilasciando un documento firmato che istruisce la revoca alla ICA.

La revoca da parte della ICA deve essere eseguita conformemente alle procedure scritte del fornitore di servizi ICA.

4.9.3.2 Sottoscrittori

Le richieste di revoca vengono autenticate dalla RA.

La richiesta di revoca viene conservata nei log della RA.

La RA autentica la richiesta di revoca che riceve (vedi sezione 3.4 in alto).

La RA trasmette la richiesta di revoca alla CA.

La CA autentica la RA e assicura che la richiesta sia stata emessa da una RA autorizzata dalla Sub-CA.

La Sub-CA revoca il certificato includendo il numero di serie del certificato nella successiva CRL che la Sub-CA emetterà, se il certificato non è scaduto.

Il codice della causa indicato nella CRL è sempre "non specificato".

La RA deve informare il sottoscrittore del nuovo stato del certificato.

4.9.4 Periodo di tolleranza della richiesta di revoca

4.9.4.1 Sub-CA

La ICA deve lavorare la revoca dei certificati Sub-CA appena ricevuta la disposizione dalla PMA. Questa revoca deve essere lavorata il più presto possibile, entro e non oltre i 10 giorni lavorativi.

4.9.4.2 Sottoscrittori

Non sussiste un periodo di tolleranza per la revoca. La parte responsabile deve richiedere la revoca appena ha identificato le circostanze che richiedono una revoca.

4.9.5 Lasso di tempo entro il quale il CA deve elaborare la richiesta di revoca

4.9.5.1 Sub-CA

La ICA deve lavorare una richiesta di revoca il più presto possibile dopo aver ricevuto la richiesta di revoca, entro e non oltre i 10 giorni lavorativi.

4.9.5.2 Sottoscrittori

La Sub-CA deve lavorare una richiesta di revoca appena è stata ricevuta, autenticata e approvata la richiesta di revoca. Il ritardo massimo per revocare un certificato sono 24 ore.

4.9.6 Necessità di controllo della revoca per gli utilizzatori

L'utilizzo di certificati revocati può avere delle conseguenze dannose o catastrofiche in certe applicazioni. La questione di quanto spesso devono essere ottenuti i dati di revoca è una decisione che deve essere presa dall'utilizzatore del certificato. Se è temporaneamente impossibile ottenere le informazioni relative alla revoca, l'utilizzatore del certificato deve rigettare l'uso del certificato o prendere la decisione consapevole di accettare il rischio, la responsabilità e le conseguenze dell'utilizzo di un certificato di cui non è garantita l'autenticità dagli standard di presente policy. Un tale uso può essere occasionalmente necessario per venire incontro a fabbisogno operativo urgente.

4.9.7 Frequenza di rilascio CRL

La CA emette una CRL ogni 24 ore ma la CRL.

4.9.8 Latenza massima della CRL

La CA emette una CRL ogni 24 ore ma la CRL è valida solo per 7 giorni.

4.9.9 Disponibilità revoca online / controllo stato

Se la CA non include la CRL nel documento firmato, le Sub-CA devono supportare il controllo dello stato online (servizio OCSP) per poter includere una risposta OCSP nel documento firmato.

4.9.10 Requisiti per il controllo della revoca online

La risposta del sistema OCSP sullo stato di validità della Sub-CA si basa sulle informazioni Sub-CA.

Il OCSP deve avere seguenti formati:

Campo	Requisiti
versione	1
Responder ID	Hash della chiave pubblica del OCSP
ProducedAT	Data e ora della firma di risposta del OCSP
CertID	Numero di serie del certificato del sottoscrittore, hash chiave emittente Sub-CA e hash nome emittente Sub-CA
This Update	Data e ora della verifica dello stato del certificato del sottoscrittore fatto nella CRL.
Next Update	Data della prossima CRL.
CertStatus	"Buono", "Revocato" o "sconosciuto"
nonce	Utilizzato se e solamente se l'applicazione dell'utente fornisce un valore per questo campo ed è riutilizzato in pieno.

extensions	Non ci sono estensioni referenziate

4.9.11 Altre forme di annunci di revoca disponibili

Non applicabile.

4.9.12 Requisiti specifici in caso di compromissione della chiave privata

Le entità che sono autorizzate a presentare una segnalazione devono farlo il più presto possibile dopo essere state informate della compromissione della chiave privata.

Per i certificati Sub-CA, la notifica della compromissione delle chiavi private deve essere eseguita conformemente alle policy del fornitore di servizi ICA.

4.9.13 Sospensione dei token

Non applicabile.

4.9.13.1 Circostanze per la sospensione

Non applicabile.

4.9.13.2 Chi può richiedere la sospensione

Non applicabile.

4.9.13.3 Procedura di richiesta della sospensione

Non applicabile.

4.9.13.4 Limiti del periodo di sospensione

Non applicabile.

4.9.13.5 Ripresa della richiesta di certificato

Non applicabile.

4.10 Servizi relativi allo stato del certificato

4.10.1 Caratteristiche operative

Il servizio OCSP utilizza le informazioni Sub-CA.

4.10.2 Disponibilità del servizio

Il servizio dello stato del certificato è disponibile conformemente al fabbisogno del servizio Protect and Sign (Firma personale).

4.11 Fine della sottoscrizione

Il contratto tra il cliente e la DOCUSIGN FRANCE disciplina la fine del rapporto.

4.12 Deposito e recupero della chiave

4.12.1 Sottoscrittori

4.12.1.1 Quale coppia di chiavi può essere depositata

Non applicabile.

4.12.1.2 Chi può presentare una domanda di recupero

Non applicabile.

4.12.1.3 Processo di recupero e responsabilità

Non applicabile.

4.12.1.4 Identificazione dell'esecuzione e autenticazione

Non applicabile.

4.12.1.5 Approvazione o rigetto delle domande di recupero

Non applicabile.

4.12.1.6 Azioni KEA e KRA durante il recupero della coppia di chiavi

Non applicabile.

4.12.1.7 Disponibilità KEA e KRA

Non applicabile.

4.12.2 Incapsulamento della chiave di sessione e policy di recupero e pratica

Non applicabile.

5 DISPOSITIVO, GESTIONE E CONTROLLI OPERATIVI

5.1 Controlli fisici

5.1.1 Ubicazione e costruzione del sito

L'ubicazione e la costruzione del dispositivo della OA che ospita la CA, RA e PS e l'equipaggiamento SSCD dei sottoscrittori remoti, deve comprendere i dispositivi utilizzati per ospitare delle informazioni di alto valore e sensibili. L'ubicazione e costruzione del sito, quando combinati con altri meccanismi di sicurezza fisica, come le guardie e i sensori anti-intrusione, devono fornire una protezione robusta contro l'accesso non autorizzato all'equipaggiamento e alla documentazione.

5.1.2 Accesso fisico

L'equipaggiamento CA e RA e il SSCD PSM dei sottoscrittori devono essere sempre protetti da un accesso non autorizzato e dal danneggiamento. Il meccanismo di sicurezza fisica minima dell'equipaggiamento deve comprendere in loco:

– Assicurare il monitoraggio, manuale o elettronico, delle intrusioni non autorizzare, in qualsiasi momento.

– Assicurare che non venga permesso un accesso non autorizzato al hardware e ai dati di attivazione.

– Assicurare che tutti i mezzi mobili e il cartaceo che contiene informazioni sensibili in testo chiaro siano conservati in un luogo sicuro.

– Qualsiasi individuo non autorizzato che entra nelle aree sicure deve essere sempre supervisionato da un impiegato autorizzato.

– Assicurare che il log di accesso sia mantenuto e ispezionato periodicamente.

– Fornire almeno tre sistemi di sicurezza crescente come il perimetro, l'edificio o la sala operativa.

– Richiedere i controlli di accesso fisico a due persone, sia per il HSM crittografato sia per i dati di attivazione per la CA e il SSCD.

Se il dispositivo viene lasciato senza sorveglianza, deve essere eseguito un controllo di sicurezza dell'equipaggiamento che ospita il dispositivo. Il controllo deve verificare almeno seguenti punti:

– L'equipaggiamento si trova in uno stato appropriato per la modalità operativa attuale.

– Per i componenti offline, tutto l'equipaggiamento è spento.

– Tutti i contenitori di sicurezza (buste a prova di manomissione, casseforti ...) sono tenute al sicuro in modo adeguato.

– I sistemi di sicurezza fisica (per es. serrature, coperture ventilazione, elettricità ...) ip1nea i sicurez3-10ms4

I moduli crittografici mobili devono essere disattivati prima di essere archiviati. Quando non vengono utilizzati, i moduli crittografici mobili e i dati di attivazione utilizzati per accedere o abilitare i moduli crittografici, devono essere posizionati in contenitori sicuri. I dati di attivazione devono essere memorizzati o documentati e conservati in modo da essere proporzionati alla sicurezza necessaria per il modulo crittografico, e non devono essere conservati insieme al modulo crittografico.

5.1.3 Energia e aria condizionata

L'OA assicura che l'energia e i dispositivi di aria condizionata siano sufficienti per supportare l'operatività del sistema PKI, utilizzando delle installazioni primarie e di backup.

5.1.4 Esposizione all'acqua

L'OA assicura che i sistemi siamo protetti in modo da minimizzare l'impatto di un'esposizione all'acqua.

5.1.5 Prevenzione incendi e protezione antincendio

L'OA assicura che i sistemi sono protetti con rilevatori di fumo e impianti antincendio.

5.1.6 Media Storage

I mezzi utilizzati nell'OA vengono trattati in modo sicuro per proteggere i supporti da danni, furti e accessi non autorizzati. Le procedure di gestione dei supporti vengono applicate per proteggere contro l'obsolescenza e il deterioramento dei supporti nell'arco del tempo in cui la documentazione deve essere conservata.

I dati sensibili devono essere protetti, in modo da non essere accessibili a utenti non autorizzati, tramite oggetti di memoria ri-utilizzati (per es. file cancellati).

La CA deve conservare un indice di tutte le risorse informative e deve assegnare una classificazione dei requisiti di protezione a quelle risorse compatibili con l'analisi del rischio.

5.1.7 Smaltimento rifiuti

Tutti i supporti utilizzati per l'archiviazione di informazioni sensibili, come le chiavi, i dati di attivazione o i file, devono essere distrutti, prima che vengano rilasciati a disposizione.

5.1.8 Backup offsite

Backup completi dei sistemi CA online, sufficiente per abilitare il recupero dopo un guasto del sistema, deve essere fatto dopo l'utilizzo della PKI conformemente alle policy della DOCUSIGN FRANCE. Le copie di backup delle informazioni commerciali e del software essenziali, vengono fatte regolarmente. I dispositivi adeguati di backup vengono forniti per assicurare che tutte le informazioni commerciali e i software essenziali possono essere recuperati in seguito a un disastro o a un guasto del supporto. La disposizione del backup per i sistemi individuali deve essere testata regolarmente per assicurare che soddisfino i requisiti del piano di continuità commerciale dell'OA (per CA). Almeno una copia completa di backup deve essere conservata in un sito offsite (ripristino in caso di disastro OA). La copia di backup deve essere conservata in un luogo con controlli fisici e procedurali commisurati a quelli del sistema operativo CA.

5.2 Controlli procedurali

5.2.1 Ruoli di fiducia

La CA deve assicurare che i ruoli vengano definiti per poter utilizzare i seguenti pacchetti di funzioni sicure, in supporto ai servizi della PKI (utilizzato dalla DocuSign France solo) con una separazione adeguata dei doveri:

- Operazione di sicurezza: Possiede la responsabilità complessiva per gestire l'esecuzione delle pratiche delle policy e della CP, e definisce tutti i ruoli PKI e incarica la persona fisica con il ruolo di fiducia.

- Operazione sistemica PKI: Disponibile per installare, configurare, fare il backup, recuperare e mantenere i sistemi PKI (offline e online).

- operazione di gestione della chiave: Gestisce tutti i HSM della PKI (online) sul SSCD sottoscrittori ed esegue le cerimonie delle chiavi (offline e online).

- operazione di verifica: Autorizzata a visionare gli archivi e i log di verifica prodotti durante l'utilizzo e la gestione dei sistemi PKI (online).

- Attivazione HSM: Disponibile per tenere i dati di attivazione necessari per l'operazione relativa al modulo di sicurezza del hardware (offline e online).

- Protezione della coppia di chiavi: Disponibile per tenere i dati di attivazione che sono necessari per la chiave privata Sub-CA e la gestione della chiave sottoscrittori (ruolo differente dal ruolo di attivazione del HSM).

- Software PKI online e amministrazione del software SSCD PSM: gestione dei ruoli tecnici della PKI e del software SSCD PSM, software e configurazione del software PKI e PSM.

- Software PKI online e operazione software SSCD PSM: usa la funzionalità del software PKI e SSCD PSM per poter gestire il ciclo di vita del certificato del sottoscrittore.

Tutto il personale è incaricato formalmente con ruoli di fiducia dalla PMA e/o dall'OA (per CA), come descritto nella CPS. Per OID 1.3.6.1.4.1.22234.2.8.3.20, il ruolo dedicato al software PSM deve essere eseguito conformemente a [PSM SSCD].

Il cliente è responsabile di definire e documentare i ruoli di fiducia e le operazioni associate. Il cliente deve definire il personale di fiducia che deve gestire la RA e il personale RA deve essere incaricato formalmente da un senior manager.

5.2.2 Numero di persone necessarie per ogni compito

Il numero di persone che fornisce i servizi della PKI viene descritto dettagliatamente nella CPS per la CA e nel documento del cliente per la RA. Il numero di persone viene definito per garantire la sicurezza di tutti i servizi (generazione della chiave, generazione del certificato, revoca, richiesta di certificato …), in modo che non possa verificarsi alcuna attività dolosa da una persona singola che agisce per contro della PKI. Tutti i partecipanti devono lavorare in un ruolo di fiducia, come definito nella sezione 5.2.1 in alto.

Le chiavi Sub-CA hanno almeno un controllo doppio.

I seguenti compiti devono essere completati da due persone autorizzate alle operazioni del sistema PKI:

- generazione chiave

- attivazione chiave

- backup chiave

- revoca certificato CA.

È vietato possedere privilegi (ruoli) per le seguenti operazioni allo stesso tempo:

- Un individuo che possiede un ruolo nell'operazione di sistema della PKI e del SSCD PSM non deve essere coinvolto in alcuna altra operazione.

- Un individuo che possiede un ruolo nell'operazione di sicurezza non deve essere coinvolto in alcuna altra operazione, eccezion fatta per l'attivazione del HSM Sub-CA e SSCD HSM, e la protezione della coppia di chiavi Sub-CA.

- Un individuo che possiede un ruolo nell'operazione di gestione della chiave non deve essere coinvolto in alcuna altra operazione, eccezion fatta per l'attivazione del HSM Sub-CA e SSCD HSM, e l'operazione della coppia di chiavi Sub-CA.

- Un individuo che possiede un ruolo nell'operazione di verifica, non deve essere coinvolto in alcuna altra operazione eccezion fatta per le operazioni di sicurezza.

- Un individuo che possiede un ruolo nell'amministrazione del software PKI e SSCD Sub-CA online, non deve essere coinvolto in operazioni software SSCD PSM e PKI Sub-CA online.

- Un individuo che possiede un ruolo nell'attivazione HSM SSCD e Sub-CA può essere coinvolto nella protezione della coppia di chiavi, se o solo se non può controllare la coppia di chiavi Sub-CA da solo/sola.

Per OID 1.3.6.1.4.1.22234.2.8.3.20, il ruolo dedicato al software PSM deve essere eseguito conformemente a [PSM SSCD].

Il cliente deve assegnare e definire il ruolo per poter eseguire almeno una separazione tra il personale responsabile dei servizi RA e il personale responsabile del software RA, per poter procedere con le seguenti operazioni: configurazione, installazione, backup, manutenzione e recupero.

5.2.3 Identificazione e autenticazione per ogni ruolo

Tutti i controlli necessari devono essere completati prima che un individuo acceda a un ruolo di fiducia all'interno dei componenti PKI.

Per OID 1.3.6.1.4.1.22234.2.8.3.20, il ruolo dedicato al software PSM deve essere eseguito conformemente a [PSM SSCD].

Tutte le persone a cui è stato assegnato un ruolo che descritto nella presente CP, sono identificate e autenticate in modo da garantire che il ruolo citato li abiliti a eseguire i loro obblighi PKI. La CPS descrive il meccanismo usato per identificare e autenticare gli individui.

5.2.4 Ruoli che richiedono la separazione dei doveri

La separazione dei doveri può essere attuata utilizzando l'equipaggiamento e le procedure PKI o entrambi. Gli impiegati della componente PKI vengono incaricati individualmente di ruoli di fiducia per operazioni definite nella sezione 5.2.1 in alto.

Per OID 1.3.6.1.4.1.22234.2.8.3.20, il ruolo dedicato al software PSM deve essere eseguito conformemente a [PSM SSCD].

A nessun individuo deve essere assegnata con più di una identità, a meno che non sia stato approvato dalla PMA.

La parte della CA relativa alla generazione del certificato e alla gestione della revoca, deve essere indipendente dalle altre organizzazioni nelle sue decisioni riguardo alla istituzione, alla fornitura e alla conservazione o alla sospensione dei servizi in conformità con le policy dei certificati applicabili; in particolare il suo senior executive, senior staff e staff con ruoli di fiducia, deve essere libero da pressioni commerciali, finanziarie e da altre pressioni che potrebbero influenzare in modo sfavorevole la fiducia nei servizi che fornisce.

5.3 Controlli del personale

5.3.1 Qualifiche, esperienza e requisiti sdoganamento

I componenti PMA e OA impiegano un numero sufficiente di personale che possiede una conoscenza esperta, l'esperienza e le qualifiche appropriate necessarie per le funzioni dell'incarico e dei servizi offerti. Il personale PKI soddisfa i requisiti di "conoscenza esperta, esperienza e qualifiche" grazie a una formazione formale e a credenziali, una esperienza sul campo o a una combinazione dei due. I ruoli di fiducia e le responsabilità, come specificato nella CPS, vengono documentati nella descrizione degli incarichi e identificati chiaramente. I subappaltatori del personale PKI hanno una descrizione degli incarichi definita per assicurare la separazione dei compiti e un privilegio minimo, e la sensibilità della posizione viene appurata in base ai compiti e ai livelli di accesso, dalla selezione del background e dalla formazione e dalla consapevolezza dell'impiegato. Il personale PKI deve essere incaricato dei ruoli di fiducia dalla PMA.

5.3.2 Procedure di controllo del background

Gli impiegati PMA e OA con ruoli di fiducia devono essere esenti da conflitti di interessi che potrebbero pregiudicare l'imparzialità delle operazioni PKI. Il cliente e l'OA non devono essere incaricati con ruoli di fiducia o gestire qualsiasi altra persona di cui si sa che abbia subito una condanna per reati gravi o altri reati che possano pregiudicare la sua adeguatezza alla posizione.

5.3.3 Requisiti formazione

La PMA e l'OA assicurano che tutto il personale che esegue dei compiti relativi a operazioni, riceva una formazione in:

- principi e meccanismi di sicurezza PKI

- versioni software in uso nel sistema PKI

- processi e flussi di lavoro aziendali PKI

- doveri che devono eseguire

- operazioni e procedure di controversie

- sufficiente conoscenza informatica.

- ripristino in caso di disastro e procedure di continuità aziendale

5.3.4 Frequenza e requisiti riqualificazione

Gli individui con ruoli di fiducia devono essere consapevoli delle modifiche nelle operazioni PKI, se applicabile. Qualsiasi modifica significativa alle operazioni deve essere accompagnata da un piano di formazione (consapevolezza) e l'esecuzione di detto piano deve essere documentata.

5.3.5 Frequenza e sequenza rotazione lavoro

La PMA e l'entità OA assicurano che qualsiasi cambiamento nello staff non pregiudicherà la sicurezza del sistema.

5.3.6 Sanzioni per azioni non autorizzate

Verranno applicate delle appropriate sanzioni disciplinari amministrative a qualsiasi personale della componente PKI che viola la CP della DOCUSIGN FRANCE.

5.3.7 Requisiti collaboratore esterno

Gli appaltatori impiegati per eseguire le funzioni della componente PKI sono soggetti a tutti i controlli del personale definiti nella sezione 5.3. Gli appaltatori possono eseguire le operazioni del sistema PKI (vedi sezione 5.2 in alto) con l'approvazione della PMA o del cliente conformemente alla componente PKI.

5.3.8 Documentazione fornita al personale

I componenti PKI rendono disponibile al loro personale la presente CP e la corrispondente CPS, e qualsiasi statuto e policy rilevanti. Gli altri documenti tecnici, operativi e amministrativi (per es. il manuale dell'amministratore, il manuale utente, ecc.) vengono forniti per abilitare il personale di fiducia all'esecuzione dei loro compiti.

5.4 Procedure audit logging

5.4.1 Tipi di eventi registrati

I file del log di verifica vengono generati dalla OA e dalla PMA per tutti gli eventi relativi alla sicurezza e ai servizi della PKI.

I file di verifica del log vengono generati per tutti gli eventi relativi alla sicurezza e ai servizi della PKI. Dove possibile, i log di verifica di sicurezza devono essere raccolti automaticamente. Lì dove ciò non fosse possibile, è necessario utilizzare un logbook, una forma cartacea o un altro meccanismo fisico. Tutti i log di verifica di sicurezza, sia quelli elettronici che non elettronici, devono essere conservati e resi disponibili durante le verifiche dell'osservanza. Ogni evento relativo a un ciclo di vita del certificato ciclo di vita viene registrato in modo da poter essere attribuito alla persona che lo esegue.

Il logging include seguenti argomenti:

- Accesso fisico al dispositivo.

- Gestione dei ruoli di fiducia.

- Accesso logico.

- Gestione del backup.

- Gestione del log.

- Dati del processo di autenticazione per i sottoscrittori e i componenti PKI.

- Data, ora, numero di telefono utilizzato, persone con cui si ha parlato e risultati finali delle telefonate di verifica.

- Accettazione e rigetto della richiesta di certificati.

- Creazione del certificato.

- Rinnovo del certificato.

- Gestione del HSM (per CA e per RA se RA utilizza il HSM e il SSCD).

- Creazione, uso e distruzione della chiave.

- Gestione dei dati di attivazione.

- Gestione dei ruoli.

- Gestione IT e network, nella misura in cui sono di pertinenza dei sistemi PKI.

- Gestione della documentazione PKI.

- Gestione della sicurezza (tentativi di accesso al sistema PKI che hanno avuto successo e che non hanno avuto successo, azioni del sistema di sicurezza e della PKI eseguite, modifiche del profilo di sicurezza, crash del sistema, guasti del hardware e altre anomalie, attività del firewall e del router; ed entrate e uscite dal dispositivo OA).

Ogni documentazione di verifica include minimo seguenti punti (documentati automaticamente o manualmente per ogni evento verificabile):

- Tipo di evento.

- Data e ora sicura in cui l'evento si è verificato.

- Risultato dell'evento: successo o fallimento, dove appropriato.

- Identità dell'entità e/o dell'operatore che ha causato l'evento.

- Identità alla quale è indirizzato l'evento.

- Causa dell'evento.

In aggiunta a ciò, la RA deve documentare tutte le informazioni utilizzate:

– Per verificare l'identità del soggetto.

– Se applicabile, qualsiasi caratteristica specifica del soggetto, incluso qualsiasi numero di riferimento presente sulla documentazione utilizzata per la verifica e qualsiasi limitazione della sua validità (vedi sezione 3.2 in alto).

– Per creare la richiesta di certificato (cioè tutte le informazioni descritte nella sezione 4.1.2.2 in alto.

– La lista di tutti gli operatori RA che sono autorizzati a iscrivere e gestire i sottoscrittori.

– Il protocollo di approvazione tecnico.

– Conformemente alla scelta operata dal cliente, la documentazione con il file prova (come definito nel [PSMP]), come prova della richiesta di certificato. Se no, la DocuSign France documenta il file prova in un sistema di archiviazione conformemente al [PSMP], anche come prova della richiesta di certificato dalla RA.

5.4.2 Frequenza lavorazione log

I log di verifica dell'operazione PKI vengono revisionati annualmente dal membro della OA responsabile della verifica, che conduce una ricerca ragionevole di qualsiasi prova di un'attività sospetta e successiva a qualsiasi operazione importante.

Un campione significante dal punto di vista statistico dei dati di verifica di sicurezza generati dalla sua entità aziendale PKI a partire dall'ultima revisione deve essere esaminato (lì dove gli intervalli di confidenza per ogni categoria di dati di verifica della sicurezza sono determinati dalla ramificazione della sicurezza della categoria e dalla disponibilità di strumenti per eseguire tale revisione), così come una ricerca ragionevole di qualsiasi prova di un'attività sospetta. Log di revisione OA a base giornaliera per la sicurezza informatica e fisica.

L'OA deve spiegare tutti gli eventi significativi in report di verifica dei log. Tale revisione comprende la verifica che il log non sia stato alterato, non ci sia discontinuità o un'altra perdita di dati di verifica e poi una ispezione veloce di tutte le entrate di log, con un'investigazione più approfondita di qualsiasi segnalazione o irregolarità presente nei log. Le azioni intraprese come risultato di questa revisione devono essere documentate.

5.4.3 Periodo di mantenimento dei log di verifica

La documentazione relativa all'operazione PKI viene tenuta presso la OA per almeno un anno, prima di essere archiviata.

5.4.4 Protezione dei log di verifica

I log degli eventi sono protetti in modo che solo gli utenti autorizzati possano accedervi.

Gli eventi vengono registrati in modo che non possano essere cancellati o distrutti facilmente (eccezion fatta per il trasferimento dei supporti di lunga durata) entro il periodo di tempo in cui devono essere conservati.

I log degli eventi sono protetti in modo da rimanere leggibili per tutta la durata del periodo della loro archiviazione.

5.4.5 Procedura di backup dei log di verifica

I log di verifica e i riepiloghi delle verifiche vengono garantiti tramite il meccanismo di backup dell'impresa, sotto il controllo dei ruoli di fiducia autorizzati, separati dalla generazione della fonte della loro componente. I backup dei log di verifica sono protetti con lo stesso livello di sicurezza definito per i log originali.

5.4.6 Sistema di raccolta verifica (interno verso esterno)

I processi di verifica devono essere richiamati al momento dello start up del sistema e devono finire solo allo shutdown del sistema. Il sistema di raccolta delle verifiche deve mantenere l'integrità e la disponibilità di tutti i dati raccolti. Se necessario, il sistema di raccolta delle verifiche protegge l'integrità dei dati. Se si verifica un problema durante il processo del sistema di raccolta delle verifiche, la PMA appura se deve sospendere o meno le operazioni finché il problema è stato risolto, e informa la componente interessata.

5.4.7 Notifica del soggetto che causa l'evento

Quando un evento è registrato dal sistema di raccolta delle verifiche, garantisce che l'evento è collegato a un ruolo di fiducia.

5.4.8 Valutazione della vulnerabilità

Il ruolo responsabile di condurre la verifica e i ruoli responsabile di realizzare l'operazione di sistema PKI spiegano tutti gli eventi significativi in un riepilogo dei log di verifica. Tale revisione comprende la verifica che il log non sia stato alterato, non ci sia discontinuità o un'altra perdita di dati di verifica e poi una ispezione veloce di tutte le entrate di log, con un'investigazione più approfondita di qualsiasi segnalazione o irregolarità presente nei log. Le azioni intraprese come risultato di questa revisione sono documentate.

Per la vulnerabilità vengono applicati seguenti regolamenti:

– Attuazione dei rilevamenti e dei controlli di prevenzione sotto il controllo della OA per proteggere i sistemi PKI dai virus e dai software sospetti.

– Documentazione e monitoraggio di un processo di correzione di una vulnerabilità che è indirizzata all'identificazione, alla revisione, alla risposta e al risanamento delle vulnerabilità.

– Avviamento ed esecuzione di una scansione della vulnerabilità (i) dopo qualsiasi modifica del sistema o del network che la PMA reputa essere significativa per la CA e il cliente per la RA, e (ii) almeno una volta ogni trimestre, degli indirizzi IP pubblici e privati identificati dalla OA come sistemi PKI (per CA).

– Avviamento di un test di penetrazione sui sistemi PKI almeno una volta l'anno e dopo gli aggiornamenti o le modifiche all'infrastruttura o all'applicazione, che la PMA reputa essere significativi per la CA e il cliente per la RA.

– Documentazione della prova che ogni scansione della vulnerabilità e test di penetrazione è stato eseguito da una persona o una entità (o gruppo collettivo di questi) con le capacità, gli strumenti, la competenza, la deontologia e l'indipendenza necessaria per fornire una vulnerabilità o un test di penetrazione affidabili; e

– Monitoraggio e rimedio della vulnerabilità conformemente alle policy di cibersicurezza dell'impresa e metodologia di mitigazione del rischio.

5.5 Archiviazione documentazione

5.5.1 Tipi di documentazioni archiviate

La documentazione archiviata della componente PKI deve essere abbastanza dettagliata da stabilire la validità di una firma e di un'attività corretta della PKI. Devono essere archiviate almeno i seguenti dati:

- documentazioni di eventi PKI:
    - Log di accesso fisico al dispositivo dell'OA (minimo un anno).
    - Log di accesso video al dispositivo dell'OA (un mese).
    - Video delle cerimonie delle chiavi, solo per CA (minimo 10 anni).
    - Log di gestione dei ruoli di fiducia per OA (minimo 10 anni).
    - Log di accesso IT per OA (minimo 5 anni).
    - Log di creazione, utilizzo e distruzione della chiave sottoscrittori e CA (minimo 5 anni) tenuti dalla DocuSign France.
    - Log di gestione dei dati di attivazione per OA (minimo 5 anni).
    - Log IT e network per OA (minimo 5 anni).
    - Documentazione PKI per OA (minimo 5 anni).
    - Report sugli incidenti di sicurezza e di verifica per OA (minimo 10 anni).
- Documentazione di verifica PKI (minimo 5 anni) tenuta da PMA.
- Documento CP (minimo 5 anni) tenuto da PMA.
- Documenti CPS (minimo 5 anni) tenuti da PMA.
- Contratto tra DOCUSIGN FRANCE e RA operante (minimo 5 anni) tenuto da PMA.
- Equipaggiamento del sistema, software e configurazione (minimo 5 anni) per DocuSign France.
- Certificati (o altre informazioni relative alla revoca) (minimo 5 anni) tenuti da CA.
- Documentazione delle richieste di certificato (minimo 5 anni) nel sistema CA.
- Altri dati o applicazioni sufficienti per verificare i contenuti dell'archivio (minimo 5 anni).
- Tutto il lavoro relativo alla PMA e ai verificatori dell'osservanza (minimo 5 anni).
- Documentazione RA (minimo 5 anni).

5.5.2 Periodo di mantenimento dell'archivio

Il periodo di mantenimento minimo per i dati archiviati è definito nella sezione 5.5.1 in alto. La PMA e il cliente decidono, in accordo con il proprietario dell'archivio, se alla fine del periodo di mantenimento di ogni archivio, vogliono cancellare o tenere tutto l'archivio o una parte di esso.

5.5.3 Protezione dell'archivio

Gli archivi vengono creati in modo da non poter essere facilmente cancellati o distrutti durante il periodo di mantenimento definito. La protezione dell'archivio assicura che solo le persone autorizzate possono accedervi.

Gli archivi vengono mantenuti in modo da assicurare l'integrità, l'autenticità e la riservatezza dei dati.

5.5.4 Procedura di backup dell'archivio

Se il supporto originale non è in grado di conservare i dati per il periodo richiesto, l'archivio definisce un meccanismo per il trasferimento periodico dei dati archiviati a un supporto nuovo.

5.5.5 Requisiti per la orodatazione documentazione

I servizi di orodatazione per la PKI non sono obbligatori.

La documentazione e i dati log hanno un periodo sicuro definito dalla PKI. I dettagli vengono dati nella sezione 6.8 in basso.

5.5.6 Sistema di raccolta archivi (interno o esterno)

Il sistema di raccolta archivi è conforme ai requisiti di sicurezza definiti nella sezione 5.4.6.

5.5.7 Procedure per ottenere e verificare le informazioni dell'archivio

I supporti che archiviano le informazioni degli archivi PKI vengono verificati al momento della loro creazione. Periodicamente, vengono testati dei campioni di informazioni archiviate per controllare la continua integrità e la leggibilità delle informazioni.

Solo il personale PMA e OA autorizzato ha il permesso di accedere agli archivi.

5.6 Passaggio chiave

5.6.1 Certificato sub-CA

Il periodo di validità della chiave privata Sub-CA viene definito in conformità con le raccomandazioni sulla sicurezza crittografata

per la lunghezza della chiave. Il periodo di validità del certificato Sub-CA viene definito nella sezione 6.3 in basso.

La Sub-CA non può generare i certificati dei sottoscrittori con un periodo di validità del certificato superiore al periodo di validità del certificato Sub-CA. Una nuova coppia di chiavi per la Sub-CA richiede la generazione di un nuovo certificato Sub-CA.

Il certificato sottoscrittori ha un periodo di validità del certificato fisso che non può essere modificato a causa della fine del periodo della Sub-CA.

Appena è stata generata una nuova coppia di chiavi per la Sub-CA, solo la nuova chiave privata viene utilizzata per firmare i certificati dei sottoscrittori.

Precedentemente, i certificati Sub-CA devono essere utilizzati per il processo di validazione del percorso di certificazione per tutti i certificati dei sottoscrittori firmati dal sottoscrittore precedente.

La PMA si riserva il diritto di modificare la chiave in qualsiasi momento.

5.6.2 Certificato dei sottoscrittori

Il periodo di validità della chiave privata sottoscrittori viene definito in conformità con le raccomandazioni sulla sicurezza crittografata per la lunghezza delle chiavi. Il periodo di validità del certificato sottoscrittori viene definito nella CP CA.

5.7 Ripristino in caso di compromissione e di disastro

5.7.1 Procedure per gestire gli incidenti e le compromissioni

Questo sistema deve essere supportato dall'impresa DOCUSIGN FRANCE che calcola l'infrastruttura e il suo incidente, la compromissione e i piani di continuità aziendale. Questi pianti devono essere testati, revisionati e aggiornati regolarmente, come da direttive date dalla DOCUSIGN FRANCE.

Se una componente PKI (per DocuSign France) individua un potenziale tentativo di hacking o un'altra forma di compromissione, esegue un'indagine per poter appurare la natura e il livello di danno. Lo scopo di un

danno potenziale viene constatato dalla PMA per poter appurare se la PKI deve essere ricostruita, o se è necessario solamente revocare alcuni certificati, e/o se la PKI è stata compromessa. In aggiunta, la PMA appura quali servizi devono essere mantenuti (revoca e informazioni sullo stato del certificato) e come, in accordo con il piano di continuità aziendale PMA.

Gli incidenti, le compromissioni e la continuità aziendale sono trattati nella CPS, che può anche affidarsi ad altre risorse e piani aziendali per l'esecuzione.

Se una componente RA (per il cliente) individua un potenziale tentativo di hacking o un'altra forma di compromissione, esegue un'indagine per poter appurare la natura e il livello di danno. Lo scopo di un danno potenziale viene constatato dal cliente per poter appurare se la RA deve essere ricostruita, o se è necessario solamente revocare alcuni certificati, e/o se la RA è stata compromessa. In aggiunta, il cliente appura quali servizi devono essere mantenuti e come, in accordo con il piano di continuità aziendale del cliente. In caso di compromissione del RA, il cliente deve informare il PMA.

Gli incidenti, le compromissioni e la continuità aziendale sono trattati nella documentazione del cliente, che può anche affidarsi ad altre risorse e piani aziendali per l'esecuzione.

5.7.2 Corruzione delle risorse informatiche, del software, e/o dei dati

Se l'equipaggiamento della PKI è danneggiato o è stato reso non operativo, ma le chiavi di firma non sono state distrutte, l'operazione viene ristabilita il più presto possibile, dando la priorità all'abilità di generare le informazioni sullo stato del certificato.

5.7.3 Procedure in caso di compromissione chiave privata

Se una chiave CA è compromessa, persa, distrutta o si sospetta sia stata compromessa:

- La PMA indaga sulla "questione chiave" e revoca il certificato associato.

- Una nuova coppia di chiavi viene generata e una nuovo certificato viene creato.

- Segnalazione al cliente.

Se il sistema utilizzato dal servizio Protect and Sign (Firma personale) per generare la coppia di chiavi sottoscrittori è stato compromesso, la PMA avverte il cliente e fornisce una lista dettagliata di rischi e di conseguenze per il cliente e per i sottoscrittori, causati dalla compromissione.

Se uno degli algoritmi o dei parametri associati utilizzati dalla CA o dai suoi sottoscrittori diventa insufficiente per l'utilizzo restante che se ne intende fare, la CA deve informare il cliente e modificare gli algoritmi utilizzati.

5.7.4 Capacità di continuità operativa successivamente al disastro

Il piano di continuità aziendale si rivolge a tutte le operazioni necessarie, come descritto nella sezione 5.7.1 in alto.

5.8 Risoluzione

5.8.1 Sub-CA

Nel caso di una risoluzione dei servizi PKI, la PMA fornisce una notifica precedente alla risoluzione, e:

- Informa il cliente.

- Distrugge la chiave privata Sub-CA.

- Pubblica le informazioni sullo stato della revoca più recenti (CRL firmata dalla CA) inviandole a tutti gli utilizzatori (se ce ne sono).

- La Sub-CA firmata dalla ICA smette di fornire certificati in accordo con e in riferimento a presente CP e in accordo con la sua CP.

- Nel caso di una Sub-CA compromessa, la PMA e la OA utilizzano entrambe mezzi sicuri per comunicare ai sottoscrittori e agli utilizzatori che devono cancellare tutti i certificati sicuri che rappresentano la Sub-CA con la coppia di chiavi compromessa / le coppie di chiavi compromesse.

- Archivia tutti i log di verifica e l'altra documentazione prima di risolvere la PKI.

- La documentazione archiviata viene trasferita alla PMA.

Nel caso di una risoluzione dei servizi OA, la OA è responsabile di conservare tutta la documentazione rilevante che si riferisce alle necessità dei sottoscrittori e delle componenti PKI. La OA trasmette quindi la sua documentazione alla PMA.

5.8.2 RA

Nel caso di una risoluzione dei servizi RA, il cliente fornisce una notifica precedente alla risoluzione, e:

- Informa la PMA tramite lettera raccomandata.

- Distrugge tutte le chiavi private utilizzate per assicurare la comunicazione con la CA.

- Pubblica le informazioni sullo stato della revoca più recenti (CRL firmata dalla CA) inviandole a tutti gli utilizzatori (se ce ne sono).

- La RA cessa di fornire le richieste di certificati alla CA.

- Nel caso di una RA compromessa, il cliente utilizza mezzi sicuri per comunicare ai sottoscrittori e utilizzatori che non devono fidarsi dei certificati sottoscrittori identificati nella lista fornita dal cliente.

- Archivia tutti i log di verifica e l'altra documentazione prima di risolvere la PKI.

- La documentazione archiviata viene trasferita a una entità designata dal cliente.

Nel caso di una risoluzione dei servizi OA, la OA è responsabile di conservare tutta la documentazione rilevante che si riferisce alle necessità dei sottoscrittori e delle componenti PKI. La OA trasmette quindi la sua documentazione al cliente.

6 CONTROLLI DI SICUREZZA TECNICA

6.1 Generazione e installazione di una coppia di chiavi

6.1.1 Generazione di coppia di chiavi

6.1.1.1 Sub-CA

Dopo che la PMA ha accettato la generazione della Sub-CA, una coppia di chiavi e la CSR vengono generate per la Sub-CA.

L'operazione della generazione della coppia di chiavi Sub-CA e della CSR viene documentata su video ed eseguita conformemente a uno script per le cerimonie delle chiavi. Il HSM utilizzato per la cerimonia delle chiavi è conforme ai requisiti definiti nella sezione 6.2.1 in basso.

La generazione della coppia di chiavi Sub-CA viene eseguita e testimoniata in un ambiente fisicamente sicuro (vedi sezione 5.1 in alto) dal personale con ruoli di fiducia (vedi sezione 5.2 in alto) alla presenza almeno di una supervisione doppia. I dati di attivazione della chiave privata vengono distribuiti ai titolari dei dati di attivazione che sono gli impiegati fidati. La generazione della chiave Sub-CA viene eseguita all'interno di un modulo di sicurezza hardware (vedi sezione 6.2 in basso). I testimoni sono delle persone diverse dal personale operativo. L'attivazione e l'inizializzazione del HSM Sub-CA avviene sotto controllo dei titolari dei dati di attivazione Sub-CA. Durante la cerimonia delle chiavi, la coppia di chiavi Sub-CA viene garantita con backup (vedi sezione 6.2. in basso).

6.1.1.2 Sottoscrittori

Il software Protect and Sign (Firma personale) deve richiedere la generazione della coppia di chiavi di firma del sottoscrittore. La generazione viene eseguita utilizzando un HSM (vedi sezione 6.2.11 in basso). La generazione deve essere eseguita in modo da evitare la compromissione della chiave privata e dei dati di attivazione associati ed evitare le operazioni di firma non richiesti. La chiave privata deve essere protetta con i dati di attivazione associati.

6.1.2 Consegna chiave privata

Non applicabile.

6.1.3 Consegna della chiave pubblica all'emittente del certificato

6.1.3.1 Sub-CA

Le chiavi pubbliche Sub-CA vengono consegnate in modo sicuro al ICA corrispondente per il rilascio del certificato durante le cerimonie delle chiavi (per il set-up della PKI) o durante il processo di registrazione (vedi le sezioni 4.1 e 4.2 in basso). Il meccanismo di consegna lega le identità controllate da Sub-CA alle chiavi pubbliche da certificare, utilizzando il formato Pkcs#10.

6.1.3.2 Sottoscrittori

Una chiave pubblica sottoscrittori viene consegnata in modo sicuro dal software Protect and Sign (Firma personale) alla Sub-CA per il rilascio del certificato. Il meccanismo di consegna vincola le identità verificate alle chiavi pubbliche da

certificare, utilizzando il formato Pkcs#10.

6.1.4 Consegna della chiave pubblica CA agli utilizzatori

Vedi sezione 2 in alto.

6.1.5 Misure chiavi

6.1.5.1 Sub-CA

La coppia di chiavi ha una lunghezza di 2048, per l'algoritmo RSA.

L'algoritmo RSA viene utilizzato con il SHA-2 come funzione hash.

6.1.5.2 Sottoscrittori

La coppia di chiavi ha una lunghezza di 2048, per l'algoritmo RSA.

L'algoritmo RSA viene utilizzato con il SHA-2 come funzione hash.

6.1.6 Generazione parametri chiave pubblica e controllo qualità

6.1.6.1 Sub-CA

I parametri della chiave pubblica devono essere sempre generati e controllati in accordo con gli standard che definiscono l'algoritmo crittografico per i parametri che devono essere utilizzati.

Le chiavi Sub-CA vengono generate in accordo con gli strumenti crittografici dei moduli di sicurezza hardware (vedi sezione 6.2.11 in basso).

6.1.6.2 Sottoscrittori

I parametri della chiave pubblica devono essere sempre generati e controllati in accordo con gli standard che definiscono l'algoritmo crittografico in cui devono essere utilizzati i parametri.

Le chiavi sottoscrittori vengono generate in accordo con gli strumenti crittografici dei moduli di sicurezza hardware o i token utilizzati per proteggere le chiavi (vedi sezione 6.2.11 in basso).

6.1.7 Scopo utilizzo chiave (al campo di utilizzo della chiave X.509 v3)

L'utilizzo di una chiave specifica viene appurata dall'estensione keyUsage nel certificato X.509. I profili dei certificati nella sezione 10 in basso specificano i valori consentiti per questa estensione per differenti tipi di certificati definiti in presente CP, e tutte le Sub-CA che emettono certificati in accordo con presente CP devono aderire a tali valori.

6.2 Protezione chiave privata e controlli tecnici modulo crittografico

6.2.1 Standard e controlli modulo crittografico

6.2.1.1 Sub-CA

La Sub-CA genera le sue coppie di chiavi e archivia le sue chiavi private in un HSM che è certificato conformemente alla classificazione specificata nella sezione 6.2.11 in basso.

6.2.1.2 Sottoscrittori

Le coppie di chiavi vengono generate e conservate in un HSM o un token che è certificato conformemente alla classificazione specificata nella sezione 6.2.11 in basso.

6.2.2 Controllo persone multiple chiave privata (N out of M)

6.2.2.1 Sub-CA

La Sub-CA esegue meccanismi tecnici e procedurali che richiedono la partecipazione di autorizzazioni di individui fidati multipli, per eseguire le operazioni crittografate Sub-CA sensibili.

6.2.2.2 Sottoscrittori: OID differente da 1.3.6.1.4.1.22234.2.8.3.20

La coppia di chiavi dei sottoscrittori viene attivata dopo l'autenticazione del sottoscrittore avvenuta con successo, utilizzando i suoi dati di attivazione conformemente al protocollo di approvazione scelto dal cliente.

6.2.2.3 Sottoscrittori: OID 1.3.6.1.4.1.22234.2.8.3.20

La coppia di chiavi dei sottoscrittori viene attivata dopo l'autenticazione del sottoscrittore avvenuta con successo, utilizzando i suoi dati di attivazione (codice OTP inviato tramite SMS al sottoscrittore), conformemente al protocollo di approvazione definito nel [PSM SSCD].

6.2.3 Deposito chiave privata

6.2.3.1 Sub-CA

In nessuna circostanza, una chiave privata Sub-CA può essere depositata a una componente PKI o una terza parte.

6.2.3.2 Sottoscrittori

In nessuna circostanza, una chiave privata deve essere depositata da una terza parte o dalle componenti PKI.

6.2.4 Backup chiave privata

6.2.4.1 Sub-CA

Le chiavi di firma privata Sub-CA devono essere garantite tramite backup con lo stesso controllo a persone multiple come quelle operative. Una copia di backup singola della chiave di firma deve essere conservata nell'ubicazione dei sistemi Sub-CA. Una seconda copia di backup deve essere tenuta in un luogo di backup Sub-CA offsite. Tutte le ubicazioni devono essere accettate dalla PMA.

6.2.4.2 Sottoscrittori

Non applicabile.

6.2.5 Archiviazione chiave privata

6.2.5.1 Sub-CA

Le chiavi private Sub-CA non devono mai essere archiviate.

6.2.5.2 Sottoscrittori

Non applicabile.

6.2.6 Trasferimento chiave privata verso e da un modulo crittografato

6.2.6.1 Chiave privata CA

Nel caso del trasferimento di una chiave privata, la coppia di chiavi Sub-CA viene trasferita in un altro modulo di sicurezza hardware (HSM) con le stesse specifiche di quelle descritte nella sezione 6.2, con una copia diretta token-to-token, tramite un percorso sicuro con il controllo a persone multiple N di M (vedi sezione 6.2).

Le chiavi Sub-CA vengono generate, attivate e conservate in HSM o in un formato criptato. Se non sono conservate su HSM, le chiavi private Sub-CA sono criptate. Una chiave privata Sub-CA criptata non può essere decriptata utilizzando un HSM con i ruoli di fiducia richiesti (titolari dei dati di attivazione), e devono essere eseguiti in presenza di persone multiple con ruoli di fiducia.

6.2.6.2 Sottoscrittori

Non applicabile.

6.2.7 Stoccaggio chiave privata su modulo crittografico

6.2.7.1 Sub-CA

Il HSM può conservare chiavi private in qualsiasi forma, finché le chiavi non sono accessibili senza i meccanismi di autenticazione che sono conformi a quelli citati nella policy di sicurezza allegata al HSM approvato.

6.2.7.2 Sottoscrittori: OID differente da 1.3.6.1.4.1.22234.2.8.3.20

Il HSM dedicato al servizio Protect and Sign (Firma personale) conserva le chiavi private in qualsiasi forma, finché le chiavi non sono accessibili senza i meccanismi di autenticazione che sono conformi a quelli citati nella policy di sicurezza allegata al HSM approvato e in accordo con il protocollo di approvazione.

6.2.7.3 Sottoscrittori: OID 1.3.6.1.4.1.22234.2.8.3.20

La ripartizione dedicata nel HSM del servizio Protect and Sign (Firma personale) conserva le chiavi private in qualsiasi forma, finché le chiavi non sono accessibili senza i meccanismi di autenticazione che sono conformi a quelli citati nella policy di sicurezza allegata al HSM approvato e in accordo con il protocollo di approvazione definito nel [PSM SSCD].

6.2.8 Metodo di attivazione chiave privata

6.2.8.1 Sub-CA

Sono richiesti numerosi ruoli di fiducia con i dati di attivazione per eseguire l'attivazione iniziale del HSM che contiene la coppia di chiavi Sub-CA corrispondente a un certificato Sub-CA. Una volta che il HSM contenente la chiave Sub-CA e la chiave Sub-CA sono operativi, solo i servizi autorizzati del sistema PKI possono utilizzare la coppia di chiavi Sub-CA nel HSM, utilizzando l'interfaccia autenticata reciprocamente dei sistemi PKI.

6.2.8.2 Sottoscrittori: OID differente da 1.3.6.1.4.1.22234.2.8.3.20

La coppia di chiavi sottoscrittori viene attivata conformemente al protocollo di approvazione del cliente. Il protocollo di approvazione deve richiedere dei dati di attivazione tecnica (per esempio: codice OTP, certificato di autenticazione utilizzato dal sottoscrittore, da autenticare dalla CA o token OTP).

6.2.8.3 Sottoscrittori: OID 1.3.6.1.4.1.22234.2.8.3.20

La coppia di chiavi dei sottoscrittori viene attivata conformemente al protocollo di approvazione definito nel [PSM SSCD]. Il protocollo di approvazione deve richiedere al sottoscrittore un codice OTP trasmesso dal PSM tramite SMS utilizzando un numero di telefono cellulare trasmesso dalla RA.

6.2.9 Metodo di disattivazione chiave privata

6.2.9.1 Sub-CA

Un HSM Sub-CA che è stato attivato, non viene mai reso disponibile a un accesso non autorizzato.

Dopo essere stati usati, i HSM vengono disattivati. Dopo la disattivazione, l'utilizzo della coppia di chiavi Sub-CA basata sul HSM deve richiedere la presenza di ruoli di fiducia con i dati di attivazione per poter riattivare detta coppia di chiavi Sub-CA (vedi sezione 6.2).

Il HSM disattiva il HSM automaticamente se si verifica un incidente.

6.2.9.2 Sottoscrittori

La coppia di chiavi dei sottoscrittori viene usata per firmare i documenti durante una transazione richiesta dalla RA, conformemente al [PSPM] e il protocollo di approvazione del cliente e la policy di firma del cliente, e viene distrutta immediatamente dopo l'utilizzo.

6.2.10 Metodo di distruzione chiave privata

6.2.10.1 Sub-CA

La distruzione di una chiave privata Sub-CA in un HSM richiede la distruzione della chiave / delle chiavi nel HSM utilizzando la funzione di azzeramento del hardware in modo da bloccare l'utilizzo delle informazioni per recuperare qualsiasi parte della chiave privata. Tutti i backup delle chiavi private Sub-CA devono essere distrutti utilizzando lo stesso livello di sicurezza. Se le funzioni HSM non sono accessibili per poter distruggere il contenuto della chiave, il HSM deve essere distrutto fisicamente.

L'operazione di distruzione viene realizzata in un ambiente fisicamente sicuro (vedi sezione 5.1 in alto) dal personale con ruoli di fiducia (vedi sezione 5.2 in alto) alla presenza almeno di una supervisione doppia.

6.2.10.2 Sottoscrittori

La distruzione di una chiave privata sottoscrittori in un HSM richiede la distruzione della chiave / delle chiavi nel HSM utilizzando la funzione di azzeramento del hardware in modo da bloccare l'utilizzo delle informazioni per recuperare qualsiasi parte della chiave privata. Se le funzioni HSM non sono accessibili per poter distruggere il contenuto della chiave, il HSM deve essere distrutto fisicamente.

6.2.11 Classificazione modulo crittografico

6.2.11.1 Sub-CA

Il modulo di sicurezza hardware utilizzato per generare le coppie di chiavi RCA viene approvato almeno in accordo con lo standard FIPS 140 - 2 livello 3 o i criteri comuni EAL4+ equivalenti.

6.2.11.2 Sottoscrittori: OID differente da 1.3.6.1.4.1.22234.2.8.3.20

Il modulo di sicurezza hardware utilizzato per generare le coppie di chiavi sottoscrittori viene approvato almeno in accordo con lo standard FIPS 140 - 2 livello 2 o i criteri comuni EAL4+ equivalenti.

6.2.11.3 Sottoscrittori: OID 1.3.6.1.4.1.22234.2.8.3.20

Il modulo di sicurezza hardware utilizzato per generare le coppie di chiavi sottoscrittori viene approvato almeno in accordo con lo standard FIPS 140 - 2 livello 3 o i criteri comuni EAL4+ equivalenti, e certificato come un SSCD compatibili con i requisiti dell'allegato III della Direttiva 1999/93/CE.

6.3 Altri aspetti della gestione della coppia di chiavi

6.3.1 Archiviazione chiave pubblica

Le chiavi pubbliche vengono archiviate come parte dell'archiviazione del certificato, come descritto nella sezione 5.5 in alto.

6.3.2 Periodi operativi del certificato e periodi di utilizzo della coppia di chiavi

6.3.2.1 Sub-CA

Il periodo operativo massimo di una chiave privata Sub-CA è di cinque (5) anni.

Il periodo operativo massimo di un certificato Sub-CA è di 5 (5) anni. **6.3.2.2 Sottoscrittori**

Una chiave privata sottoscrittori può essere utilizzata finché il certificato associato è valido, e può essere utilizzata per decriptare i dati criptati finché è necessario.

Il periodo di validità del certificato sottoscrittori viene dato nella sezione 10.

6.4 Dati di attivazione

6.4.1 Generazione e installazione dati di attivazione

6.4.1.1 Sub-CA

I dati di attivazione Sub-CA utilizzati per proteggere il HSM contenente le chiavi private Sub-CA vengono generati durante la cerimonia delle chiavi PKI iniziale. I dati di attivazione utilizzati per sbloccare le chiavi private, in congiunzione con qualsiasi altro controllo di accesso, deve avere un livello appropriato di forza per proteggere le chiavi o i dati, e deve soddisfare i requisiti della policy di sicurezza applicabile del modulo

crittografico utilizzato per conservare le chiavi. Alcuni dei dati di attivazione più critici sono i backup (la CPS fornisce i dettagli esatti).

Gli individui incaricati dalla PMA devono ricevere i loro dati di attivazione durante la cerimonia delle chiavi tramite la riunione faccia a faccia. La creazione e la distribuzione dei dati di attivazione sono registrati. I dati di attivazione non vengono mai trasmessi da altri mezzi.

6.4.1.2 Sottoscrittori: OID differente da 1.3.6.1.4.1.22234.2.8.3.20

Il protocollo di approvazione (vedi sezione 4.3 in alto) richiede i dati di attivazione tecnica (per esempio: codice OTP, certificato di autenticazione utilizzato dal sottoscrittore, da autenticare dalla CA o token OTP). Questi dati di attivazione vengono generati dalla RA o dalla piattaforma del Protect and Sign (Firma personale) o accettati dal cliente (per esempio, il cliente può accettare l'utilizzo del certificato fornito al sottoscrittore per poter autenticare il sottoscrittore durante il protocollo di approvazione). Se i dati di attivazione vengono generati dal cliente o accettati dal cliente, questi dati di attivazione devono essere trasmessi in modo sicuro alla Protect and Sign (Firma personale) per poter essere utilizzati dalla Protect and Sign (Firma personale) per autenticare il sottoscrittore.

6.4.1.3 Sottoscrittori: OID 1.3.6.1.4.1.22234.2.8.3.20

Il protocollo di approvazione (vedi sezione 4.3 in alto) richiede dati di attivazione tecnici che sono un codice OTP inviato tramite SMS.

Questo codice OTP viene generato dalla piattaforma Protect and Sign (Firma personale) conformemente al protocollo di approvazione definito nel [PSM SSCD].

6.4.2 Protezione dati di attivazione

6.4.2.1 Sub-CA

I dati di attivazione sono protetti contro una divulgazione da una combinazione di meccanismo di controllo dell'accesso crittografico e fisico. I titolari dei dati di attivazione sono responsabili della loro protezione e della loro tracciabilità.

La PMA richiede che i titolari dati di attivazione conservino i loro dati di attivazione in una cassaforte con un accesso controllato sia dai titolari sia dagli impiegati con ruoli di fiducia.

Se i dati di attivazione sono scritti sulla carta, questa carta deve essere conservata in modo sicuro in una cassaforte.

6.4.2.2 Sottoscrittori: OID differente da 1.3.6.1.4.1.22234.2.8.3.20

Il sottoscrittore è responsabile di assicurare la protezione dei suoi dati di attivazione.

Se i dati di attivazione sono gestiti dal cliente, dalla RA e/o dalla Protect and Sign (Firma personale), queste entità sono anche responsabili della protezione dei dati di attivazione in modo da evitare l'utilizzo dei dati di attivazione da entità che non siano il sottoscrittore.

6.4.2.3 Sottoscrittori: OID 1.3.6.1.4.1.22234.2.8.3.20

Il sottoscrittore è responsabile di assicurare la protezione dei suoi dati di attivazione.

Se i dati di attivazione sono gestiti dalla Sign (Firma personale), questa entità è anche responsabili della protezione dei dati di attivazione in modo da evitare l'utilizzo dei dati di attivazione da entità che non siano il sottoscrittore.

6.4.3 Altri aspetti dei dati di attivazione

6.4.3.1 CA

I dati di attivazione vengono modificati se le chiavi dei moduli di sicurezza hardware vengono ricreate o se i moduli di sicurezza hardware vengono restituiti al produttore per la manutenzione. Gli altri aspetti della gestione dei dati di attivazione vengono indicati nella CPS.

6.4.3.2 Sottoscrittori (persone fisiche)

Non applicabile.

6.5 Controlli di sicurezza computer

6.5.1 Requisiti tecnici specifici sicurezza computer

Le seguenti funzioni di sicurezza del computer vengono fornite dal sistema operativo o tramite una combinazione tra il sistema operativo, il software e salvaguardia fisica. Le componenti PKI attuano le seguenti funzioni (sistema informatico CA e RA se applicabile):

- Richiesta dei login autenticati per i ruoli di fiducia.
- Fornitura del controllo di accesso discrezionale.
- Richiesta di utilizzo dell'autenticazione per la comunicazione di sessione.
- Richiesta dell'identificazione dell'utente.
- Fornitura dell'isolamento del dominio per i processi che coinvolgono i ruoli che utilizzano i servizi della PKI.
- Rimozione dei servizi e dei port non desiderati dalle componenti PKI.

Quando l'equipaggiamento PKI viene ospitato sulle piattaforme certificate per i requisiti di assicurazione della sicurezza del computer, quando possibile, il sistema (hardware, software e sistema operativo) opera in detta configurazione certificata.

Queste piattaforme utilizzano almeno la stessa versione del sistema operativo del computer di quella che ha ricevuto la classificazione di valutazione. I sistemi dei computer OA sono configurati minimo con gli account richiesti, i servizi di network e un login non remoto.

La generazione della coppia di chiavi Sub-CA viene eseguita sui HSM online, eccezion fatta durante il setup del sistema PKI, dove il HSM utilizzato online viene impostato in un ambiente offline.

Il software PSM deve essere installato conformemente a [PSM SSCD].

Le workstation per le cerimonie delle chiavi sono dedicate alle operazioni relative alle cerimonie delle chiavi e non sono connesse ad alcun network pubblico. I computer utilizzati per l'amministrazione dei sistemi PKI sono dedicati solamente a questo compito.

I seguenti regolamenti vengono applicati alla CA e alla RA:

– Seguire una procedura documentata per incaricare gli individui con ruoli di fiducia e assegnare loro la responsabilità per ogni componente PKI.

– Documentare la responsabilità e i compiti assegnati ai ruoli di fiducia e attuare la "separazione dei compiti" per detti ruoli di fiducia basati su aspetti relativi alla sicurezza delle funzioni da eseguire su ogni componente PKI.

– Assicurare che solo il personale assegnato ai ruoli di fiducia abbia accesso alle componenti PKI.

– Assicurare che un individuo con un ruolo di fiducia agisca solamente con lo scopo di detto ruolo, quando esegue i compiti amministrativi assegnati a quel ruolo sulla componente PKI.

– Richiedere agli impiegati e agli appaltatori di osservare il principio del "privilegio minimo" quando effettuano l'accesso, o quando vengono configurati i privilegi sul sistema PKI (vedi sezione 5.2 in alto).

– Richiedere che ogni individuo con un ruolo di fiducia utilizzi una credenziale univoca creata da o assegnata a quella persona per poter autenticare alla componente PKI.

– Se un controllo dell'autenticazione utilizzato dai ruoli di fiducia è un nome utente e una password, allora la gestione di tali autenticazioni deve essere eseguita in accordo con la policy di sicurezza delle società di capitali.

– Richiedere ai ruoli di fiducia per effettuare il logout dal servizio PKI della componente PKI e per bloccare le workstation quando non sono in uso.

– Configurare le workstation con time-out per inattività, che effettuano il logout dell'utente e bloccano le workstation dopo un periodo di tempo prefissato di inattività senza che l'utente abbia effettuato alcun inserimento (le componenti PKI consentono a una workstation di rimanere attiva e non presidiata se la workstation è resa sicura in altro modo e se sono in funzione dei compiti amministrativi che in caso di time-out per inattività o un blocco di sistema verrebbero interrotti).

– Revisione di tutti gli account di sistema e disattivare qualsiasi account che non è più necessario per le operazioni.

– Se applicabile a una componente PKI (vale solo per una componente PKI che usa un sistema di controllo dell'accesso differente da un certificato per un ruolo di fiducia), bloccare l'accesso dell'account alla componente PKI dopo un numero definito di tentativi massimi falliti, premesso che questo provvedimento di sicurezza sia supportato dalla componente PKI e non indebolisca la sicurezza di questo controllo dell'autenticazione.

– Attuare un processo che disabiliti tutti gli accessi privilegiati di un individuo alla componente PKI entro 24 ore dalla risoluzione dell'impiego del individuo (con un ruolo di fiducia) o del rapporto contrattuale con la componente PKI.

– Implementare l'autenticazione forte per l'accesso dell'amministratore a tutte le componenti PKI.

6.5.2 Classificazione sicurezza computer

Nessuna stipulazione. Per OID 1.3.6.1.4.1.22234.2.8.3.20, il software PSM viene certificato conformemente a [PSM SSCD].

6.6 Controlli tecnici ciclo di vita

6.6.1 Controlli di sviluppo del sistema

I controlli dello sviluppo del sistema per la PKI sono seguenti:

- Utilizzare un software che è stato destinato e sviluppato con una metodologia di sviluppo formale e documentata, conformemente alla valutazione dei criteri comuni (per CA).

- Il hardware e il software fornito deve essere acquistato in modo da ridurre la probabilità che un particolare componente possa essere stato manomesso.

- Il hardware e il software deve essere sviluppato in un ambiente controllato e il processo di sviluppo deve essere definito e documentato. Questo requisito non vale per hardware o software commerciale disponibile sul mercato.

- Tutto il hardware deve essere spedito o consegnato tramite metodi controllati che forniscono una catena continua di tracciabilità, dal luogo di acquisto fino al luogo delle operazioni.

- Il hardware e il software devono essere dedicati all'esecuzione delle attività della PKI. Non ci devono essere altre applicazioni; dispositivi hardware, connessioni a network o software componenti installati che non sono parte dell'operazione PKI.

- È necessario che si provveda in modo accurato a prevenire che sull'equipaggiamento venga caricato del software sospetto.

Solo le applicazioni richieste per eseguire le operazioni PKI devono essere ottenute da fonti autorizzate dalla policy locale. Il hardware e il software PKI devono essere scansionati per verificare che non ci siano codici sospetti, al primo utilizzo e successivamente a intervalli periodici.

Gli aggiornamenti del hardware e del software devono essere acquistati o sviluppati allo stesso modo dell'equipaggiamento originale, e devono essere installati dal personale fidato e addestrato in un modo definito.

6.6.2 Controlli di gestione della sicurezza

La configurazione del sistema PKI, così come le modifiche e gli aggiornamenti, devono essere documentati e controllati. Una procedura deve essere utilizzata per l'installazione e la manutenzione continua del sistema PKI. Il software PKI deve essere verificato, affinché si sia sicuri che è quello fornito dal venditore, senza modifiche, e nella versione che si intende utilizzare. Ci deve essere un meccanismo per rilevare una modifica non autorizzata sul software o sulla configurazione. Una metodologia per la gestione della configurazione formale deve essere utilizzata per l'installazione e la manutenzione continua del sistema.

Valgono seguenti regolamenti:

– Attuare un sistema di amministrazione informatica sotto il controllo della OA che monitorizza, rileva e registra qualsiasi modifica nella configurazione relativa alla sicurezza dei sistemi PKI.

– Richiedere al personale con ruoli di fiducia di seguire le segnalazioni di possibili eventi di sicurezza critica.

– Condurre una revisione umana dell'applicazione e dei log di sistema e assicurare che il monitoraggio, in logging, la segnalazione e le funzione di verifica dell'integrità dei log operino correttamente (vedi sezione 5.4.8 in alto).

6.6.3 Controlli di sicurezza ciclo di vita

Per il software e il hardware valutati, la PMA monitorizza i requisiti dello schema di manutenzione per assicurare lo stesso livello di fiducia.

Le domande di capacità vengono monitorate e le proiezioni dei futuri requisiti di capacità vengono fatte per assicurare che siano disponibili una energia e una archiviazione di processo adeguate.

6.7 Controlli di sicurezza rete

Il sistema PKI deve attuare dei provvedimenti di sicurezza appropriati per assicurare che siano garantiti contro un rifiuto del servizio e da attacchi di intrusione. Tali provvedimenti devono includere l'utilizzo di guardie, firewall e router filtranti.

I port e i servizi della rete non utilizzati devono essere spenti. Qualsiasi software di rete presente deve essere necessario per il funzionamento del sistema PKI.

Valgono seguenti regolamenti:

– Qualsiasi dispositivo di controllo limitante utilizzato per proteggere la rete sul quale è ospitato l'equipaggiamento PKI, deve rifiutare tutti i servizi che non sono necessari all'equipaggiamento PKI, anche se questi servizi sono abilitati per altri dispositivi in rete.

– Segmentazione dell'equipaggiamento PKI nelle reti o nelle zone, in base al loro rapporto funzionale, logico e fisico (incluso l'ubicazione). Solo il flusso autorizzato, utilizzato per l'amministrazione e i servizi della PKI, tra l'equipaggiamento PKI deve essere autorizzato.

– Mantenimento e protezione delle componenti PKI in almeno una zona dedicata, e esecuzione di una separazione tra le interfacce accessibili da internet e le interfacce accessibili da necessità interne (il front end e il back end come l'architettura N-Thirds devono essere posizionati).

– Attuazione e configurazione di una rete di amministrazione (un sistema utilizzato per fornire funzioni di supporto alla sicurezza, come l'autenticazione, il controllo limitante del network, il logging di verifica, la riduzione e l'analisi del log di verifica, la scansione della vulnerabilità, l'antivirus quando è applicabile e l'amministrazione informatica) che protegga i sistemi e le comunicazioni tra i sistemi PKI e le comunicazioni con sistemi non PKI all'infuori da tali zone (incluse quelle con le unità aziendali organizzative che non forniscono servizi relativi alla PKI) e quelli su reti pubbliche.

– Configurazione di ogni controllo limitativo della rete (firewall, switch, router, gateway o altri dispositivi di controllo della rete o sistema) con regolamenti che supportino solo i servizi, i protocolli, i port e le comunicazioni che la componente PKI ha identificato come necessari per le sue operazioni.

– Configurazione delle componenti PKI, rimuovendo o disabilitando tutti gli account, le applicazioni, i servizi, i protocolli e i port che non vengono utilizzati nelle operazioni della componente PKI, e consentendo solamente quelli che sono approvati dalla componente PKI.

– Revisione delle configurazioni del sistema PKI almeno una volta la settimana (per CA) e conformemente alla policy di sicurezza del cliente per RA, determinazione se le modifiche fatti hanno violato le policy di sicurezza della componente PKI.

– Garanzia dell'accesso dell'amministrazione alle componenti PKI solo a persone che agiscono con ruoli di fiducia e richiesta della loro tracciabilità per la sicurezza della componente PKI.

– Attuazione di una autenticazione forte per ogni componente del sistema PKI che supporti una autenticazione con fattori multipli.

– Modifica delle chiavi e delle password di autenticazione per qualsiasi account privilegiato o account di servizio su un sistema PKI, ogni volta che l'autorizzazione della persona ad accedere a livello amministrativo a quell'account sul sistema PKI è stata modificata o revocata.

– Applicazione dei patch di sicurezza, visionati dall'editor e dall'entità software come la CERT, obbligatoriamente, per evitare un attacco concreto e ad alto rischio al sistema PKI, con sistemi PKI entro sei mesi dalla disponibilità del patch di sicurezza, a meno che la PKI non stabilisca che il patch di sicurezza introdurrebbe una vulnerabilità aggiuntiva o una instabilità che supera i benefici dell'applicazione del patch di sicurezza.

Per OID 1.3.6.1.4.1.22234.2.8.3.20, il software PSM deve essere installato conformemente a [PSM SSCD].

6.8 Orodatazione

Le procedure elettroniche o manuali devono essere utilizzate per mantenere l'ora del sistema. Gli adeguamenti dell'orologio sono degli eventi verificabili come elencato nella sezione 5.4 in alto. La cerimonia delle chiavi utilizza una procedura manuale.

Per un orario sicuro sulla documentazione di verifica, è necessario che tutti i componenti del sistema Sub-CA siano sincronizzati regolarmente con un servizio orario come il servizio Network Time Protocol (NTP). L'orario derivato dal servizio orario deve essere utilizzato per costituire l'orario di:

- Ora di validità iniziale di un certificato sottoscrittori.

- Ora di validità iniziale della CRL e la risposta OCSP.

Le informazioni aggiuntive vengono date nella CPS applicabile. Il cliente deve occuparsi del sistema RA per controllare l'orario del sistema.

7 PROFILI CERTIFICATO, CRL E OCSP

7.1 Profilo certificato

7.1.1 Numeri versione

I certificati emessi sono i certificati X.509 v3 (campo versione popolato con intero "2").

7.1.2 Estensioni certificato

Qualsiasi Sub-CA che afferma delle estensioni private critiche deve essere interoperativo nella loro comunità di utilizzo previsto.

La Sub-CA dell'emittente e i certificati dei sottoscrittori possono contenere qualsiasi estensione come specificato dalla RFC 5280 nel certificato, ma deve contenere le estensioni richieste da presente CP. Qualsiasi estensione opzionale o aggiuntiva deve essere non critica e non deve essere in conflitto con il certificato e i profili CRL definiti in presente CP. La sezione 10 contiene questi profili di certificato.

7.1.3 Identificatori oggetto algoritmo

I certificati emessi in conformità con presente CP devono utilizzare i seguenti OID per le firme:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

I certificati emessi in conformità con presente CP devono utilizzare i seguenti OID per le firme:

Sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(5)}

I certificati in conformità con presente CP devono utilizzare i seguenti OID per identificare le informazioni della chiave pubblica del soggetto:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}

7.1.4 Forme del nome

I capi relativi al soggetto e all'emittente del certificato devono essere compilati con un nome distinto univo, in accordo con uno o più standard della serie X.500, con il tipo di caratteristiche vincolati più avanti con [RFC5280] e la sezione 3.1.

7.1.5 Restrizioni nome

La Sub-CA afferma le restrizioni critiche e non critiche dei nomi all'infuori di quelle specificate nei profili del certificato nella sezione 10 in basso per il certificato Sub-CA e il certificato sottoscrittori.

7.1.6 Identificatore oggetto policy dei certificati

La Sub-CA non deve contenere gli OID della policy dei certificati definiti in presente CP, elencati nella sezione 1.2 di presente CP, nell'estensione della policy dei certificati, se emette un certificato sottoscrittori che contiene un OID elencato nella sezione 1.2.

Il certificato sottoscrittori deve avere un solo OID, elencato nella sezione 1.2 di presente CP, nell'estensione della policy dei certificati.

7.1.7 Utilizzo dell'estensione delle restrizioni della policy

Non applicabile.

7.1.8 Sintassi e semantica dei qualificatori della policy

I certificati emessi in conformità con presente CP possono contenere dei qualificatori della policy come la notifica all'utente, il nome della policy e i riferimenti CP e CPS come descritto nella sezione 10 in basso.

7.1.9 Semantiche di lavorazione dell'estensione della policy dei certificati critici

La semantica di lavorazione per l'estensione critica della policy dei certificati deve essere conforme ai regolamenti di lavorazione del percorso di certificazione X.509, come descritto nella sezione 10 in basso.

7.2 Profilo CRL

Vedi sezione 10 in basso.

7.3 Profilo OCSP

Vedi sezione 10 in basso.

8 VERIFICA DI CONFORMITÀ E ALTRE VALUTAZIONI

8.1 Frequenza o circostanze della valutazione

Le componenti PKI sono soggette a una verifica periodica dell'osservanza, almeno una volta l'anno, per consentire alla PMA di autorizzare o meno (a seconda del risultato della verifica) le componenti PKI ospitate dalla OA per operare nel rispetto di presente CP, conformemente alla "Guida alla verifica delle PKI" fornita dalla ICA.

La PMA ha il diritto di richiedere una verifica non periodica dell'osservanza delle componenti PKI (specialmente la RA) che operano nel rispetto di presente CP. La PMA indica la motivazione per qualsiasi verifica non periodica dell'osservanza.

Durante il periodo in cui la CA emette dei certificati, la PMA deve monitorare l'aderenza alla sua policy dei certificati, alla dichiarazione della pratica di certificazione e ai requisiti RA, e controllare severamente la sua qualità del servizio, eseguendo delle auto-verifiche almeno una volta l'anno, con un campione selezionato a caso di un numero di campioni più grande di uno, o almeno il tre percento dei certificati da lei emessi durante il periodo che inizia immediatamente dopo che è stato preso il campione di auto-verifica precedente preso.

Prima di autorizzare un cliente all'utilizzo del servizio Protect and Sign (Firma personale), utilizzando un OID certificato (1.3.6.1.4.1.22234.2.8.3.7, 1.3.6.1.4.1.22234.2.8.3.20 e 1.3.6.1.4.1.22234.2.8.3.9), la PMA verifica le procedure RA e la gestione RA definiti dal cliente, per poter essere sicura che queste siano coerenti con i requisiti definiti nella PC. Se le procedure RA soddisfano i requisiti CP, la PMA autorizza il cliente a utilizzare il servizio Protect and Sign (Firma personale) con la sua RA.

In aggiunta a questo, la PMA incarica un verificatore esterno di constatare la conformità della CA con i requisiti ETSI per gli OID 1.3.6.1.4.1.22234.2.8.3.7, 1.3.6.1.4.1.22234.2.8.3.20 e 1.3.6.1.4.1.22234.2.8.3.9, ogni anno da un verificatore esterno.

Quando un cliente vuole utilizzare il servizio Protect and Sign (firma personale) con un OID certificato (1.3.6.1.4.1.22234.2.8.3.7, 1.3.6.1.4.1.22234.2.8.3.20 e 1.3.6.1.4.1.22234.2.8.3.9), il cliente (come RA) deve essere verificato da un verificatore esterno, scelto dalla PMA, per poter constatare la sua conformità con presente CP e i requisiti ETSI conformemente all'OID scelto. Altrimenti, il cliente non può rivendicare che il certificato sottoscrittori è conforme al certificato OID. Il programma di verifica è pianificato conformemente a seguenti punti, con una verifica all'anno per la RA:

– La prima verifica viene realizzata da una verifica esterna.

– Il primo anno dopo la verifica iniziale, la verifica viene realizzata conformemente al programma di verifica della DOCUSIGN FRANCE.

– Il secondo anno dopo la verifica iniziale, la verifica viene realizzata conformemente al programma di verifica della DOCUSIGN FRANCE.

– Il terzo anno dopo la verifica iniziale, la verifica viene realizzata da un verificatore esterno.

Nel caso in cui durante la verifica interna eseguita dalla DOCUSIGN FRANCE dovessero essere scoperti dei rilevamenti più importanti, la RA deve sistemarli e una verifica verrà condotta durante lo stesso anno, per poter controllare i rilevamenti.

8.2 Identità/qualifiche del valutatore

I verificatori dell'osservanza devono dimostrare la loro competenza nel campo della verifica dell'osservanza e devono avere famigliarità con i requisiti di presente CP. I verificatori dell'osservanza devono eseguire queste verifiche dell'osservanza come primaria responsabilità. La PMA deve rivedere con attenzione i metodi utilizzati per verificare le componenti PKI per la sua base dei requisiti di verifica. La PMA è responsabile di scegliere il verificatore per le sue proprie componenti PKI. In aggiunta, la PMA deve approvare i verificatori selezionati.

Il verificatore dell'osservanza è una ditta privata che è indipendente dall'entità che viene verificata, o è sufficientemente separata dal punto di vista organizzativo da tale entità da fornire una valutazione imparziale e indipendente.

La PMA appura se un verificatore dell'osservanza soddisfa questi requisiti per poter verificare la CA e la RA.

8.3 Argomenti coperti dalla valutazione

Lo scopo della verifica dell'osservanza deve essere di verificare che un componente operi in accordo con presente CP e la corrispondente CPS.

Per la CA, il perimetro di verifica è il rapporto contrattuale della OA, della CA e del cliente, e il controllo della RA fatto dalla PMA.

Per la RA, il perimetro di verifica è:

– La protezione conformemente a presente CP, KWS CP e documento PSMP, l'utilizzo e la gestione delle coppie di chiavi KWS utilizzate per proteggere la comunicazione con la CA.

– La protezione conformemente a presente CP, KWS CP e documento PSMP, l'utilizzo e la gestione del software cliente Protect and Sign (Firma personale) fornito dalla DocuSign France.

– La creazione della richiesta tecnica di certificato.

– La documentazione della RA rispetto ai requisiti fissati in presente CP.

– Le "procedure RA" definite dal cliente per identificare, autenticare e gestire la richiesta di certificato alla CA.

– Il protocollo di approvazione RA e l'attuazione della "WYSWSY" per informazioni da fissare nel certificato come definiti nella sezione 4.3 in alto.

– La protezione e la gestione dei dati personali dei sottoscrittori.

8.4 Azioni intraprese come risultato del deficit

La PMA può constatare che le componenti PKI non soddisfino gli obblighi fissati in presente CP. Nel caso di non-osservanza, la PMA può sospendere l'operazione della componente PKI non osservante, o può decidere di interrompere i rapporti con la componente PKI interessata, o decidere che debbano essere intraprese delle altre azioni correttive.

Se il verificatore dell'osservanza trova una discrepanza con i requisiti di presente CP, è necessario eseguire seguenti azioni:

– Il verificatore dell'osservanza nota la discrepanza.

– Il verificatore dell'osservanza notifica l'entità della discrepanza. Il verificatore e l'entità deve informare la PMA immediatamente.

– La parte responsabile della correzione della discrepanza appura quali ulteriori notifiche o azioni sono necessarie ai sensi dei requisiti di presente CP, e poi procede nell'eseguire tali notifiche e nell'intraprendere tali azioni senza indugio, in relazione all'approvazione della PMA.

A seconda della natura e della serietà della discrepanza, e di quanto velocemente può essere corretta, la PMA può decidere di arrestare temporaneamente l'operazione di una componente PKI (di norma, terminare temporaneamente o definitivamente un rapporto con un cliente), di revocare un certificato emesso dalla componente PKI o intraprendere altre azioni che reputa appropriate. In base al risultato della verifica, la PMA può decidere di revocare la CA.

8.5 Comunicazione dei risultati

Un report sulla verifica dell'osservanza, che comprende l'identificazione dei provvedimenti correttivi intrapresi o intrapresi dalla componente, viene fornito alla PMA e alle persone competenti nell'entità. Il report identifica le versioni della CP e della CPS e qualsiasi altro criterio di verifica utilizzati come base per la valutazione.

Il report di verifica dell'osservanza non è disponibile su internet per gli utilizzatori. Ciononostante, può essere fornito a un tribunale o a qualsiasi istituzione ufficiale in base a una richiesta legale. In aggiunta, deve essere disponibile, in parte o in toto, all'entità verificata, conformemente alla decisione della PMA.

9 ALTRE ATTIVITÀ E QUESTIONI LEGALI

9.1 Contributi

9.1.1 Contributi per il rilascio del certificato o il rinnovo

Questi servizi vengono definiti nel contratto stipulato tra la DOCUSIGN FRANCE e il cliente.

9.1.2 Contributi per l'accesso al certificato

Nessun contributo.

9.1.3 Contributi per la revoca o l'accesso alle informazioni sullo stato

Non applicabile.

9.1.4 Contributi per altri servizi

Questi servizi vengono definiti nel contratto stipulato tra la DOCUSIGN FRANCE e il cliente.

9.1.5 Politica di rimborso

Questi servizi vengono definiti nel contratto stipulato tra la DOCUSIGN FRANCE e il cliente.

9.1.6 Lista multe

Questi servizi vengono definiti nel contratto stipulato tra la DOCUSIGN FRANCE e il cliente.

9.2 Responsabilità finanziaria

9.2.1 Copertura assicurativa

La DOCUSIGN FRANCE mantiene dei livelli ragionevoli di copertura assicurativa.

9.2.2 Altro patrimonio

La DOCUSIGN FRANCE ha sufficienti risorse finanziarie per mantenere le operazioni e per eseguire i servizi della PKI.

9.2.3 Copertura assicurativa o copertura da garanzia per sottoscrittori

Se risulta un danno a un cliente a causa di un errore della DOCUSIGN FRANCE, la DOCUSIGN FRANCE attiva la sua assicurazione per coprire una parte del danno arrecato al cliente, nei limiti indicati negli accordi contrattuali tra la DOCUSIGN FRANCE e il cliente.

9.3 Segretezza delle informazioni commerciali

9.3.1 Scopo delle informazioni riservate

PMA garantisce un trattamento speciale per seguenti informazioni riservate:

- documentazioni e archiviazioni di OA.
- dati di identità personale.
- chiavi private Sub-CA.
- chiave privata sottoscrittori.
- richiesta di certificato sottoscrittori.
- dati di attivazione Sub-CA.

- report e risultati verifica.
- piano di continuità aziendale.
- contratto e accordo con il cliente.
- Policy di sicurezza del dispositivo interno.
- Dati di attivazione.
- CPS.

Il trattamento delle informazioni aziendali confidenziali fornite dalla RA e dal cliente nel contesto di presentazione di una richiesta di certificato per i sottoscrittori, viene inserito in accordo con le condizioni del contratto stipulato tra il cliente applicabile e la DOCUSIGN FRANCE.

Ogni RA e cliente deve mantenere la riservatezza delle informazioni aziendali confidenziali chiaramente marcate o etichettate come confidenziali o che devono essere intese ragionevolmente come confidenziali, vista la loro natura, e deve trattare tali informazioni con lo stesso livello di attenzione e sicurezza come la CA tratta le proprie informazioni più riservate.

9.3.2 Informazioni non incluse nello scopo delle informazioni riservate

Tutte le informazioni pubblicate da il PS (CP e certificati CA) vengono considerate come non confidenziali.

9.3.3 Responsabilità di protezione delle informazioni riservate

Le componenti PKI devono essere responsabili della protezione delle informazioni riservate che possiedono, in accordo con le leggi applicabili e ai contratti esistenti. Le componenti PKI non devono divulgare le informazioni dei certificati o relative ai certificati a nessuna terza parte a meno che ciò non sia stato autorizzato da presente policy, richiesto per legge, da una normativa o da un regolamento governativo o da una disposizione di un tribunale con giurisdizione competente.

9.4 Privacy delle informazioni personali

9.4.1 Piano privacy

Per scopi dei servizi riferiti alla PKI, le componenti PKI possono raccogliere, conservare o lavorare le informazioni identificabili come personali. Qualsiasi utilizzo o divulgazione del genere deve avvenire in accordo con le leggi e le normative applicabili, in particolare con il European Data Protection Act (legge sulla protezione dei dati personali) e la presente policy di certificazione.

La DocuSign France tratta i dati personali dei sottoscrittori in accordo con le leggi e le normative applicabili, in particolare con il European Data Protection Act (legge sulla protezione dei dati personali) e la presente policy di certificazione.

Le entità RA devono sviluppare una policy sulla privacy, conformemente alla legge europea, e stipulare nel contratto tra il cliente e la DOCUSIGN FRANCE come devono proteggere qualsiasi informazione che raccolgono, identificabile come personale.

I sottoscrittori devono dare accesso e la capacità di correggere o modificare le loro informazioni personali o organizzative, in seguito a una richiesta adeguata al cliente, conformemente alla policy del servizio Protect and Sign (Firma personale) e ai regolamenti del cliente. Tali informazioni devono essere fornite solo dopo che sono stati presi i provvedimenti adeguati per autenticare l'identità della parte richiedente.

Se delle informazioni personali o organizzative dei sottoscrittori devono essere modificate, ciò deve essere fatto prima di generare il certificato. Una volta generato il certificato sottoscrittori, non è possibile per i sottoscrittori richiedere una modifica e la cancellazione della documentazione RA e CA che riguarda i suoi dati personali privati. Il cliente è il solo punto di contatto per il sottoscrittore ad avere accesso ai suoi dati personali, conformemente ai termini e alle condizioni del cliente.

9.4.2 Informazioni trattate come private

Le informazioni del sottoscrittore devono essere trattate come private, così come qualsiasi informazione protetta ai sensi della legge nazionale della Sub-CA e della RA.

9.4.3 Informazioni non ritenute private

Qualsiasi informazione contenuta in un certificato è un'informazione intrinsecamente pubblica e non deve essere considerata una informazione riservata.

9.4.4 Responsabilità di protezione delle informazioni private

La PMA, la OA e la componente PKI ha la responsabilità di proteggere le informazioni private e deve astenersi dalla divulgazione di esse, a meno che non sia stato incaricato dalla Sub-CA e dalla RA ai sensi dell'applicazione della legge.

9.4.5 Notifica e consenso di utilizzazione delle informazioni private

Tutte le informazioni private provenienti da una componente PKI non possono essere utilizzate senza un consenso esplicito del sottoscrittore (vedi sezione 4.1) e del PMC al trattamento dedicato.

9.4.6 Divulgazione in forza di un processo giudiziario o amministrativo

La Sub-CA è conforme alla sua legge nazionale ed ha delle procedure sicure per concedere l'accesso ai dati privati.

La RA è conforme alla sua legge nazionale ed ha delle procedure sicure per concedere l'accesso ai dati privati.

9.4.7 Altre circostanze di divulgazione di informazioni

La PMA ottiene il consenso dalle componenti PKI al trasferimento dei loro dati privati in caso del trasferimenti di una attività come descritto nella sezione 5.8.

9.5 Diritti di proprietà intellettuale

La PMA deve mantenere la proprietà intellettuale dei certificati CA che pubblica. Presente CP deve essere di proprietà della PMA. Qualsiasi marchio di servizio, marchio di fabbrica o nome commerciale contenuto in un certificato o in una domanda di certificato deve rimanere di proprietà del suo proprietario. La coppia di chiavi Sub-CA e il corrispondente certificato devono essere di proprietà della PMA.

9.6 Dichiarazioni e garanzie

9.6.1 Dichiarazioni e garanzie PMA

La PMA definisce la presente CP e la corrispondente CPS. La PMA stabilisce che le componenti PKI sono conformi a presente CP. I processi, le procedure e il quadro della verifica utilizzati per appurare l'osservanza sono documentati nella CPS.

La PMA assicura che tutti i requisiti di una componente PKI, come dettagliati nella presente CP e nella corrispondente CPS, sono attuati come applicabili per consegnare e gestire i servizi di certificazione.

La PMA ha la responsabilità di osservanza delle procedure prescritte in presente CP, anche quando la componente PKI è presa in incarico nella sua funzione da sub-appaltatori. Le componenti PKI forniscono tutti i loro servizi di certificazione in coerenza con la loro CPS.

La PMA ha la responsabilità di verificare la RA e di approvare le procedure della RA prima di concedere al cliente (RA) di utilizzare il servizio Protect and Sign (Firma personale) con uno degli OID referenziati nella sezione 1.2 in alto.

9.6.2 Dichiarazioni e garanzie Sub-CA

La Sub-CA è responsabile di:

- Proteggere e garantire l'integrità e la riservatezza dei suoi dati di attivazione e/o della chiave privata.
- Utilizzare da sola la propria chiave privata e il certificato, con strumenti associati specificati nella CPS, per lo scopo per cui sono stati generati.
- Rispettare e operare le sessioni della CPS che riguardano i loro compiti (questa parte della CPS deve essere trasmessa alla corrispondente componente).
- Consentire al team di verificatori di controllare e verificare l'osservanza della presente CP e delle componenti CP/CPS, e comunicare loro le informazioni richieste, in accordo con le intenzioni della PMA.
- Documentare le loro procedure interne per completare la CPS globale.
- Utilizzare ogni mezzo (tecnico e umano) necessario per raggiungere la realizzazione della CP/CPS che ha attuato e per i quali è responsabile.
- Se la chiave privata del sottoscrittore è andata persa, è stata rubata, potenzialmente compromessa a causa di una compromissione dei dati di attivazione o per un'altra ragione, informare il cliente.
- Deve eseguire una valutazione del rischio per valutare i rischi commerciali e appurare i requisiti di sicurezza necessari e le procedure operative. L'analisi del rischio deve essere revisionata regolarmente e, se necessario, rivista.
- Deve attuare e definire la CP e la CPS conformemente ai principi impostati nella policy di sicurezza della DOCUSIGN FRANCE.

9.6.3 Dichiarazioni e garanzie RA

La RA è responsabile di:

- Per OID 1.3.6.1.4.1.22234.2.8.3.7 e 1.3.6.1.4.1.22234.2.8.3.20: Assicurare che i sottoscrittori siano identificati e autenticati adeguatamente, e che la richiesta di certificato dei sottoscrittori sia accurata e autorizzata correttamente.
- Per OID 1.3.6.1.4.1.22234.2.8.3.9: Assicurare che la prova dell'identificazione dei sottoscrittori e dei soggetti, oltre all'accuratezza dei loro nomi e dei dati associati siano esaminati correttamente come parte del servizio definito o, dove applicabile, siano conclusi tramite presa in esame dell'attestazione da parte di una fonte appropriata e autorizzata, e che le richieste di certificati siano accurate, autorizzate e complete, conformemente alla prova raccolta o all'attestazione.
- Prima di stipulare un rapporto contrattuale con un sottoscrittore, la RA deve informare il sottoscrittore dei termini e delle condizioni relativi all'utilizzo del certificato. La RA deve comunicare queste informazioni tramite un mezzo durevole (per es. con un'integrità che perdura nel tempo) di comunicazione, che possano essere trasmesse elettronicamente e in un linguaggio subito comprensibile.
- Presentare delle informazioni accurate e complete alla CA nella richiesta di certificato, conformemente al documento della PSMP.

- Dare ai sottoscrittori la capacità di vedere le informazioni che verranno inserite nel certificato sottoscrittori per creare la loro identità (vedi sezione 4.3 in alto) durante protocollo di approvazione.
- Concedere al team di verificatori team di verificare e comunicare loro le informazioni richieste, conformemente all'intenzione della PMA, al controllo e alla verifica dell'osservanza della presente CP e dei componenti CPS e delle procedure RA.
- Segnalare alla PMA quando si verifica un incidente nella sicurezza dei servizi CA che sono stati eseguiti dalla OA.
- Rispettare la CP e la corrispondente CPS.
- Proteggere il suo sistema di informazioni e garantire la sicurezza dei dati trasmessi alla PKI.
- Raccogliere e verificare le informazioni dei sottoscrittori per poter create il certificato sottoscrittori.
- Documentare e archiviare
- Autenticare e identificare i sottoscrittori.
- Presentare delle informazioni accurate e complete sul sottoscrittore alla Sub-CA.
- Proteggere le informazioni dei sottoscrittori.
- Esercitare un'attenzione ragionevole per evitare un uso non autorizzato della chiave privata del soggetto.
- Designare e mantenere una lista di tutti gli operatori RA.
- Segnalare al cliente il caso di incidente relativo alla procedura CP e RA.
- Rispettare il contratto stipulato tra il cliente e la DOCUSIGN FRANCE.

9.6.4 Dichiarazioni e garanzie del cliente

Rendere disponibile il documento firmato ai sottoscrittori.

– Esercitare un'attenzione ragionevole per evitare un uso non autorizzato della chiave privata del "Protect and Sign Personal signature".

– Informare il sottoscrittore se la chiave privata del cliente è andata persa, è stata rubata, potenzialmente compromessa a causa di una compromissione dei dati di attivazione o per un'altra ragione.

– Informare il sottoscrittore se la chiave privata del sottoscrittore è andata persa, è stata rubata, potenzialmente compromessa a causa di una compromissione dei dati di attivazione o per un'altra ragione.

– Nel caso in arrivasse l'informazione che la CA che ha emesso il certificato del sottoscrittore è stata compromessa, assicurare che il certificato non sia stato utilizzato dal sottoscrittore o da un utilizzatore del certificato.

– Stipula il contratto con l'entità RA e OA quando sono entità legali diverse da essa con una identificazione chiara dei servizi della PKI avviata dall'entità e tutti gli obblighi RA e OA e le garanzie, conformemente ai servizi della PKI gestiti.

– Definisce la procedura RA e la procedura di gestione RA.

– Seleziona il livello OID da presente CP.

– Segnala alla PMA il verificarsi di un incidente causato dalla RA.

– Seleziona e definisce il protocollo di approvazione.

– Rispetta la CP e la corrispondente CPS.

– Protegge il suo sistema di informazioni e garantisce la sicurezza dei dati trasmessi alla PKI.

– Concede al team di verificatori team di verificare e comunicare loro le informazioni richieste, conformemente all'intenzione della PMA, al controllo e alla verifica dell'osservanza della presente CP e dei componenti CPS, il contratto tra la DOCUSIGN FRANCE e il cliente, la procedura RA e PSMP.

9.6.5 Dichiarazioni e garanzie OA

L'OA è responsabile di:

- Rispettare la sua policy di sicurezza.

- Proteggere e garantire l'integrità e la riservatezza dei suoi dati segreti e/o della chiave privata.

- Consentire al team di verificatori di controllare e verificare l'osservanza della presente CP / criteri di verifica e i componenti della CPS oltre alla policy di sicurezza OA, e comunicare loro qualsiasi informazione utile, in accordo con le intenzioni della PMA.

- Segnalare alla PMA quando si verifica un incidente nella sicurezza dei servizi PKI che sono stati eseguiti dalla OA.

- Rispettare e operare le sessioni della CPS che riguardano i loro compiti (questa parte della CPS deve essere trasmessa alla corrispondente componente).

- Proteggere i token di identità e i dati di attivazione associati.

- Proteggere e garantire l'integrità e la riservatezza dei suoi dati segreti e/o della chiave privata.

- Documentare le loro procedure interne per completare la CPS globale e la sua policy di sicurezza.

- Rispettare gli accordi, in parte o in toto, che la vincolano alla PMA e al cliente.

9.6.6 Sottoscrittori

La persona fisica è responsabile di:

- Rappresentare accuratamente se stessa in tutte le comunicazioni con la RA.

- Utilizzare i dati di attivazione solo tramite l'applicazione del cliente, conformemente al servizio Protect and Sign (Firma personale) e al protocollo di approvazione.

- Quando vengono utilizzati, proteggere i dati di attivazione in qualsiasi momento e impedirne l'accesso non autorizzato, in accordo con presente policy, come stipulato nei loro accordi con i sottoscrittori.

- Tollerare tutti i termini, le condizioni e le restrizioni imposti per l'utilizzo dei loro certificati, come fissato in presente CP e nell'accordo con il sottoscrittore.

- Utilizzare i certificati forniti dalla Sub-CA solo per scopi autorizzati e legali, in accordo con l'entità CP.

- Interrompere l'utilizzo dei certificati emessi, se diventano invalidi, e rimuoverli da tutte le applicazioni su cui sono stati installati.

9.6.7 Dichiarazioni e garanzie di altri partecipanti

9.6.7.1 Dichiarazioni e garanzie dell'utilizzatore del certificato

Qualsiasi utilizzatore del certificato è responsabile di validare un certificato digitale utilizzando:

- Accettare l'utilizzo del certificato solo per scopi indicati nelle estensioni keyUsage del certificato.
- Verificare la validità del certificato, utilizzando le procedure descritte nella [RFC5280], prima di fare qualsiasi affidamento al detto certificato.
- Verificare il OID contenuto in ogni certificato del percorso di certificazione sicura, per poter essere sicuro di accettare il certificato giusto.
- Istituire la fiducia nella Sub-CA che ha emesso il certificato con i metodi descritti in un altro punto di presente CP, e utilizzando l'algoritmo di validazione del percorso descritto in [RFC5280].
- Preservare i dati firmati in originale, le applicazioni necessarie per leggere e lavorare quei dati e le applicazioni crittografate necessarie per verificare le firme digitali su quei dati per tutto l'arco della durata in cui è necessario poter verificare detta firma.
- Interrompere l'utilizzo dei certificati emessi (sottoscrittori, Sub-CA ...), se diventano invalidi, e rimuoverli da tutte le applicazioni su cui sono stati installati.

9.7 Esclusione di garanzia

Le PMA garantisce tramite i servizi della PKI:

- L'identificazione e l'autenticazione della Sub-CA, con il certificato Sub-CA generato dalla ICA.
- La gestione dei certificati corrispondenti e delle informazioni sullo stato del certificato riguardo al presente CP.
- Il contenuto del certificato sottoscrittori conformemente alle informazioni trasmesse da RA riguardo ai sottoscrittori.
- La coppia di chiavi sottoscrittori viene utilizzata solo dal sottoscrittore, conformemente a un protocollo di approvazione scelto dal cliente e ai dati di attivazione richiesti dal sottoscrittore.

Le RA garantisce tramite i servizi della PKI:

- L'identificazione e l'autenticazione dei sottoscrittori, con un certificato sottoscrittori generato dalla Sub-CA applicabile.
- Quando è applicabile, la trasmissione dei dati di attivazione al sottoscrittore corretto.

La PMA non fornisce alcuna garanzia, espressa o implicita, stabilita per legge o altro, e declina qualsiasi responsabilità per il successo o il fallimento dell'utilizzazione della PKI o per la validità legale, l'accettazione o qualsiasi altro tipo di riconoscimento dei suoi certificati diversamente citati in alto. Non possono essere individuate altre garanzie da parte della PMA e dagli utilizzatori nel loro rapporto contrattuale (se esistente).

9.8 Limitazioni di responsabilità

La DOCUSIGN FRANCE non pretende nulla in riferimento all'idoneità o all'autenticità dei certificati emessi in conformità con presente CP. Gli utilizzatori possono solo utilizzare questi certificati a loro rischio. La PMA non si assume alcuna responsabilità in relazione all'utilizzo del certificato o delle in

9.10 Durata e termine

9.10.1 Durata

Presente CP e le versioni successive sono efficaci in seguito all'approvazione della PMA.

9.10.2 Risoluzione

Nel caso in cui i servizi PKI cessano di operare, è necessario che la PMA ne faccia un annuncio pubblico.

In seguito alla risoluzione del service, la PMA archivia immediatamente la sua documentazione, inclusi i certificati emessi, la CP, la CPS e la ARL, conformemente alla sezione 5.8 in alto.

9.10.3 Effetto della risoluzione e mantenimento in vita

La fine della validità della presente CP termina tutti gli obblighi e le responsabilità per la PMA.

La Sub-CA non può continuare a fornire i certificati elettronici riferiti a presente CP.

9.11 Notifiche individuali e comunicazioni con i partecipanti

La PMA fornisce a tutti i partecipanti la nuova versione della CP, tramite PS, appena è stata validata dalla PMA.

9.12 Modifiche

9.12.1 Procedura di modifica

Almeno una volta l'anno, la PMA revisiona la CP e la CPS. A discrezione della PMA, possono essere messe in atto delle revisioni aggiuntive, in qualsiasi momento. Gli errori ortografici o correzioni tipografiche che non modificano il significato della CP sono consentite senza alcuna notifica. Prima di approvare qualsiasi modifica a presente CP, la PMA deve informare i componenti PKI.

Se la PMA desidera raccomandare delle modifiche o delle correzioni alla CP, tali modifiche devono arrivare alle parti interessate identificate dalla PMA. La PMA raccoglie, riassume e propone le modifiche alla CP conformemente con le procedure di approvazione.

9.12.2 Meccanismo di notifica e periodo

La PMA comunica alle componenti PKI la sue intenzioni di modificare la CP/CPS entro e non oltre 2 mesi dall'inizio di un processo di modifica della CP/CPS e conformemente allo scopo della modifica.

9.12.3 Circostanze in cui è necessario modificare il OID

O presenti OID della CP devono essere modificati se la PMA appura che una modifica del CP modifica il livello di fiducia fornito dai requisiti CP o dal materiale CPS.

9.13 Disposizioni per la risoluzione di controversie

Le disposizioni per risolvere le controversie tra la DOCUSIGN FRANCE e i suoi clienti devono essere fissate nel contratto applicabile tra le parti.

9.14 Legge Applicabile

Subordinatamente a qualsiasi limite che appare nella legge applicabile, la legge FRANCESE disciplina l'esecutività, la costruzione, l'interpretazione e la validità della CP, indipendentemente dal contratto o da un'altra scelta di disposizioni legali e senza la pretesa di istituire una qualsivoglia natura commerciale nello Stato della Francia.

Presente disposizione ai sensi della legge applicabile si applica solo alla CP. Il contratto con il cliente che incorpora la CP come riferimento, potrebbe avere delle disposizioni con una propria legge applicabile, premesso che questa sezione 9.14 disciplini l'esecutività, la costruzione, l'interpretazione e la validità delle condizioni della CP, separatamente e a parte dai termini di tale accordo, soggetto a qualsiasi limitazione scaturente dalla legge applicabile.

9.15 Osservanza delle leggi applicabili

La CP è soggetta alle leggi applicabili, ai regolamenti, alle normative, alle ordinanze, ai decreti e agli ordini francesi e europee, inclusi ma non limitato alle restrizioni sull'esportazione o l'importazione del software, hardware, o delle informazioni tecniche e degli argomenti relativi alla privacy e alla firma.

Il cliente e la DOCUSIGN FRANCE concordano di conformarsi alle leggi e alle normative applicabili nel loro contratto.

9.16 Varie disposizioni

9.16.1 Intero accordo

Presente CP costituisce l'intero accordo tra le parti e sostituisce tutti gli altri termini, indipendentemente che siano espressi o impliciti nella legge. Nessuna modifica di presente CP entra in forza o in vigore se non in forma scritta, firmata dal firmatario autorizzato. La mancata applicazione di una o tutte queste sezioni in una particolare istanza o istanze non deve costituire una rinuncia di esse o precludere una successiva applicazione di esse. Tutte le disposizioni in presente CP che per natura esulano dai termini della performance dei servizi, come quelli senza limitazione, tali informazioni confidenziali corrispondenti e i diritti di proprietà intellettuale sopravvivono tali termini, finché non sono completati e verranno applicati a tutti i successori e gli assegnamenti della parte.

9.16.2 Cessione

Eccezion fatta per i punti specificati da altri contratti, solo la PMA può assegnare e delegare presente CP a un'altra parte di sua scelta.

9.16.3 Separabilità

Se si dovesse appurare che una sezione di presente CP non è corretta o non valida, le altre sezioni di presente CP rimangono efficaci finché la CP non è stata aggiornata. Il processo per aggiornare presente CP viene descritto nella sezione 9.12.

9.16.4 Rinuncia ai diritti e all'obbligo

Nessuna rinuncia a qualsiasi violazione o inadempienza o mancanza di esercizio di un qualche diritto ivi contenuto sarà considerata come rinuncia di qualsiasi violazione successiva o inadempienza o rinuncia di

qualsiasi diritto futuro di esercitare un tale diritto. Le intestazioni del CP sono state inserite solamente per comodità e non possono essere utilizzate per interpretare la CP.

9.16.5 Forza maggiore

DOCUSIGN FRANCE non è responsabile per un guasto o un ritardo nella sua prestazione inclusa nella CP, per causa che vanno oltre il suo ragionevole controllo, inclusi, ma non limitati a, un atto di forza maggiore, guerra civile o militare, disastri naturali, incendio, epidemie, inondazioni, terremoti, sommosse, guerre, difetti dell'equipaggiamento, guasto delle linee di telecomunicazione, mancanza di accesso a internet, sabotaggio e azioni governative o qualsiasi altro evento o situazione non prevedibile.

DOCUSIGN FRANCE NON HA ALCUNA RESPONSABILITÀ PER I RITARDI, LA MANCATA CONSEGNA, IL MANCATO PAGAMENTO, LE CONSEGNE ERRATE O L'INTERRUZIONE DEL SERIVZIO CAUSATI DA AZIONI DI UNA TERZA PARTE (TIPO LA RA O IL CLIENTE) O DALL'INFRASTRUTTURA DI INTERNET O DI UN QUALSIASI NETWORK ESTERNA ALLA DOCUSIGN FRANCE.

9.17 Altre disposizioni

9.17.1 Interpretazione

Tutti i riferimenti a "sezioni" in presente CP si riferiscono alle sezione di presente CP. Come vengono utilizzati in questa CP, i pronomi neutri e qualsiasi variazione di essi devono essere considerati come comprensivi del femminile e del maschile, e tutti i termini utilizzati al singolare devono essere considerati come comprensivi del plurale, e viceversa, a seconda di quello che richiede il contesto. I termini "del presente", "in presente" e "ivi contenuto" e altri termini di simile importazione sono riferiti a presente CP come insieme, in quanto essi possono di tanto in tanto essere modificati e completati, e non a una qualsiasi suddivisione di contenuto in presente CP. I termini "include" e "includono", quando vengono utilizzati nella presente non intendono essere esclusivi e significano, rispettivamente, "include, senza limitazione" e "includono, senza limitazione".

9.17.2 Conflitto di disposizioni

Nel caso di un conflitto tra le disposizioni di presente CP, la CPS e qualsiasi accordo dei sottoscrittori, l'ordine di precedenza deve essere CP, CPS e poi l'accordo dei sottoscrittori.

9.17.3 Periodo di limitazione delle azioni

Qualsiasi azione legale che comprende una controversia che è riferita a questa PKI o a uno dei servizi relativi a un certificato emesso da questa PKI deve essere intrapresa prima della fine della data definita nel contratto tra la DOCUSIGN FRANCE e il cliente, il periodo indicato dalla PMA dopo la scadenza del certificato in discussione o la data di disposizione del servizio o dei servizi in discussione che coinvolgono il certificato della PKI, a seconda di ciò che si verifica prima. Se una qualsiasi azione che comprende una controversia relativa a un certificato emesso da questa PKI o da un servizio che comprende certificati emessi da questo certificato della PKI, non è stata iniziata prima di tale tempo, una tale azione sarà considerata prescritta.

9.17.4 Notifica di responsabilità limitata

Presente CP non rivendica di essere costruito per un accordo tra le parti, e non implica alcuna responsabilità da nessuna delle parti.

10 PROFILO CERTIFICATO, CRL, DELTA CRL E OCSP

10.1 Sub-CA

10.1.1 OID: 1.3.6.1.4.1.22234.2.8.3.7, 1.3.6.1.4.1.22234.2.8.3.20 e 1.3.6.1.4.1.22234.2.8.3.9

Certificato base	**Valore**		
Versione	2 (=versione 3)		
Numero di serie	Definito dal software		
Emittente	C = FR O = KEYNECTIS OU = KEYNECTIS per Adobe CN = KEYNECTIS CDS CA		
NonPrimadel	AAAA/MM/GG HH:MM:SS Z (data del rilascio del certificato)		
NonDopoil	2018/10/11 07:00:0 Z (data della fine della vita dell'emittente CA)		
Soggetto	**Tipo caratteristica**	**Valore caratteristica**	**Directory String1**
	C	FR	PrintableString
	O	OPENTRUST	UTF8String
	OU	0002 478217318	UTF8String
	CN	CA firma personale con firma cloud	UTF8String
Informazioni sulla chiave pubblica del soggetto	Generazione chiave (algoritmo e OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Misura chiave	2048	
Firma (algoritmo e OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Estensioni	**Criticità (vero/falso)**	**Valore**
Authority Key Identifier	**FALSO**	
keyIdentifier		9f 22 78 d7 71 1b de 33 b0 7f c9 20 7a a9 a8 e0 4e 62 e3 fb
Subject Key Identifier	**FALSO**	
Metodi per la generazione di un ID della chiave		Definiti dal software (SHA1 160bits della chiave pubblica del soggetto)
Key Usage	**VERO**	
keyCertSign		Set
cRLSign		Set
Extended Key Usage	**FALSO**	
Documenti Acrobat authentiques		1.2.840.113583.1.1.5
Certificate Policies	**FALSO**	
policyIdentifier		Qualsiasi policy
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		
policyIdentifier		1.2.840.113583.1.2.1
policyQualifier-cps		http://www.opentrust.com/PC/

1 DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String o BMPString

Estensioni	**Criticità (vero/falso)**	**Valore**
policyQualifier-unotice		
Basic Constraint	**VERO**	
cA		Vero
pathLenConstraint		0
CRL Distribution Points	**FALSO**	
distributionPoint		http://trustcenter-crl.certificat2.com/Internal/OPENTRUST_CDS_CA.crl

Reasons		n/d
cRLIssuer		n/d

10.2 Sottoscrittori

10.3 Qualifica senza SSCD (OID: 1.3.6.1.4.1.22234.2.8.3.7)

Certificato base	**Valore**		
Versione	2 (=versione 3)		
Numero di serie	Definito dal software		
Emittente	C = FR O = OPENTRUST OU = 0002 478217318 CN = CA firma personale con firma cloud		
NonPrimadel	AAAA/MM/GG HH:MM:SS Z (data del rilascio del certificato)		
NonDopoil	YYYY/MM/DD HH:MM:SS Z (la durata è impostata nel documento di configurazione del cliente e limitata a un massimo si 3 anni)		
Soggetto	**Tipo caratteristica**	**Valore caratteristica**	**Directory String2**
	C	FR	PrintableString
	O	OPENTRUST	UTF8String
	OU	RA *<nome>*	UTF8String
	OU	*<Numero di identificazione transazione>*	UTF8String
	OU	*Identité vérifiée en présence physique de l'Opérateur d'AE*	UTF8String
	OU	*Identità verificata personalmente con RA*	UTF8String
	OU (opzionale)	*<compilato conformemente ai requisiti del cliente>*	UTF8String
	OU (opzionale)	*<compilato conformemente ai requisiti del cliente>*	UTF8String
	CN	*<Nome e cognome del sottoscrittore come >*	UTF8String
Informazioni sulla chiave pubblica del soggetto	Generazione chiave (algoritmo e OID)		rsaEncryption (1.2.840.113549.1.1.1)
	Misura chiave		2048
Firma (algoritmo e OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

[2] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Estensioni	**Criticità (vero/falso)**	**Valore**
Authority Key Identifier	**FALSO**	
keyIdentifier		Definito dall'emittente CA (nel suo Subject Key Identifier)
Subject Key Identifier	**FALSO**	
Metodi per la generazione di un ID della chiave		Definiti dal software (SHA1 160bits della chiave pubblica del soggetto)
Key Usage	**VERO**	
Non disconoscimento		Set
Extended Key Usage	**FALSO**	
Documenti Acrobat authentiques		1.2.840.113583.1.1.5
Certificate Policies	**FALSO**	
policyIdentifier		1.3.6.1.4.1.22234.2.8.3.7
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		Questo certificato è stato emesso in accordo con la CPS Adobe, policy dei certificati OpenTrust e PSGP OpenTrust 1.3.6.1.4.1.22234.2.4.6.1.8
policyIdentifier		1.2.840.113583.1.2.1

policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		Questo certificato è stato emesso anch'esso in accordo con la CPS Adobe.
Basic Constraint	**VERO**	
cA		Falso
pathLenConstraint		N/D
Qualified Certificate Statements	**FALSO**	
Statement 1		Osservanza QC
CRL Distribution Points	**FALSO**	
distributionPoint		http://trustcenter-crl.certificat2.com/public/cloud-signingpersonal-signature-ca.crl
Reasons		n/d
cRLIssuer		n/d
Accesso alle informazioni dell'authority	**FALSO**	
Ocsp		http://ocsp.certificat.com/cloud-signing-personal-signatureca
Nome alternativo soggetto	**FALSO**	**Questa estensione è opzionale**
rfc822Name		**<indirizzo e-mail professionale sottoscrittore>**
Time stamping	**FALSO**	http://tsp.certificat.com/tsa-cds

10.4 Qualifica con SSCD (OID: 1.3.6.1.4.1.22234.2.8.3.20)

Certificato base	**Valore**		
Versione	2 (=versione 3)		
Numero di serie	Definito dal software		
Emittente	C = FR O = OPENTRUST OU = 0002 478217318 CN = CA firma personale con firma cloud		
NonPrimadel	AAAA/MM/GG HH:MM:SS Z (data del rilascio del certificato)		
NonDopoil	YYYY/MM/DD HH:MM:SS Z (la durata è impostata nel documento di configurazione del cliente e limitata a un massimo si 3 anni)		
Soggetto	**Tipo caratteristica**	**Valore caratteristica**	**Directory String2**
	C	FR	PrintableString
	OU	RA *<nome>*	UTF8String
	OU	*<Numero di identificazione transazione>*	UTF8String
	OU	*Identité vérifiée en présence physique de l'Opérateur d'AE*	UTF8String
	OU	*Identità verificata personalmente con RA*	UTF8String
	OU (opzionale)	*<compilato conformemente ai requisiti del cliente>*	UTF8String
	OU (opzionale)	*<compilato conformemente ai requisiti del cliente>*	UTF8String
	CN	*<Nome e cognome del sottoscrittore come >*	UTF8String

Informazioni sulla chiave pubblica del soggetto	Generazione chiave (algoritmo e OID)	rsaEncryption (1.2.840.113549.1.1.1)
	Misura chiave	2048
Firma (algoritmo e OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)	

Estensioni	**Criticità (vero/falso)**	**Valore**
Authority Key Identifier	**FALSO**	
keyIdentifier		Definito dall'emittente CA (nel suo Subject Key Identifier)
Subject Key Identifier	**FALSO**	
Metodi per la generazione di un ID della chiave		Definiti dal software (SHA1 160bits della chiave pubblica del soggetto)
Key Usage	**VERO**	
Non disconoscimento		Set
Extended Key Usage	**FALSO**	
Documenti Acrobat authentiques		1.2.840.113583.1.1.5
Certificate Policies	**FALSO**	
policyIdentifier		1.3.6.1.4.1.22234.2.8.3.20
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		Questo certificato è stato emesso in accordo con la CPS Adobe, policy dei certificati OpenTrust e PSGP OpenTrust 1.3.6.1.4.1.22234.2.4.6.1.15
policyIdentifier		1.2.840.113583.1.2.1
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		Questo certificato è stato emesso anch'esso in accordo con la CPS Adobe.
Basic Constraint	**VERO**	
cA		Falso
Estensioni	**Criticità (vero/falso)**	**Valore**
pathLenConstraint		N/D
Qualified Certificate Statements	**FALSO**	
Statement 1		Osservanza QC
Statement 2		Dispositivo di creazione della firma sicura
CRL Distribution Points	**FALSO**	
distributionPoint		http://trustcenter-crl.certificat2.com/public/cloud-signingpersonal-signature-ca.crl
Reasons		n/d
cRLIssuer		n/d
Accesso alle informazioni dell'authority	**FALSO**	
Ocsp		http://ocsp.certificat.com/cloud-signing-personal-signature-ca
Nome alternativo soggetto	**FALSO**	**Questa estensione è opzionale**
rfc822Name		**<Indirizzo e-mail professionale sottoscrittore>**

Time stamping	**FALSO**	http://tsp.certificat.com/tsa-cds

10.5 Certificato ETSI 102 042 (LCP) (OID: 1.3.6.1.4.1.22234.2.8.3.9)

Certificato base	**Valore**		
Versione	2 (=versione 3)		
Numero di serie	Definito dal software		
Emittente	OU = 0002 478217318 C = FR O = OPENTRUST OU = 0002 478217318 CN = CA firma personale con firma cloud		
NonPrimadel	AAAA/MM/GG HH:MM:SS Z (data del rilascio del certificato)		
NonDopoil	YYYY/MM/DD HH:MM:SS Z (la durata è impostata nel documento di configurazione del cliente e limitata a un massimo si 3 anni)		
OSoggetto	**Tipo caratteristica**	**Valore caratteristica**	**Directory String4**
	C	FR	PrintableString
	O	OPENTRUST	UTF8String
	OU	RA *<nome>*	UTF8String
	OU	*<Numero di identificazione transazione>*	UTF8String
	OU (opzionale)	*<compilato conformemente ai requisiti del cliente>*	UTF8String
	OU (opzionale)	*<compilato conformemente ai requisiti del cliente>*	UTF8String
	OU (opzionale)	*<compilato conformemente ai requisiti del cliente>*	UTF8String
	CN	*<Nome e cognome del sottoscrittore come >*	UTF8String
Informazioni sulla chiave pubblica del soggetto	Generazione chiave (algoritmo e OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Misura chiave	2048	
Firma (algoritmo e OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Estensioni	**Criticità (vero/falso)**	**Valore**
Authority Key Identifier	**FALSO**	
keyIdentifier		Definito dall'emittente CA (nel suo Subject Key Identifier)
Subject Key Identifier	**FALSO**	
Metodi per la generazione di un ID della chiave		Definiti dal software (SHA1 160bits della chiave pubblica del soggetto)
Key Usage	**VERO**	
Firma digitale		Set
Extended Key Usage	**FALSO**	
Documenti Acrobat authentiques		1.2.840.113583.1.1.5
Certificate Policies	**FALSO**	
policyIdentifier		1.3.6.1.4.1.22234.2.8.3.9
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		Questo certificato è stato emesso in accordo con la CPS Adobe, policy dei certificati OpenTrust e PSGP OpenTrust 1.3.6.1.4.1.22234.2.4.6.1.7
policyIdentifier		1.2.840.113583.1.2.1
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		Questo certificato è stato emesso anch'esso in accordo con la CPS Adobe.

Basic Constraint	**VERO**	
cA		Falso
pathLenConstraint		N/D
CRL Distribution Points	**FALSO**	
distributionPoint		http://trustcenter-crl.certificat2.com/public/cloud-signing-personal-signature-ca.crl
Reasons		n/d
cRLIssuer		n/d
Accesso alle informazioni dell'authority	**FALSO**	
Ocsp		http://ocsp.certificat.com/cloud-signing-personal-signature-ca
Nome alternativo soggetto	**FALSO**	**Questa estensione è opzionale**
rfc822Name		**<Indirizzo e-mail professionale sottoscrittore>**
Time stamping	**FALSO**	http://tsp.certificat.com/tsa-cds

10.6 Profilo CRL

10.6.1 CRL per la CA firma personale con firma cloud

Campi CRL	**Valore**		
Versione	V2		
DN emittente	C = FR O = OPENTRUST OU = 0002 478217318 CN = CA firma personale con firma cloud		
QuestoAggiornamento	Data di generazione da parte di CA		
ProssimoAggiornamento	Data di generazione da parte di CA + 7 giorni		
Firma (algoritmo e OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		
Estensione CRL	**Incluso**	**Critico (Vero/Falso)**	**Valore**
NumeroCRL	Sì	Falso	Intero incrementato
AKI	Sì	Falso	Hash chiave emittente
Campi inserimento CRL	**Valore**		
Numero di serie certificato revocato	Numero di serie certificato		
Estensione inserimento CRL	**Incluso**	**Critico (Vero/Falso)**	**Valore**
Motivazione revoca	Opzionale	Falso	[Deve essere revocato con motivazione non specificata]

http://trustcenter-crl.certificat2.com/public/cloud-signing-personal-signature-ca.crl