Policy di Registrazione

Emendamento alla policy dei certificati di DOCUSIGN FRANCE per l'uso della piattaforma QUICKSIGN come servizio di registrazione per identificare i sottoscrittori

QUICKSIGN_Registration_Policy_V2.04

QuickSign, 38 rue du Sentier 75002 Parigi - RCS: Parigi B 450 439 963 Telefono: +33 1 825 20 500 - www.quicksign.com

Versione	2.04	
Stato	Bozza	☒Finale
Autore		VELOCE

Elenco Diffusione	Interno	☒ Esterno
		Pubblico

Storia				
Versione	**Data**	**Autore**	**Commenti**	**Stato**
V.1.0	27/09/2016	MC		Verificato da XR Pubblicato
V.1.99	28/08/2017	FV	Aggiornamento a seguito di periodo di transizione dell'Art51 Versione bozza	In attesa di DocuSign e di Approvazione di verifica
V2.04	12/09/2019	XR	Revisione con CA e approvazione della PMA (12 settembre 2019)	Approvazione
V2.05	02/12/2019	XR	Revisione con la CA dell'autenticazione della richiesta di Revoca.	Approvazione

INDICE

1. INTRODUZIONE

1.1. Panoramica

La Presente policy di registrazione (RP) costituisce una modifica del documento “DBD_Protect and Sign Personal Signature ETSI CP” di DOCUSIGN FRANCE. Essa illustra come il servizio di registrazione online [QUICKSIGN QES ONBOARD ID] gestito da QUICKSIGN soddisfi i requisiti previsti per le Registration Authority (RA) che emettono certificati qualificati con ETSI EN 319 411-2 QCP-n-qscd.

In tale contesto, QUICKSIGN opera come Registration Authority (RA) e utilizza la piattaforma di QUICKSIGN come servizio di registrazione per identificare i Sottoscrittori che richiedono delle firme personali in base a certificati emessi da una Certification Authority (CA).

La presente RP si basa su:

- [CP]: DBD_Protect_and_Sign_Personal_Signature_ETSI_CP_v_1_8.
- [PSMP]: “Proof Signature and Management Policy”, versione 6 minima che definisce il processo tecnico per la firma elettronica e l'interazione con il Cliente.
- RFC 3647 “Certificate Policy and Certification Practices Framework” rilasciato dalla Internet Engineering Task Force (IETF).
- Documenti ETSI:
  - [119 312]: “ETSI TS 119 312 V1.1.1.1 (2014-11): Firme elettroniche e infrastrutture (ESI); Suite crittografiche”;
  - [319 401]: « ETSI EN 319 401 V2.2.1 (2018-04) Firme elettroniche e infrastrutture (ESI), Requisiti di policy generale per i fornitori di servizi fiduciari. »;
  - [319 411]:
    - “ETSI EN 319 411-1 V1.2.2 (2018-04)”: « Firme elettroniche e infrastrutture (ESI), Policy e requisiti di sicurezza per i Fornitori di servizi fiduciari che rilasciano certificati, Parte 1: Requisiti generali »;
    - “ETSI EN 319 411-2 V2.2.2 (2018-04)”: « Firme elettroniche e infrastrutture (ESI); Policy e requisiti di sicurezza per i fornitori di servizi fiduciari che rilasciano certificati; Parte 2: Requisiti per i fornitori di servizi fiduciari che rilasciano certificati qualificati UE ».
- -[ETSI 319 411]:
  - Firme elettroniche e infrastrutture (ESI), Policy e requisiti di sicurezza per i fornitori di servizi fiduciari che rilasciano certificati, Parte 1 : Requisiti generali “
  - Firme elettroniche e infrastrutture (ESI); Policy e requisiti di sicurezza per i fornitori di servizi fiduciari che rilasciano certificati; Parte 2: Requisiti per i fornitori di servizi fiduciari che rilasciano certificati qualificati UE “.

La numerazione di questo documento è in linea con DBD_Protect and Sign Personal Signature ETSI CP.

1.2. Nome documento e identificazione

Nel contesto del presente documento, l'OID della CP di DOCUSIGN FRANCE da considerare è:

- OID = 1.3.6.1.4.1.1.22234.2.8.3.20: Tale profilo è implementato dalla CA ed è già certificato

ETSI (101 456 con SSCD) e da novembre 2018 è stato rilasciato con il nuovo profilo di certificato. Tale OID attuale è sostituito dall'OID di seguito;

- OID = 1.3.6.1.4.1.1.22234.2.14.3.31 : Tale profilo è implementato dalla nuova CA DocuSign France ed è qualificato eIDAS con il nuovo profilo di certificato.

Si noti che la CP per questi due OID è identica, tenendo conto di tali informazioni la migrazione CA OID non avrà alcun impatto sulla Politica di registrazione di Quicksign

1.3. Componenti PKI

1.3.1. Registration Authority (RA)

La RA è di proprietà di, ed è gestita da, QUICKSIGN.

La RA supporta i seguenti servizi della PKI(Public Key Infrastructure- Infrastruttura a chiave pubblica):

- Autenticazione del Sottoscrittore tramite verifica che utilizza il Documento di identità;
- Autenticazione e autorizzazione della Registration Authority delegata (DRA - Delegate Registration Authority);
- Costituzione di un rapporto contrattuale con la DRA che incarica la DRA di adempiere ai suoi obblighi come previsto dalla presente Policy di registrazione;
- Formazione della DRA;
- Collaborazione con la CA nel controllo e nella verifica delle attività gestite dalla DRA;
- Invio della richiesta di Certificato alla CA;
- Autenticazione della revoca e processo di revoca, e in particolare, invio della richiesta di revoca del Certificato alla CA;
- Generazione del percorso log e documentazione delle informazioni di registrazione.

1.3.2. Registration Authority delegata (DRA)

La DRA opera sotto la supervisione e le regole stabilite da QUICKSIGN in qualità di RA.

QUICKSIGN stipula un rapporto contrattuale solo con le DRA che, a causa della natura dei servizi che forniscono, sono obbligate ad assicurare che la loro organizzazione è stata istruita al rispetto dei requisiti legali aggiornati per la verifica del documento di identità e in incontri di persona in conformità con le norme di due diligence per gli istituti che vendono prodotti finanziari, o norme equivalenti.

La DRA è verificata dalla RA o dalla Autorità di gestione della policy (PMA - Policy Management Authority), prima di stipulare un rapporto contrattuale con la RA.

La RA istituisce un elenco di DRA, che comprende il riferimento del contatto, il piano di verifica e le persone di riferimento autorizzate a gestire le richieste di revoca per ogni DRA,

La DRA supporta i seguenti servizi della PKI:

- Identificazione e autenticazione iniziale del Sottoscrittore;
- Se applicabile, aggiornamento del Documento di identità e dei dati di registrazione (e-mail, numero di telefono ...) dopo aver diligentemente verificato che il collegamento tra i dati di registrazione aggiornati e il Sottoscrittore è ancora accurato;
- Se applicabile, autenticazione del Sottoscrittore con un mezzo sicuro di autenticazione con un accesso remoto tramite un portale DRA;
- Invio di una richiesta di Certificato alla RA;
- Invio di una revoca della richiesta di Certificato alla RA;

- Generazione del percorso log e documentazione delle informazioni di registrazione.

Tutte le informazioni scambiate tra la RA e la DRA vengono scambiate in modo sicuro, in conformità con le procedure definite dalla RA nelle sue specifiche tecniche.

Gli obblighi della DRA sono definiti nel contratto tra la RA e la DRA.

1.4. Uso del certificato

L'unico uso del certificato coperto dalla presente RP è quello di verificare la firma elettronica applicata su documenti che usano il servizio di registrazione della QUICKSIGN. QUICKSIGN non è responsabile per un uso diverso.

1.5. Amministrazione della Policy

All'interno della RA, una persona di riferimento è stata assegnata per:

- documentare tutti gli incidenti di sicurezza verificatisi alla CA;
- gestire le modifiche nel presente documento di policy di registrazione in seguito alla convalida della PMA;
- assicurare che le procedure operative relative all'attività della RA siano eseguite in conformità con la presente policy di registrazione.

La persona da contattare è:

M Xavier Roussillon

QUICKSIGN

38, rue du Sentier

75002 PARIS

1.6. Definizioni

Termine	Definizione
Autenticazione	Un processo ove una parte ha presentata una identità e sostiene di essere tale identità, e la seconda parte conferma che tale asserzione di identità è vera.
Certificato	Un certificato è una struttura di dati che è firmata digitalmente da una Certification Authority, e che contiene le seguenti informazioni: • l'identità della Certification Authority che lo emette; • l'identità del Sottoscrittore certificato; • una chiave pubblica che corrisponde a una chiave privata, sotto il controllo del Sottoscrittore certificato; • il periodo operativo; • un numero di serie. • il formato del Certificato in conformità con la raccomandazione ITU-T X.509 versione 3.
Certification Authority	Un'autorità di fiducia di uno o più utenti, per la creazione e l'assegnazione dei Certificati. Più in particolare, nel contesto di questo

	documento, la CA è responsabile di: • emettere i certificati; • definire le regole che vengono applicate all'identificazione e assicurare che vengano rispettate; • assicurare l'affidabilità del servizio di firma digitale a terzi. La CA utilizza una piattaforma di firma CA. Nel contesto di questo documento, la CA è DOCUSIGN FRANCE.
Cliente	Un'entità che usa il servizio di firma CA per poter chiedere ai suoi Sottoscrittori di firmare in modo digitale un documento presentato. Nel contesto di questo documento, il Cliente agisce come Registration Authority delegata.
Registration Authority delegata	Un'entità che è responsabile, nel rispetto delle regolazioni RA ed entro la cornice di un contratto con la RA, di raccogliere i documenti di identificazione dell'utente, controllare l'identità dell'utente, raccogliere i riferimenti di contatto per autenticare l'utente online, autenticare gli utenti online affinché possano aggiornare i loro documenti di identificazione o i riferimenti di contatto, e richiedere la Revoca del certificato, quando necessario.
Documenti di identità	I documenti di identità dell'utente possono essere: • un documento di identità ufficiale (passaporto, carta d'identità); • o uno schema di identificazione elettronica che è stato notificato da uno Stato Membro della Commissione Europea in conformità con l'articolo 9 del regolamento eIDAS (regolamento n. 910/2014); o qualsiasi altro documento di identificazione elettronica che è stato emesso dopo un incontro personale, durante il quale è stato controllato un documento di identità ufficiale.
Certificato qualificato	Un certificato che soddisfi i requisiti elencati nell'articolo 3 e nell'allegato I del regolamento eIDAS.
Autorità di gestione della policy(PMA - Policy Management Authority)	L'entità incaricata della gestione delle componenti e dei servizi PKI. La PMA approva la Policy dei certificati (CP) e la Certification Practice Statement (CPS) utilizzata a supporto dei servizi di certificazione della PKI. La PMA si riserva il diritto di verificare la PKI come indicato nella sezione 8 della presente RP. Nel contesto di questo documento, la PMA è gestita da DOCUSIGN FRANCE.
Registration Authority	Un'entità che è responsabile, sotto il controllo della CA e nell'ambito del contratto con la CA, di identificare e autenticare i soggetti dei Certificati. Opzionalmente, la RA può trasmettere i documenti firmati al Sottoscrittore e archiviare i file di registrazione dell'utente. Nel contesto di questo documento, la RA è gestita da QUICKSIGN.
Revoca	Un processo ove il Periodo operativo del Certificato viene terminato prematuramente. Il Periodo operativo dei Certificati richiesti da QUICKSIGN è definito nella Policy dei certificati CA.

Secure Signature Creation Device (dispositivo di creazione di una firma sicura)	Un dispositivo di creazione di una firma che soddisfa i requisiti esposti nella Direttiva 1999/93/CE della Piattaforma europea e del Consiglio Europeo e riconosciuto dal Regolamento eIDAS nell'articolo 51.
Dispositivi qualificati di creazione di una firma elettronica	A σιγνατυρε χρεατιον δε^ιχε μεεετινγ τηε ρεθυιρεμεντσ ΕΤΣΙ EN 319 411-2 ΘΧΠ -ν-θσχδ
Sottoscrittore	La persona fisica che riceve un Certificato dalla Certification Authority e che usa una chiave privata che viene tenuta in un SSCD, per firmare in modo digitale il documento inviato dal Cliente.
Numero di identi-ficazione della transazione	Un identificatore univoco composto a caso di lettere e di cifre, assegnato a una singola richiesta di identificazione e che garantisce l'unicità del certificato.

2. Responsabilità pubblicazione e archivio

Il presente documento è pubblicato dalla RA sul sito della società: http://www.quick- sign.com/.

Può essere anche pubblicato dall'Autorità di gestione della policy come modifica della policy dei certificati, in accordo con il suo regolamento di pubblicazione.

3. Identificazione e Autenticazione

3.1. Denominazione

La denominazione nei certificati richiesti dalla RA è conforme alla Raccomandazione ITU-T X.509 o IETF RFC 5280 e alla policy dei certificati CA (sezione 10).

3.2. Convalida iniziale dell'identità

3.2.1. Metodo per comprovare il possesso della chiave privata

La prova della proprietà della chiave privata che corrisponde al Certificato del Sottoscrittore utilizzata per firmare, è fornita dalle risorse tecniche e organizzative della Piattaforma di firma CA.

3.2.2 Autenticazione dell'identità dell'organizzazione

Tale parte non è applicabile. La RA accetta le richieste solo dalle persone fisiche che richiedono dei certificati elettronici qualificati inoltrati per loro conto e non per terzi, dove il soggetto corrisponde al Sottoscrittore. Pertanto, il servizio di registrazione RA non comprende il processo di verifica dell'associazione di una persona con una organizzazione o una persona giuridica.

3.2.3 Autenticazione dell'identità della persona fisica

Prima di tutto, la DRA esegue l'Autenticazione dell'identità della persona fisica (Sottoscrittore), rispettando le regolazioni RA e in conformità con i requisiti definiti contrattualmente dalla RA.

La DRA, al momento della registrazione iniziale, verifica 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 della persona fisica viene controllata:

- dalla presenza fisica della persona fisica; o
- in remoto, utilizzando dei mezzi di identificazione elettronici, per i quali è stata assicurata la presenta fisica della persona fisica prima del rilascio del certificato qualificato, e che soddisfano i requisiti fissati nell'articolo 8 del regolamento eIDAS nel rispetto dei livelli di assicurazione “sostanziali” o “elevati”; o
- tramite un certificato di una firma elettronica qualificata o un sigillo elettronico qualificato; o
- utilizzando un altro metodo di identificazione riconosciuto a livello nazionale, che fornisce un'assicurazione equivalente alla presenza fisica, in termini di affidabilità, come da indicazioni dell'articolo 24(1) del regolamento eIDAS. L'assicurazione equivalente viene confermata da un organismo di valutazione della conformità.

Viene fornita la prova di:

- il nome del Sottoscrittore (compreso il cognome e i nomi, in conformità con le pratiche di identificazione nazionale).
- la data e il luogo di nascita, il riferimento a un documento 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.

Se viene fornita la prova di un documento di identità riconosciuto a livello nazionale, la DRA verifica che questo documento sia ancora valido e che sia autentico.

La DRA raccoglie i riferimenti del documento di identità, o, opzionalmente, carica una copia del documento di identità. La DRA raccoglie anche il numero di telefono del sottoscrittore e il suo indirizzo e-mail. La DRA aggiorna le informazioni di registrazione, se sono state modificate.

Se applicabile, la DRA fornisce al sottoscrittore un mezzo sicuro di autenticazione, gestito in modo sicuro dalla DRA, in conformità con le regole di sicurezza bancarie, associato in modo sicuro con il sottoscrittore e considerato come controllato dal sottoscrittore

La DRA documenta le informazioni di registrazione per almeno 7 anni dopo la scadenza del certificato.

3.2.4 Convalida dell'autorità

Tale parte non è applicabile. La RA accetta gli ordini solo dalle persone che richiedono dei certificati elettronici qualificati inoltrati per loro conto e non per terzi. Pertanto, il servizio di registrazione RA non comprende il processo di verifica dell'associazione di una persona con una organizzazione o una persona giuridica.

3.2.5 Informazioni sui sottoscrittori non verificati

Come descritto precedentemente, tutti i dettagli personali e le informazioni da conservare nei certificati sono verificati dalla DRA prima che la RA invii qualsiasi informazione alla CA. Non esistono informazioni non verificate utilizzate dalla RA per compilare il certificato.

3.2.6 Criteri per l'interoperabilità

I certificati consegnati dai componenti della PKI sono gestiti secondo le regole e i requisiti dichiarati dalla CA e dal Cliente in conformità ai requisiti di Adobe e ETSI 319-411.

3.3. Identificazione e autenticazione per le richieste di ricreare le chiavi

Nel caso di una richiesta di ricreare le chiavi, i dati di registrazione del Sottoscrittore vengono aggiornati in conformità con la procedura descritta nel paragrafo 3.2 della Certification Practices Statement della RA.

3.4. Identificazione e autenticazione per le richieste di revoca

L'Autenticazione del richiedente viene eseguita dalla RA, seguendo la procedura descritta nella Certification Practices Statement.

4. Requisiti Operativi Per il Ciclo di Vita Del Certificato

4.1. Domanda di certificato

Durante l'autenticazione del Sottoscrittore, la DRA controlla se il documento di identità utilizzato durante la registrazione iniziale è ancora valido. Se il documento di identità non è valido, la DRA richiede al Sottoscrittore di aggiornare le sue informazioni di identificazione. In ogni caso, solo la DRA invia alla RA le informazioni di identità registrate durante la convalida iniziale dell'identità.

In ogni caso, la DRA richiede quindi un certificato. La richiesta viene inviata in modo sicuro alla RA con almeno le seguenti informazioni:

- Almeno un nome di battesimo;
- Almeno un cognome;
- Indirizzo e-mail attuale;
- Numero di cellulare; (se è richiesto l'invio di OTP via SMS)
- Informazioni per l'identificazione del Sottoscrittore:
  - Tipo di documento di identità,
  - Numero del documento di identità
  - Data di scadenza o di emissione del documento di identità;
  - Paese di emissione
  - Data di nascita
  - Una copia del documento di identità ufficiale con le seguenti informazioni leggibili : Tipo di documento di identità, numero del documento di identità, Data di scadenza o di emissione del documento di identità, paese di rilascio, data di nascita
- Identificazione Funzionario della DRA (Nome, Cognome o Numero di identificazione unico)
  Facoltativo: copia del Documento d'identità ufficiale;
- Riferimento della DRA;
- Il documento da firmare.

4.2. Elaborazione della domanda di certificato

La RA controlla inoltre, nell'interfaccia del servizio di registrazione della RA, l'identità del Sottoscrittore, chiedendogli di compilare un modulo fornito dall'interfaccia del servizio di registrazione della RA, con una verifica tecnica del documento di identità. Se la domanda di certificato viene eseguita durante un incontro personale, la DRA garantisce che solo il Sottoscrittore in persona compili questo modulo, con i mezzi tecnici che stanno solo sotto il suo esclusivo controllo.

Tali informazioni vengono raccolte in modo sicuro dalla RA, conformemente alle sue procedure e alla sua interfaccia. La RA controlla la coerenza tra le informazioni inserite dal Sottoscrittore nell'interfaccia della RA, da un lato, e le informazioni del documento di identità inviate dal sistema informatico DRA, dall'altro.

Se questo controllo non può essere eseguito dalla RA, il servizio di registrazione della RA non invia alcuna richiesta di Certificato alla CA e rigetta la domanda fatta dal Sottoscrittore.

Una volta completato il processo di registrazione, e il Sottoscrittore ha accettato i termini e le condizioni del servizio, la RA richiama la piattaforma di firma CA per inoltrare una richiesta di Certificato, trasmettendo almeno le seguenti informazioni:

- Nome (tutti);
- Cognome;
- Indirizzo e-mail attuale;
- Numero di cellulare; (se è richiesto l'invio di OTP via SMS)

Al termine del processo, la RA richiama la piattaforma di firma della CA per sigillare il File di prova trasmettendo almeno le informazioni di richiesta del certificato DRA (rif. §4.1.). Domanda di Certificato).

Tali informazioni vengono scambiate in modo sicuro.

4.3. Rilascio del certificato

La CA autentica la RA.

La CA gestisce il Protocollo di Consenso con il Sottoscrittore per poter raccogliere il suo consenso alla firma del Documento e l'Accordo del Sottoscrittore.

La CA autentica il Sottoscrittore utilizzando un codice OTP inviato dalla CA al Sottoscrittore tramite SMS su un numero di cellulare trasmesso dalla RA.

La CA emette i certificati in modo sicuro, per conservarne l'autenticità.

La CA firma il documento con la chiave privata del sottoscrittore e cancella la chiave privata del sottoscrittore.

La CA mette a disposizione della RA il Certificato contenuto nel documento firmato (contenuto nel file di prova).

La RA raccoglie il File di prova dalla CA.

4.4. Accettazione del certificato

I termini e le condizioni (Accordo con il sottoscrittore) del servizio offerto dalla CA e dalla RA indicano cosa costituisce l'accettazione del Certificato. Prima di stipulare un rapporto contrattuale con un Sottoscrittore, la RA informa il Sottoscrittore dei termini e delle condizioni del servizio relativo all'uso del Certificato. Tali termini e condizioni citano almeno:

- La policy dei certificati qualificata applicabile;
- Le limitazioni dell'uso del servizio;
- Gli obblighi del Sottoscrittore;
- I termini di revoca del certificato;
- Le condizioni in cui le informazioni di registrazione e i log degli eventi vengono registrati e archiviati;
- Il fatto che il certificato non è pubblicato;

- Le limitazioni della responsabilità;
- Le regole della privacy dei dati.

I termini e le condizioni sono rese disponibili tramite dei mezzi durevoli di comunicazione e firmati dal Sottoscrittore (vedi la sezione 4.3 in alto).

II cognome e il nome del Sottoscrittore vengono citati sulla pagina da firmare come informazioni da validare da parte del Sottoscrittore da includere nel Certificato. Il Sottoscrittore accetta i termini e le condizioni del servizio accettando almeno uno dei riquadri (vedi la sezione 4.3 in alto).

Se il documento di identità era valido per la richiesta di certificato, la RA rende disponibile il Documento firmato con il certificato incorporato al Sottoscrittore e alla DRA.

Se il documento di identità non era valido per la richiesta di certificato, la RA non inoltra il documento firmato con il certificato incorporato al Sottoscrittore e alla DRA. La DRA ha al massimo 5 giorni, successivi all'emissione del certificato, per controllare e verificare il nuovo documento di identità. Se il nuovo documento di identità non è valido, la DRA presenta una richiesta di revoca alla RA. Se il nuovo documento di identità non è stato controllato entro 5 giorni, la RA presenta anche una richiesta di revoca alla CA. In entrambi i casi, il file di prova non è archiviato dalla RA ed è distrutto dalla CA. Se il nuovo documento di identità è valido, la RA rende disponibile il documento firmato con il certificato incorporato al sottoscrittore e alla DRA.

4.5. Coppia di chiavi e uso del certificato

I sottoscrittori devono usare le loro chiavi private per gli scopi indicati nella sezione 1.4 in alto.

4.6. Rinnovo del certificato

Tale parte non è applicabile, in conformità con la Policy dei certificati CA.

4.7. Ricreazione delle chiavi del certificato

La ricreazione delle chiavi del certificato viene eseguita in conformità con le procedure descritte nei paragrafi 4.1. fino a 4.4. Per l'autenticazione del sottoscrittore si applica il paragrafo 3.3.

4.8. Modifica del certificato

Tale parte non è applicabile, in conformità con la Policy dei Certificati CA.

4.9. Revoca e sospensione del certificato

4.9.1. Circostanze per una revoca

Una richiesta di revoca può essere fatta entro 8 giorni dall'emissione del certificato.

4.9.2. Chi può richiedere una revoca

Il sottoscrittore può presentare una richiesta di revoca alla RA, nei seguenti casi:

- le informazioni DN sono compilate in modo errato;
- il certificato corrispondente alla chiave privata è andato perso o è compromesso o si sospetta che lo sia;
- la DRA ha mancato di adempiere ai suoi obblighi e alle norme di sicurezza descritti nella presente RP;

La DRA deve presentare una revoca alla RA, nei seguenti casi:

- le informazioni DN sono compilate in modo errato;
- il Certificato corrispondente alla chiave privata è andato perso o è compromesso o si sospetta che lo sia;
- il documento di identità valido richiesto per adempiere una transazione remota (nel caso in cui il documento di identità che è stato utilizzato per la convalida

dell'identità iniziale avvenuta personalmente non è valido): è stato controllato e non è valido;

La RA deve presentare una revoca alla CA, nei seguenti casi:

- le informazioni DN sono compilate in modo errato;
- il certificato corrispondente alla chiave privata è andato perso o è compromesso o si sospetta che lo sia;
- la DRA ha mancato di adempiere ai suoi obblighi e alle norme di sicurezza descritti nella presente RP.

4.9.3. Procedimento di richiesta della revoca

Se la revoca viene richiesta dal Sottoscrittore, deve indirizzare la richiesta inviando una e-mail all'indirizzo e-mail dedicato della RA. L'indirizzo e-mail e le informazioni da includere nella richiesta di revoca, sono esposte nei termini e condizioni del servizio. L'indirizzo e-mail è disponibile 24 ore su 24. Non esiste un servizio clienti che possa essere contattato telefonicamente.

Per poter autenticare la richiesta di Revoca, il Sottoscrittore deve essere disponibile durante le otto (8) ore lavorative successive alla sua presentazione. Durante questo periodo di otto (8) ore lavorative, sarà contattato dal Funzionario di Revoca della RA al numero di telefono fornito per generare il Certificato designato. Se il Sottoscrittore non risponde al telefono, la richiesta di Revoca è considerata non valida e la RA non procederà con la richiesta di Revoca. Se il Sottoscrittore desidera ancora revocare il suo certificato, deve presentare una nuova richiesta di Revoca dall'inizio.

Dopo che la richiesta di revoca è stata autenticata, la RA segue la procedura descritta nel paragrafo 4.9.3 della Policy dei certificati. Appena la piattaforma di firma CA ha confermato la revoca, la RA informa la DRA e il sottoscrittore tramite e-mail. La revoca viene eseguita entro 24 ore.

Se la revoca viene richiesta dalla DRA, la DRA deve indirizzare la richiesta inviando una e-mail all'indirizzo e-mail dedicato della RA. L'indirizzo e-mail e le informazioni da includere nella richiesta di revoca, sono riportate nel contratto tra la QUICKSIGN e la DRA. L'indirizzo e-mail è disponibile 24 ore su 24. Dopo che la richiesta di revoca è stata autenticata, la RA segue la procedura descritta nel paragrafo 4.9.5 della Policy dei certificati. Appena la piattaforma di firma CA ha confermato la revoca, la RA informa la DRA e il sottoscrittore tramite e-mail. La revoca viene eseguita entro 24 ore.

Se la revoca viene richiesta dalla RA, la RA deve seguire la procedura descritta nel paragrafo 4.9.5 della Policy dei certificati. Appena la piattaforma di firma CA ha confermato la revoca, la RA informa la DRA e il sottoscrittore tramite e-mail. La revoca viene eseguita entro 24 ore.

Le richieste di revoca e le azioni successive sono documentate manualmente dalla RA.

5. Struttura, Gestione e Controlli Operativi

5.1. Controlli fisici

Tutti i controlli fisici, inclusa l'ispezione dei locali e la costruzione delle strutture del centro dati utilizzati per avviare il servizio di registrazione, sono controllati da un revisore tecnico indipendente.

L'accesso fisico agli uffici della RA è ristretto alle sole persone autorizzate. Le persone non autorizzate devono sempre essere accompagnate da personale autorizzato e il loro accesso agli uffici deve essere registrato. L'accesso ai centri dati principali è limitato alle sole persone autorizzate.

I controlli vengono eseguiti per evitare la perdita, il danneggiamento o la compromissione del patrimonio e l'interruzione delle attività aziendali; per evitare la compromissione o il furto delle informazioni e di strutture che elaborano le informazioni; e per prevenire il prelievo non autorizzato dei patrimoni della RA. Tali controlli sono descritti nella valutazione del rischio e nel processo di

gestione, oltre che nel Piano di continuità aziendale.

Viene definito un perimetro di sicurezza protetto per proteggere i componenti critici da intrusioni; l'accesso a tale perimetro di sicurezza è controllato, specialmente con allarmi che rilevano un'intrusione.

5.2. Controlli procedurali

Tutti i ruoli da eseguire nella RA e nella DRA sono ben identificati, in modo da eseguire una separazione dei compiti. Ogni ruolo è descritto e documentato, e ogni persona assegnata a un ruolo è identificata.

La RA e la DRA amministrano l'accesso dell'utente di ogni ruolo. L'amministrazione comprende la gestione dell'account utente e la modifica o la rimozione tempestiva dell'accesso. L'accesso alle informazioni e alle funzioni del sistema di domanda è ristretto, in conformità con la policy di controllo degli accessi. Il personale è identificato e autenticato prima di usare le applicazioni critiche del servizio di registrazione, e è responsabile per le proprie attività tramite il log eventi o il log classico.

5.3. Controlli del personale

Il personale DRA e RA incaricato del processo di iscrizione, che gestisce l'infrastruttura o fornisce supporto ai sottoscrittori è ben qualificato e formato.

Il personale DRA e RA che non lavora seguendo le regole e le procedure stabilite è passibile di sanzioni disciplinari in conformità con il diritto del lavoro francese.

I ruoli e le responsabilità in materia di sicurezza sono documentati nella descrizione delle mansioni e messi a disposizione di tutto il personale interessato. Il personale è consapevole della separazione dei compiti e del minor privilegio, in conformità con la sensibilità della posizione.

Il personale esercita delle procedure e processi amministrativi e di gestione che sono in linea con le procedure di gestione della sicurezza sulle informazioni della RA.

Il personale dirigente possiede l'esperienza o la formazione in materia di sicurezza delle informazioni e della firma.

Il personale che prende decisioni in merito al processo di iscrizione è libero da qualsiasi conflitto di interessi e ha pieno potere decisionale, tranne che in situazioni di crisi.

Il personale è incaricato formalmente dei ruoli di fiducia dal senior management, in conformità con il principio del “minor privilegio”. Il personale ha accesso ai ruoli di fiducia solo dopo aver dimostrato la propria qualifica per il ruolo descritto. Il personale della RA prova la propria affidabilità presentando il proprio casellario giudiziale oltre a delle buone referenze da precedenti datori di lavoro.

5.4. Procedure di logging di verifica

I file di log di verifica vengono generati per tutti gli eventi relativi alla sicurezza e ai servizi della RA e della DRA. Dove possibile, i log di verifica di sicurezza vengono raccolti automaticamente. Lì dove ciò non fosse possibile, è necessario utilizzare un logbook o un altro meccanismo fisico. Tutti i log di sicurezza, sia quelli elettronici che non elettronici, vengono conservati e resi disponibili durante le verifiche di conformità.

La privacy delle informazioni del soggetto è mantenuta.

I log di verifica sono protetti in modo che solo gli utenti autorizzati possano accedervi e/o usarli. I log di verifica vengono registrati in modo tale da non poter essere facilmente cancellati o distrutti (ad eccezione del trasferimento su supporti a lungo termine) entro il periodo di tempo in cui devono essere conservati. I log di verifica sono protetti in modo da rimanere leggibili per tutta la durata del periodo della loro archiviazione. I log di verifica e i riepiloghi di verifica sono sottoposti a backup tramite un meccanismo di backup aziendale.

Una scansione della vulnerabilità degli indirizzi IP pubblici e privati viene eseguita mensilmente.

I log di verifica che forniscono le informazioni sulle attività potenzialmente sospette vengono regolarmente esaminati dall'amministratore di sistema. Se un sistema di sicurezza segnala all'amministratore di sistema un potenziale problema di sicurezza, i log vengono esaminati immediatamente.

5.4.1. Registration Authority

Il logging comprende almeno i seguenti argomenti:

- Accesso fisico alla struttura;
- Gestione dei ruoli di fiducia;
- Accesso logico;
- Gestione del backup;
- Gestione del log;
- Autenticazione e richiesta della revoca;
- Raccolta del file di prova dalla CA;
- Dati di registrazione inviati dalla DRA;
- Gestione dell'informatica e della rete.

5.4.2. Registration Authority delegata

Il logging comprende almeno i seguenti argomenti:

- l'identificazione e l'autenticazione del Sottoscrittore, incluse le informazioni relative al documento di identità del Sottoscrittore, la sua e-mail e il suo numero di telefono;
- le circostanze dell'identificazione e dell'autenticazione del Sottoscrittore;
- la gestione dei mezzidiautenticazione del Sottoscrittore;
- Accesso logico;
- Gestione del backup;
- Gestione dei ruoli di fiducia;
- gestione del log di accesso; in particolare, la DRA deve avere un elenco di tutti gli accessi che sono autorizzati a iscrivere e gestire i sottoscrittori;
- Gestione informatica e della rete.

5.5. Archiviazione della documentazione

5.5.1. Registration Authority

La RA documenta almeno:

- le seguenti informazioni di registrazione:
  - L'identità della DRA;
  - Il metodo utilizzato per validare i documenti di identificazione (per es. incontro personale);
  - Il ruolo di QUICKSIGN in qualità di RA;
  - I log di registrazione;
- l'accettazione del sottoscrittore dei suoi obblighi:

- consentire alla RA e/o alla DRA di tenere una registrazione delle informazioni utilizzate durante la registrazione, qualsiasi caratteristica specifica per il soggetto inserita nel certificato, e la trasmissione di tali informazioni a terzi, alle stesse condizioni previste dalla presente policy, nel caso in cui la RA cessi di fornire i suoi servizi;
- se e a quali condizioni, il Sottoscrittore richiede e il soggetto acconsente alla pubblicazione del Certificato;
- conferma che le informazioni contenute nel certificato siano corrette.

Il documento è archiviato per almeno sette anni dopo la scadenza del certificato.

La riservatezza e l'integrità della documentazione attuale e archiviata relativa ai Certificati qualificati, è mantenuta. La documentazione è archiviata completamente e in modo riservato, in conformità con le pratiche commerciali divulgate; se richiesto, essa deve essere messa a disposizione per fornire la prova della certificazione ai fini di procedimenti legali. In particolare, il sistema di archiviazione e i metodi applicati devono assicurare che:

- Tutti i supporti utilizzati per archiviare la documentazione RA siano protetti da danni e archiviati solamente in aree con accesso ristretto. Il supporto è criptato e necessita di un controllo speciale di accesso per essere letto;
- I supporti siano controllati dal sistema di archiviazione per identificare i supporti che rischiano di essere obsoleti o deteriorati. I supporti identificati devono essere sostituiti dall'amministratore del sistema, assicurandosi che i dati non vadano persi e che non siano stati recuperati dallo specchio del sistema di archiviazione;
- Tutti i supporti utilizzati per archiviare i dettagli personali vengano cancellati e distrutti alla fine della loro durata;
- Nessun mezzo utilizzato nel sistema di archiviazione sia utilizzato o riutilizzato in un altro contesto, a causa del sistema di file criptati utilizzato, che è diverso da quelli utilizzati per archiviare i dati operativi.

5.5.2. Registration Authority delegata

La DRA documenta le seguenti informazioni di registrazione:

- Il tipo di documento presentato dal Sottoscrittore a supporto della registrazione;
- Il numero di identificazione o, se applicabile, copia del documento di identità;
- Il log di registrazione;
- Luogo di conservazione delle copie delle domande e dei documenti di identificazione, compreso l'Accordo firmato con il Sottoscrittore;
- Il metodo utilizzato per validare i documenti di identificazione (per es. incontro personale);

Il documento viene archiviato per almeno sette anni dopo la scadenza del certificato.

La riservatezza e l'integrità della documentazione archiviata relativa ai Certificati qualificati è mantenuta. La documentazione è archiviata in modo completo e riservato, in conformità con le pratiche commerciali divulgate; se richiesto, essa deve essere resa messa a disposizione per fornire la prova della certificazione ai fini di procedimenti legali. In particolare, il sistema di archiviazione e i metodi applicati devono assicurare che:

- Tutti i supporti utilizzati per archiviare la documentazione DRA siano protetti da danni e archiviati solamente in aree con accesso ristretto. Il supporto è criptato e necessita di un controllo speciale di accesso per essere letto;

- I supporti siano controllati dal sistema di archiviazione per identificare i supporti che rischiano di essere obsoleti o deteriorati. I supporti identificati devono essere sostituiti dall'amministratore del sistema, assicurandosi che i dati non vadano persi e che non siano stati recuperati dallo specchio del sistema di archiviazione;
- Tutti i supporti utilizzati per archiviare i dettagli personali vengano cancellati e distrutti alla fine della loro durata;
- Nessun mezzo utilizzato nel sistema di archiviazione sia utilizzato o riutilizzato in un altro contesto, a causa del sistema di file criptati utilizzato, che è diverso da quelli utilizzati per archiviare i dati operativi.

5.6. Passaggio della chiave

Il periodo di validità del Certificato dei Sottoscrittori è definito nella policy dei certificati CA.

5.7. Recupero in caso di compromissione e di disastro

QUICKSIGN ha un piano di continuità aziendale. Esso identifica i rischi e descrive le azioni e le misure per affrontare gli incidenti e gli altri eventi compromettenti.

5.8. Cessazione

5.8.1. Registration Authority

Se QUICKSIGN prevede la cessazione del suo ruolo di Registration Authority per la CA, deve:

- darne notizia alla CA prima della cessazione, in conformità con le procedure concordate nel contratto commerciale,
- inviare una lettera raccomandata alla PMA,
- distruggere tutte le chiavi private utilizzate per rendere sicura la comunicazione con la CA, entro il giorno successivo alla cessazione,
- interrompere la consegna delle richieste di certificato,
- informare i Sottoscrittori e le parti facenti affidamento nel caso in cui sia stato compromesso il suo ruolo di Registration Authority.

La decisione dell'entità alla quale QUICKSIGN deve consegnare la documentazione archiviata deve essere presa dalla CA.

5.8.2. Registration Authority delegata

Se la DRA prevede la cessazione del suo ruolo di Registration Authority Delegata, deve:

- darne notizia alla RA prima della cessazione, in conformità con le procedure concordate nel contratto commerciale,
- inviare una lettera raccomandata alla RA,
- interrompere la consegna delle richieste di certificato,
- informare i sottoscrittori e le parti facenti affidamento nel caso in cui sia stato compromesso il suo ruolo di Registration Authority Delegata.

La decisione dell'entità alla quale la DRA deve consegnare la documentazione archiviata è definita contrattualmente tra la RA e la DRA.

6. Controlli di sicurezza tecnica

6.1. Generazione e installazione di una coppia di chiavi

La CA genera le chiavi in modo sicuro e la chiave privata è segreta. La CA verifica che il dispositivo sia certificato come QSCD qualificato, che soddisfi i requisiti del regolamento eIDAS.

6.2. Protezione delle chiavi private e Tecnica modulo crittografico

La generazione della coppia di chiavi CA è effettuata in conformità con la CP della CA.

6.3. Altri aspetti della Gestione della Coppia di chiavi

Gli altri aspetti della Gestione della coppia di chiavi vengono eseguiti dalla CA, in conformità con la CP della CA.

6.4. Dati di attivazione

Il protocollo di approvazione, che comprende la generazione, l'installazione e la protezione dei dati di attivazione, è eseguito dalla CA in conformità con le sue procedure. In particolare, il Sottoscrittore utilizza un codice OTP generato dalla CA e trasmesso al numero di telefono registrato per il Sottoscrittore.

6.5. Controlli di sicurezza computer

I controlli (per es. firewall) proteggono i domini di rete interni della RA e della DRA dagli accessi non autorizzati. Anche i firewall sono configurati dalla RA e dalla DRA per prevenire tutti i protocolli e accessi non richiesti dalle relative operazioni. La RA e la DRA assicurano che l'accesso al sistema sia limitato a persone debitamente autorizzate.

I dati sensibili sono protetti dall'essere rivelati tramite degli oggetti di archiviazione riutilizzati e accessibili a utenti non autorizzati.

6.6. Controllo di sicurezza del ciclo di vita

La RA e la DRA utilizzano sistemi e prodotti affidabili che sono protetti da modifiche, e assicurano la sicurezza tecnica e l'affidabilità dei processi da essi supportati.

Un'analisi dei requisiti di sicurezza viene eseguita nella fase di progettazione e di specifica dei requisiti di qualsiasi progetto intrapreso dalla RA, in particolare per assicurare che la sicurezza sia integrata nel sistema informatico DRA.

Le procedure di controllo delle modifiche sono applicate alle versioni, alle modifiche e alle correzioni del software d'emergenza, per qualsiasi software operativo e modifiche alla configurazione. Le procedure comprendono la documentazione delle modifiche.

L'integrità dei sistemi e delle informazioni della RA e della DRA è protetta dai virus, da software sospetti e non autorizzati. I danni derivati da incidenti di sicurezza e da malfunzionamenti sono ridotti al minimo grazie all'uso di procedure di segnalazione e di risposta agli incidenti. I supporti utilizzati nella RA e nella DRA sono gestiti in modo sicuro per proteggere i supporti da danni, furti e accessi non autorizzati. Le procedure di gestione dei supporti proteggono contro l'obsolescenza e il deterioramento dei supporti nel periodo di tempo in cui è richiesta la conversazione della documentazione. Sono stabilite e attuate procedure per tutti i ruoli di fiducia e amministrativi che hanno un impatto sulla fornitura di servizi di certificazione.

Le procedure sono specificate e applicate per assicurare che i patch di sicurezza siano applicati entro un periodo ragionevole dal momento in cui sono stati resi disponibili, che i patch di sicurezza non siano applicati se introducono una instabilità che supera i vantaggi derivanti dalla loro applicazione, e che le ragioni della mancata applicazione delle patch di sicurezza siano documentate e scelte dalla RA e dal team DRA.

6.7. Controlli di sicurezza rete

La RA e la DRA mantengono e proteggono tutti i loro sistemi in almeno una zona sicura, e eseguono e configurano una procedura di sicurezza che protegge i sistemi e le comunicazioni tra i livelli del sistema all'interno delle zone sicure.

6.8. Orodatazione

Per mantenere il tempo del sistema vengono utilizzate procedure elettroniche o manuali. Per un

periodo garantito su registrazioni di verifica, la RA si sincronizza regolarmente con un servizio a tempo.

7. Quadro di riferimento per la definizione di altre policy di certificazione basate sul presente documento

La RA non ha altre Policy di Registrazione all'infuori di presente documento.

8. Verifica di Conformità e Altre Valutazioni

8.1. Frequenza o circostanze della valutazione

8.1.1. Registration Authority

Servizio di registrazione dopo la fine del periodo di transizione (art. 51 dell'eIDAS),un revisore esterno esegue una valutazione in conformità con l'ETSI.

Prima di prestare il proprio servizio, la RA è sottoposta a revisione da parte di un revisore esterno a fronte di ETSI 319 411-2 (QCP-n-qscd).

Il primo anno successivo alla verifica esterna, è eseguita una verifica della RA da parte della CA, in conformità con il programma di verifica della Piattaforma di firma CA.

Il secondo anno dopo la verifica esterna, deve essere eseguita una nuova verifica esterna.

Nel caso in cui durante la verifica interna eseguita dalla CA dovessero emergere dei risultati rilevanti, la RA risolverà tali questioni e entro lo stesso anno verrà eseguita una verifica esterna.

8.1.2. Registration Authority Delegata

La RA controlla che la DRA adempia ai suoi impegni e alla presente Policy di registrazione. Un piano di verifica viene definito dalla RA e approvato dalla PMA.

La DRA accetta che la RA o la PMA effettui una verifica di conformità, prima di intraprendere il proprio ruolo di DRA.

La DRA accetta che la RA e la PMA effettuino una verifica ogni qualvolta sia necessario per assicurare la conformità con la presente Policy di registrazione e con la CP.

Se durante una di queste verifiche viene rilevata una grave mancanza di conformità, la Registration Authority Delegata osserverà senza indugio la RP e la CP. Se la questione non viene risolta entro un termine stabilito dal revisore, la RA sospenderà i propri servizi finché non sarà raggiunto una conformità effettiva, alle condizioni previste nel contratto tra la RA e la DRA.

8.2. Argomenti coperti dalla Valutazione

8.2.1. Registration Authority

Il perimetro per una verifica di QUICKSIGN in qualità di Registration Authority è:

- La protezione, l'uso e la gestione delle coppie di chiavi utilizzate per proteggere la comunicazione con la CA;
- La creazione della richiesta tecnica di Certificato;
- La documentazione della RA rispetto ai requisiti stabiliti nella presente CP;
- La procedura di registrazione definita dalla RA per identificare, autenticare e gestire la richiesta di Certificato alla CA.
- La procedura di revoca;
- La gestione dei ruoli di fiducia;
- La gestione dell'informatica e degli incidenti;
- La sicurezza fisica;
- Gestione dei file di prova;

- La protezione e gestione dei dati personali dei sottoscrittori.

8.2.2. Registration Authority delegata

Il perimetro di una verifica della DRA è:

- Il livello dei requisiti per le procedure di registrazione definito dalla RA nel paragrafo 1.3.2, per identificare, autenticare e gestire le domande di Certificato;
- La protezione, l'uso e la gestione dei mezzi utilizzati per proteggere la comunicazione con la RA;
- La gestione del file di prova;
- La gestione dei ruoli di fiducia;
- Il tipo e la gestione dei mezzi di autenticazione sicuri del sottoscrittore;
- La gestione informatica e degli incidenti utilizzata per gestire il Sottoscrittore e il portale DRA;
- La sicurezza fisica;
- La protezione e gestione dei dati personali dei Sottoscrittori.

9. Altre questioni commerciali e legali

9.1. Tariffe

Tali servizi sono definiti nel contratto stipulato tra la RA e la DRA.

9.2. Responsabilità finanziaria

La RA mantiene livelli ragionevoli di copertura assicurativa e sufficienti risorse finanziarie per il mantenimento delle operazioni. La copertura assicurativa o di garanzia è definita nel contratto tra la RA e la DRA.

9.3. Riservatezza delle informazioni commerciali

La RA mantiene la riservatezza delle informazioni aziendali riservate, compresi i dati relativi all'identità personale, la richiesta di certificato del sottoscrittore, i risultati e i rapporti delle verifiche, il piano di continuità aziendale e il contratto con la DRA.

9.4. Privacy delle informazioni personali

9.4.1. Registration Authority

La RA tutela la riservatezza e l'integrità dei dati di registrazione, in conformità con la legge europea applicabile sulla privacy dei dati. L'insieme di regole sulla privacy dei dati della RA è documentato nel suo ISSP. Tali regole sono presentate a ogni Sottoscrittore prima di qualsiasi transazione nei termini e condizioni del servizio, che devono essere approvati dal Sottoscrittore cliccando sul riquadro di spunta.

QUICKSIGN, in qualità di RA, è controllata dalla Autorità di Protezione dei Dati di Parigi (CNIL) e nomina un Responsabile della protezione dei dati. I suoi riferimenti di contatto sono i seguenti:

Xavier Roussillon

QUICKSIGN

38, rue du Sentier

75002 PARIS

9.4.2. Registration Authority delegata

La DRA protegge la riservatezza e l'integrità dei dati di registrazione. Le Regole sulla privacy dei dati della DRA sono documentate e sono conformi alla legge europea applicabile sulla privacy dei dati.

9.5. Diritti di proprietà intellettuale

Tale parte non è applicabile. La PMA mantiene la proprietà intellettuale dei certificati CA che pubblica.

9.6. Dichiarazioni e garanzie

9.6.1. Registration Authority

La RA avvisa la PMA in caso di incidente di sicurezza.

La RA informa il Sottoscrittore in merito ai termini e alle condizioni relative all'uso di un Certificato, prima di presentare una richiesta di Certificato alla CA. Il Sottoscrittore accetta i termini e le condizioni del servizio, cliccando sul riquadro sullo schermo. La RA invia una e-mail al Sottoscrittore contenente i termini e le condizioni del servizio, o, facoltativamente, rende disponibili tali termini sul sito web.

La RA protegge il proprio sistema di informazioni e garantisce la sicurezza dei dati trasmessi alla

PKI.

La RA autentica la DRA e il sottoscrittore.

La RA approva la procedura della DRA e i mezzi di autenticazione sicura utilizzati dalla DRA per l'autenticazione del sottoscrittore, prima di autorizzare una DRA all'uso del servizio. Il metodo utilizzato per autorizzare una DRA è approvato dalla PMA.

La RA instaura un rapporto contrattuale con una DRA che incarica la DRA di adempiere ai suoi obblighi ai sensi della presente policy di registrazione;

La RA si adopera al meglio per garantire che la DRA rispetti i suoi obblighi ai sensi della presente Policy di registrazione, e che lo faccia per l'intero periodo.

La RA collabora con la CA nelle attività di controllo e di verifica svolte sulla DRA;

La RA informa la PMA in merito a tutte le nuove DRA che desiderano utilizzare il servizio e trasmette una sintesi della procedura DRA.

La RA informa il sottoscrittore nel caso in cui la chiave privata del sottoscrittore sia andata smarrita, sia stata rubata o sia potenzialmente compromessa a causa di una compromissione dei dati di attivazione o per altri motivi.

La RA garantisce che nessun Certificato venga utilizzato dal Sottoscrittore o da un utilizzatore, se è stato comunicato dalla CA che il Certificato dell'Abbonato è stato compromesso.

La RA trasmette alla CA solo richieste di revoca autenticate.

La RA sostiene i team di verifica in modo costruttivo e compie ogni ragionevole sforzo necessario per completare una verifica e comunicarne i risultati.

9.6.2. Registration Authority delegata

Gli obblighi della DRA sono definiti contrattualmente tra la RA e la DRA.

La DRA garantisce che ogni Sottoscrittore per il quale è stata presentata una domanda di certificato alla CA tramite la RA, sia stato identificato e autenticato correttamente, e che la richiesta di certificato sia stata eseguita in modo accurato e sia stata debitamente autorizzata. La DRA garantisce che la richiesta di certificato inoltrata contenga esclusivamente informazioni accurate e complete.

La DRA garantisce che la sua organizzazione possiede le competenze, l'affidabilità, l'esperienza e le qualifiche necessarie, e ha ricevuto la formazione adeguata in materia di sicurezza e di norme sulla protezione dei dati personali per l'identificazione e l'autenticazione in conformità con le norme di due diligence per gli istituti che vendono prodotti finanziari, o norme equivalenti.

La DRA protegge il suo sistema di informazioni e garantisce la sicurezza dei dati trasmessi alla RA.

La DRA protegge la riservatezza e l'integrità dei dati di registrazione.

9.7. Esclusione di garanzia

La DRA garantisce la convalida e l'autenticazione iniziale dell'identità del sottoscrittore. La RA garantisce che stipulerà un rapporto contrattuale solo con le DRA che, a causa della natura dei servizi che forniscono, sono obbligate a garantire che la loro organizzazione è stata istruita al rispetto dei requisiti legali aggiornati per la verifica del documento di identità e in incontri di persona in conformità con le norme di due diligence per gli istituti che vendono prodotti finanziari, o norme equivalenti.

La RA garantisce inoltre che si assicurerà della capacità finanziaria della DRA. La RA non fornisce alcuna altra garanzia, espressa o implicita, stabilita per legge o di altro tipo, e declina qualsiasi responsabilità per la convalida iniziale dell'identità e l'autenticazione del Sottoscrittore.

Di conseguenza, a condizione che la DRA abbia adempiuto al suo ruolo come descritto nel presente documento, la RA garantisce l'identificazione e l'autenticazione del sottoscrittore. La RA non fornisce

alcuna garanzia, espressa o implicita, stabilita per legge o di altro tipo, e declina qualsiasi responsabilità per il successo o il fallimento dell'utilizzazione della PKI o per la validità legale o l'accettazione dei certificati CA.

9.8. Limitazioni di responsabilità

La RA non avanza alcuna pretesa in merito all'idoneità o all'autenticità dei certificati emessi in conformità con la presente RP. Le parti facenti affidamento possono solo utilizzare tali Certificati a loro rischio. La RA non si assume alcuna responsabilità in relazione ad un uso del Certificato che sia diverso da quello descritto nel presente documento.

La DRA risponde dell'esattezza di tutte le informazioni di registrazione, nel rispetto delle condizioni del contratto tra la RA e la DRA. La RA non è responsabile per eventuali ritardi, mancate consegne, mancati pagamenti, consegne errate o interruzioni del servizio causati da terzi, inclusa la DRA..

9.9. Indennità

La RA non avanza alcuna pretesa in merito all'idoneità o all'autenticità dei Certificati rilasciati ai sensi della presente RP. Non vi è alcun obbligo di effettuare pagamenti relativi ai costi associati al malfunzionamento o all'uso improprio dei dati personali che vengono verificati per una richiesta di Certificato.

9.10. Durata e cessazione

La RP e le versioni successive sono efficaci previa approvazione della PMA.

In caso di cessazione dell'attività della RA, la RA deve seguire la procedura descritta nel paragrafo 5.8. del presente documento.

9.11. Avvisi individuali e comunicazioni con i partecipanti

QUICKSIGN, in qualità di Registration Authority, fornisce una nuova versione della presente policy di registrazione attraverso il suo sito web.

9.12. Modifiche

La RA rivede il presente documento e la sua certification practices statement almeno una volta l'anno. A discrezione della RA, possono essere messe in atto delle revisioni aggiuntive, in qualsiasi momento. Qualsiasi modifica viene approvata dalla PMA.

9.13. Disposizioni per la risoluzione di controversie

Le disposizioni per la risoluzione delle controversie tra la RA e la DRA sono stabilite nel contratto applicabile tra le parti.

9.14. Legge Applicabile

Fatte salve le limitazioni previste dalla legge applicabile, la legge FRANCESE disciplina l'applicabilità, la costruzione e la validità della presente policy, indipendentemente dal contratto o da altre disposizioni relative alla scelta della legge e senza l'obbligo di stabilire un nesso commerciale in FRANCIA.

Tali disposizioni in materia di legge applicabile si applicano solo alla policy di registrazione. I contratti con un Cliente che fanno riferimento alla presente policy possono avere le proprie disposizioni in materia di legge applicabile, a condizione che tale sezione disciplini l'applicabilità, la costruzione e la validità della presente policy, indipendentemente dai termini e dalle condizioni di tali altri accordi.

9.15. Conformità con la Legge Applicabile

La presente policy di registrazione è soggetta alle leggi, norme, regolamenti, ordinanze e decreti e applicabili francesi ed europei. La RA e la DRA concordano di rispettare le leggi e i regolamenti applicabili ai loro contratti.

9.16. Disposizioni varie

La presente RP costituisce l'intero accordo tra le parti e sostituisce tutti gli altri termini, indipendentemente che siano espressi o impliciti per legge. Nessuna modifica del presente RP entra in forza o diventa efficace se non è in forma scritta e firmata dal firmatario autorizzato. La mancata applicazione di una o di tutte queste sezioni in un caso in particolare non costituisce una rinuncia e non preclude una successiva applicazione. Tutte le disposizioni della presente RP che per loro natura si estendono oltre la durata della prestazione dei servizi (ad esempio, informazioni riservate e diritti di proprietà intellettuale) sono soggette a tali termini e si applicano a tutti i successori della parte.

Se una sezione della presente RP è incorretta o invalida, le altre sezioni della presente RP rimangono efficaci finché la RP non sia stata aggiornata.