La signature électronique certifiée tranquille.

Policy di registrazione QUICKSIGN

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

27 settembre 2016

QUICKSIGN_Registration_Policy_V1.0

Versione	1.0	
Stato	Bozza	Finale
Autore	Margo Companie	QUICKSIGN

Lista di diffusione	Interna	Esterna
		Pubblica

Storico				
Versione	Data	Autore	Commenti	Stato
V.1.0	27/09/2016	MC		Verificato da XR Pubblicato

CONTENUTI

1. INTRODUZIONE

1.1. Sintesi

Presente policy di registrazione (RP) è una modifica del documento "Policy dei certificati – CA firma personale con firma cloud (ETSI 102 042 e ETSI 101 456)" della DOCUSIGN FRANCE. Essa spiega come il servizio di registrazione online [QUICKSIGN QES ON-BOARD ID] gestito dalla QUICKSIGN soddisfi i requisiti esposti dalle Registration Authority (RA) che emettono certificati qualificati con SSCD rispetto agli standard ETSI TS 101 456.

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

Questa RP si basa su:

- [CP]: "Policy dei certificati – CA firma personale con firma cloud (ETSI 102 042 e ETSI 101 456) emessa dalla DOCUSIGN FRANCE, v. 1.3.;
- [PSGP]: "Protect and Sign – Firma personale - Firma attestata e policy di gestione" emesso dalla DOCUSIGN FRANCE, v. 1.4.;
- [ETSI 101 456]: "Requisiti del ETSI 101 456 solo per certificati qualificati - Firme elettroniche e infrastrutture (ESI): requisiti policy per la certification authority che emette i certificati qualificati", ETSI TS 101 456, v. 1.4.3.;

La numerazione di questo documento è in linea con la corrispondenza citata nell'allegato D di ETSI TS 101 456.

1.2. Nome documento e identificazione

Nel contesto di presente documento, l'OID della CP della DOCUSIGN FRANCE da considerare è l'OID 1.3.6.1.4.1.22234.2.8.3.20, che corrisponde a un certificato qualificato con un livello di fiducia SSCD.

1.3. Componenti PKI

1.3.1. Registration Authority (RA)

La RA è di proprietà e gestita dalla QUICKSIGN.

La RA supporta i seguenti servizi della PKI:

- Autenticazione del sottoscrittore tramite verifica che utilizza il documento di identità;
- Autenticazione e autorizzazione della Registration Authority delegata (DRA);
- Costituzione di un rapporto contrattuale con la DRA che incarica la DRA di adempiere ai suoi obblighi come da 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 dalla QUICKSIGN in qualità di RA.

La 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 personali in accordo con i regolamenti di due diligence per le istituzioni che vendono prodotti finanziari, o regolamenti equivalenti.

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

Una lista di DRA, con incluso il riferimento del contatto, il piano di verifica e le persone di riferimento autorizzate a gestire le richieste di revoca per ogni DRA, viene istituita dalla RA.

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 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 QUICKSIGN nelle sue specifiche tecniche.

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

1.4. Utilizzo del certificato

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

1.5. Amministrazione della policy

All'interno della QUICKSIGN, 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 validazione della PMA;
- assicurare che le procedure operative relative all'attività della RA siano eseguite in conformità con presente policy di registrazione.

La persona da contattare è:

Ms Margo COMPANIE
Sviluppo commerciale
QUICKSIGN
38, rue du Sentier
75002 PARIS

1.6. Definizioni

Termine	Definizione
Autenticazione	Un processo ove una parte ha presentata una identità e rivendicazioni di essere tale identità, e la seconda parte conferma che questa 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 terze parti. La CA utilizza una piattaforma di firma CA. Nel contesto di questo documento, la CA è la 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	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 di presente RP. Nel contesto di questo documento, la PMA viene gestita dalla 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 viene gestita dalla QUICKSIGN.
Revoca	Un processo ove il periodo operativo del certificato viene terminato prematuramente. Il periodo operativo dei certificati richiesti dalla QUICKSIGN viene 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 dai regolamenti eIDAS nell'articolo 51.
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 identificazione della transazione	Un identificatore univoco composto a caso di lettere e di cifre, assegnato a una singola richiesta di identificazione e che assicura l'unicità del certificato.

2. RESPONSABILITÀ PUBBLICAZIONE E ARCHIVIO

Presente documento è pubblicato dalla QUICKSIGN 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. Validazione 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, viene fornita dalle risorse tecniche e organizzative della piattaforma di firma CA.

3.2.2 Autenticazione dell'identità dell'organizzazione

Questa parte non è applicabile. La QUICKSIGN accetta le richieste solo dalle persone fisiche che richiedono dei certificati elettronici qualificati inoltrati per loro conto e non per terze parti, dove il soggetto corrisponde al sottoscrittore. Quindi il servizio di registrazione QUICKSIGN non comprende il processo di verifica dell'associazione di una persona con una organizzazione o una persona legale.

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 di assicurare il certificato qualificato, e che soddisfano i requisiti fissati nell'articolo 8 dei regolamenti della 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 completo (incluso 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 of 7 anni.

3.2.4 Validazione dell'autorità

Questa parte non è applicabile. La QUICKSIGN accetta gli ordini solo dagli individuali che richiedono dei certificati elettronici qualificati inoltrati per loro conto e non per terze parti. Quindi il servizio di registrazione QUICKSIGN non comprende il processo di verifica dell'associazione di una persona con una organizzazione o una persona legale.

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 sono conformi agli standard ETSI TS 101 456 con SSCD.

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 validazione 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:

- Nome (tutti);
- Cognome;
- Indirizzo e-mail attuale;
- Numero di cellulare;
- Prova di un documento di identità, che è:
- O: Tipo di documento di identità, numero del documento di identità e periodo di validità del documento di identità;

  O: copia del documento di identità ufficiale;
- Riferimento della DRA;
- Il documento da firmare.

4.2. Lavorazione della domanda di certificato

La RA controlla inoltre, nell'interfaccia della QUICKSIGN, l'identità del sottoscrittore, chiedendo al sottoscrittore di compilare un modulo fornito dall'interfaccia della QUICKSIGN, con una verifica tecnica del documento di identità. Se la domanda di certificato viene eseguita

durante un incontro personale, la DRA si assicura che solo il sottoscrittore in persona compili questo modulo, con i mezzi tecnici che stanno solo sotto il suo controllo.

Queste 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 QUICKSIGN 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 è approvato in base ai termini e alle 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;
- Numero di identificazione della transazione;
- Eventi relativi alla autenticazione del sottoscrittore e alla transazione della DRA;
- Il documento da firmare.

Queste informazioni vengono scambiate in modo sicuro.

4.3. Rilascio del certificato

La CA autentica la RA.

La CA utilizza il protocollo di approvazione 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 elabora il certificato contenuto nel documento firmato (contenuto nel file di prova) disponibile alla RA.

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'utilizzo del certificato. Questi 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 viene pubblicato;
- Le limitazioni della responsabilità;
- Le regolazioni 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).

Il cognome e il nome del sottoscrittore vengono citati sulla pagina da firmare (protocollo di approvazione) 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 certificate, 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 viene archiviato dalla RA e viene 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 utilizzo 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

Questa 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 viene applicato il paragrafo 3.3.

4.8. Modifica del certificato

Questa 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 5 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 sospettato di essere compromesso;
- la DRA ha mancato di adempiere ai suoi obblighi e ai regolamenti di sicurezza descritti in presente CPS;

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 sospettato di essere compromesso;
- 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 validazione dell'identità iniziale avvenuta personalmente personale 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 sospettato di essere compromesso;
- la DRA ha mancato di adempiere ai suoi obblighi e ai regolamenti di sicurezza descritti in presente CPS.

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 è possibile stipulare un contratto di servizio clienti tramite telefono. 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 esposte 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 vengono documentate manualmente dalla RA.

5. DISPOSITIVO, GESTIONE E CONTROLLI OPERATIVI

5.1. Controlli fisici

Tutti i controlli fisici, inclusa l'ispezione delle premesse e la costruzione dei dispositivi del centro dati utilizzati per avviare il servizio di registrazione, vengono controllati da un verificatore tecnico indipendente.

L'accesso fisico agli uffici della RA è ristretto alle sole persone autorizzate. Le persone non autorizzate devono sempre essere accompagnate dallo staff 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 dei dispositivi che elaborano le informazioni; e per prevenire il prelievo non

autorizzato dei patrimoni della RA. Questi controlli vengono 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 temporale o la rimozione 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 dovrà affrontare delle sanzioni disciplinari in conformità con la legge sul lavoro francese.

I ruoli di sicurezza e le responsabilità sono documentati nella descrizione del lavoro e sono resi disponibili a tutto il personale interessato. Il personale è consapevole della separazione dei compiti e del privilegio minimo, 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 QUICKSIGN.

Il personale manageriale possiede l'esperienza o la formazione relativa alla sicurezza delle informazioni e della firma.

Lo staff che prende decisioni in merito al processo di iscrizione è libero da qualsiasi conflitto di interessi e ha il piano potere decisionale, eccezion fata per le situazioni di crisi.

Il personale è incaricato formalmente dei ruoli di fiducia dal management senior, in conformità con il principio del "minimo privilegio". Il personale ha accesso ai ruoli di fiducia solo dopo aver comprovata la propria qualifica per il ruolo descritto. Lo staff della QUICKSIGN prova la propria

affidabilità presentando il proprio casellario giudiziale oltre a delle buone referenze da precedenti datori di lavoro.

5.4. Procedure audit logging

I file di verifica del log vengono generati per tutti gli eventi relativi alla sicurezza e alla RA e ai servizi 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 dell'osservanza.

La privacy delle informazioni del soggetto viene 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 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 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 vengono garantite tramite un meccanismo di backup dell'impresa.

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 revisionati dall'amministratore di sistema. Se un sistema di sicurezza segnala all'amministratore di sistema un potenziale problema di sicurezza, i log vengono rivisti immediatamente.

5.4.1. Registration Authority

Il logging comprende almeno i seguenti argomenti:

- Accesso fisico al dispositivo;
- 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 mezzi di autenticazione del sottoscrittore;
- Accesso logico;
- Gestione del backup;
- Gestione dei ruoli di fiducia;
- gestione del log di accesso; in particolare, la DRA deve avere una lista di tutti gli accessi che sono autorizzati a iscrivere e gestire i sottoscrittori;
- Gestione dell'informatica e della rete.

5.5. Archiviazione della documentazione

5.4.1. 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 della QUICKSIGN in qualità di una 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 presente sul certificato, e il passaggio di queste informazioni a terze parti, alle stesse condizioni di quelle richiesta da 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 consente di pubblicare il certificato;
- conferma che le informazioni contenute nel certificato siano corrette.

Il documento viene archiviato per almeno sette anni.

La segretezza e l'integrità della documentazione attuale e archiviata, in riferimento ai certificati qualificati, viene mantenuta. La documentazione viene archiviata completamente e in modo riservato, in conformità con le pratiche commerciali rivelate; se richiesto, deve essere resa disponibile per fornire una prova della certificazione per 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;
- Il supporto viene supervisionato 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 sono andati persi e che non sono stati recuperati dallo specchio del sistema di archiviazione;

- Tutti i supporti utilizzati per archiviare i dettagli personali vengono cancellati e distrutti alla fine della loro durata;
- Nessun mezzo utilizzato nel sistema di archiviazione può essere 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 seguenti informazioni di registrazione:

- Il tipo di documento presentato dal sottoscrittore per supportare la registrazione;
- Il numero di identificazione, o, se applicabile, copia del documento di identità;
- Il log di registrazione;
- L'ubicazione del salvataggio delle copie delle domande e dei documenti di identificazione, incluso 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.

La segretezza e l'integrità della documentazione archiviata, in riferimento ai certificati qualificati, viene mantenuta. La documentazione viene archiviata completamente e in modo riservato, in conformità con le pratiche commerciali rivelate; se richiesto, deve essere resa disponibile per fornire una prova della certificazione per 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;
- Il supporto viene supervisionato 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 sono andati persi e che non sono stati recuperati dallo specchio del sistema di archiviazione;
- Tutti i supporti utilizzati per archiviare i dettagli personali vengono cancellati e distrutti alla fine della loro durata;
- Nessun mezzo utilizzato nel sistema di archiviazione può essere 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 chiave

Il periodo di validità del certificato sottoscrittori viene definito nella policy dei certificati CA.

5.7. Ripristino in caso di compromissione e di disastro

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

5.8. Risoluzione

5.8.1. Registration Authority

Se la QUICKSIGN prevede la cessazione del suo ruolo di registration authority per la CA, deve:

- darne notizia alla CA prima della risoluzione, 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 risoluzione,
- interrompere la consegna delle richieste di certificato,
- informare i sottoscrittori e gli utilizzatori nel caso in cui è stata compromessa nel suo ruolo di registration authority.

La decisione dell'entità alla quale la 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 risoluzione, 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 gli utilizzatori nel caso in cui è stata compromessa nel suo ruolo di registration authority delegata.

La decisione dell'entità alla quale la DRA deve consegnare la documentazione archiviata, viene definiti 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 SSCD qualificato, che soddisfa i requisiti della regolamentazione (UE) n. 910/2014.

6.2. Protezione chiave privata e tecnica modulo crittografico

La generazione della coppia di chiavi CA viene eseguita 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 accordo 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, viene 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 da operazioni rilevanti. La RA e la DRA assicurano che l'accesso al sistema è limitato ai soli individui autorizzati.

I dati sensibili sono protetti dall'essere rivelati tramite degli oggetti archiviati 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 QUICKSIGN, in particolare per assicurare che la sicurezza venga costruita nel sistema informatico DRA.

Le procedure di controllo delle modifiche sono applicate alle delibere, alle modifiche e al 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, dal software sospetto e non autorizzato. I danni derivati da incidenti di sicurezza e da malfunzionamenti sono minimizzati dall'utilizzo dei report sugli incidenti e le procedure di risposta. I supporti utilizzati nella RA e nella DRA vengono trattati 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 nell'arco del tempo in cui la documentazione deve essere conservata. Le procedure vengono stabilite e eseguite per tutti i ruoli di fiducia e amministrativi che impattano sulle disposizioni dei servizi di certificazione.

Le procedure sono specificate e applicate per assicurare che i patch di sicurezza vengano applicati entro un periodo ragionevole dal momento in cui sono stati resi disponibili, che i patch

di sicurezza non vengano applicati se introducono una instabilità che supera i vantaggi derivanti dalla loro applicazione, e che la motivazione per non applicare un patch di sicurezza venga documentata e scelta 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 sistemi del sistema all'interno delle zone di sicurezza.

6.8. Orodatazione

Le procedure elettroniche o manuali vengono utilizzate per mantenere l'ora del sistema. Per un periodo garantito su registrazioni di verifica, la QUICKSIGN sincronizza regolarmente con un servizio a tempo.

7. QUADRO PER LA DEFINIZIONE DI ALTRE POLICY DI CERTIFICATI COSTRUITI SU PRESENTE DOCUMENTO

La QUICKSIGN 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

Prima di iniziare il ruolo di servizio di registrazione, un verificatore esterno esegue una valutazione ETSI in conformità con la TS 101 456.

Il primo e il secondo anno successivo alla verifica esterna, viene eseguita una verifica della RA da parte della CA, in conformità con il programma di verifica della piattaforma di firma CA.

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

Nel caso in cui durante la verifica interna eseguita dalla CA dovessero essere scoperti dei rilevamenti più importanti, la QUICKSIGN risolverà questi problemi e entro lo stesso anno verrà eseguita una verifica esterna.

8.1.2. Registration Authority delegata

La RA controlla che la DRA sia adempiente 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 condurrà una verifica dell'osservanza, prima di iniziare il proprio ruolo in qualità di DRA.

La DRA accetta che la RA e la PMA condurranno una verifica ogni qualvolta sarà necessario per assicurare che sia adempiente con presente policy di registrazione e con la CP.

Se durante una di queste verifiche viene rilevata una mancanza di conformità, la registration authority delegata provvederà ad adempiere senza indugio alla RP e alla CP. Se la questione non viene risolta entro un periodo determinato dal verificatore, la RA sospenderà i propri servizi finché non sarà raggiunto un adempimento effettivo, alle condizioni fornite nel contratto tra la RA e la DRA.

8.2. Argomenti coperti dalla valutazione

8.2.1. Registration Authority

Il perimetro per una verifica della QUICKSIGN in qualità di registration authority è:

- La protezione, l'utilizzo 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 fissati in presente CP;
- La procedura di registrazione definita dalla QUICKSIGN 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;
- La sicurezza fisica;
- La protezione e gestione dei dati personali dei sottoscrittori.

8.2.2. Registration Authority delegata

I perimetri di una verifica della DRA sono:

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

9. ALTRE ATTIVITÀ E QUESTIONI LEGALI

9.1. Contributi

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

9.2. Responsabilità finanziaria

La QUICKSIGN mantiene dei livelli ragionevoli di copertura assicurativa e sufficienti risorse finanziarie per mantenere le operazioni. L'assicurazione o la copertura di garanzia è definita nel contratto tra la QUICKSIGN e il cliente.

9.3. Segretezza delle informazioni commerciali

La QUICKSIGN mantiene la segretezza delle informazioni aziendali confidenziali, inclusi i dati relativi all'identità personale, la richiesta di certificato del sottoscrittore, i risultati e i report delle verifiche, il piano di continuità aziendale e il contratto con il cliente.

9.4. Privacy delle informazioni personali

9.4.1. Registration Authority

La QUICKSIGN protegge la segretezza e l'integrità dei dati di registrazione, in conformità con la legge europea applicabile sulla privacy dei dati. L'impostazione della QUICKSIGN del regolamento della privacy dei dati è documentata nel suo ISSP. Queste regolazioni vengono presentate a ogni sottoscrittore prima di qualsiasi transazione, e i termini e le condizioni del servizio in cui sono contenute devono essere accettati dal sottoscrittore cliccando sul riquadro di spunta.

La QUICKSIGN viene supervisionata dalla Data Protection Authority di Parigi (CNIL) e fa capo a un funzionario di Data Protection. I suoi riferimenti di contatto sono seguenti:

Xavier Roussillon
Director of Operations
QUICKSIGN
38, rue du Sentier
75002 PARIS

9.4.2. Registration Authority delegata

La DRA protegge la segretezza e l'integrità dei dati di registrazione. La impostazione della DRA delle regole relative alla privacy dei dati viene documentata e è conforme alla legge europea applicabile sulla privacy dei dati.

9.5. Diritti di proprietà intellettuale

Questa 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 QUICKSIGN avverte la PMA in caso di un incidente di sicurezza.

La QUICKSIGN informa il sottoscrittore in merito ai termini e alle condizioni che riguardano l'utilizzo 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 QUICKSIGN invia una e-mail al sottoscrittore contenente i termini e le condizioni del servizio, o, opzionalmente, mette a disposizione questi termini sul sito web.

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

La QUICKSIGN autentica la DRA e il sottoscrittore.

La QUICKSIGN 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'utilizzo del servizio. Il metodo utilizzato per autorizzare una DRA viene approvato dalla PMA.

La QUICKSIGN costituisce un rapporto contrattuale con una DRA che incarica la DRA di adempiere ai suoi obblighi come da presente policy di registrazione;

La QUICKSIGN deve impegnarsi al meglio per assicurare che la DRA rispetterà i suoi obblighi emergenti da presente policy di registrazione, e che lo farà per l'intero periodo.

La QUICKSIGN collabora con la CA nel controllo e nella verifica delle attività eseguite dalla DRA;

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

La QUICKSIGN informa il sottoscrittore se la chiave privata del sottoscrittore è andata persa, è stata rubata o è potenzialmente compromessa a causa di una compromissione dei dati di attivazione o per altre ragioni.

La QUICKSIGN assicura che nessun certificato venga utilizzato dal sottoscrittore o da un utilizzatore, se la CA ha detto che il certificato del sottoscrittore è stato compromesso.

Solo la QUICKSIGN trasmette le richieste di revoca autenticate alla CA.

La QUICKSIGN deve supportare i team di verifica in modo costruttivo e deve mettere in atto ogni sforzo ragionevole necessario per completare una verifica e per comunicare il risultato.

9.6.2. Registration Authority delegata

Gli obblighi della DRA vengono definiti contrattualmente tra la QUICKSIGN e la DRA.

La DRA assicura che ogni sottoscrittore per il quale è stata presentata una domanda di certificato alla CA tramite la RA, è stato identificato e autenticato adeguatamente, e che la richiesta

di certificato è stata eseguita in modo accurato e ed è stata autorizzata debitamente. La DRA assicura che la richiesta di certificato inoltrata contiene solo informazioni accurate e complete.

La DRA assicura che la sua organizzazione possiede le competenze, l'affidabilità, l'esperienza e le qualifiche necessarie, e ha ricevuto la formazione adeguata riguardo alla sicurezza e alle regole sulla protezione dei dati personali per l'identificazione e l'autenticazione in conformità con i regolamenti di due diligence per le istituzioni che vendono prodotti finanziari, o regolamenti equivalenti.

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

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

9.7. Esclusione di garanzia

La DRA garantisce la validazione e l'autenticazione iniziale dell'identità del sottoscrittore. La QUICKSIGN garantisce che stipulerà 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 personali in accordo con i regolamenti di due diligence per le istituzioni che vendono prodotti finanziari, o regolamenti equivalenti.

La RA garantisce anche che rende sicura la capacità finanziaria della DRA. La RA non fornisce altre garanzie, espressa o implicita, stabilita per legge o altro, e declina qualsiasi responsabilità per la validazione iniziale dell'identità e l'autenticazione del sottoscrittore.

Di conseguenza, premesso che la DRA abbia adempiuto al suo ruolo come descritto in 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 altro, 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 QUICKSIGN non pretende nulla in riferimento all'idoneità o all'autenticità dei certificati emessi in conformità con presente RP. Gli utilizzatori possono solo utilizzare questi certificati a loro rischio. La QUICKSIGN non si assume alcuna responsabilità per l'utilizzo del certificato diverso dall'utilizzo descritto nel presente documento.

La DRA è responsabile per quanto concerne l'accuratezza di tutte le informazioni di registrazione, subordinatamente ai termini del contratto tra la QUICKSIGN e la DRA. La QUICKSIGN

non ha alcuna responsabilità per il ritardo, la mancata consegna, il mancato pagamento, la consegna errata o l'interruzione del servizio causati da una terza parte, inclusa la DRA.

9.9. Indennità

La RA non pretende nulla in riferimento all'idoneità o all'autenticità dei certificati emessi in conformità con presente RP. Non esiste alcun obbligo di pagare i costi associati al malfunzionamento o all'utilizzo errato dei dettagli personali verificati per una richiesta di certificato.

9.10. Durata e termine

La RP e le versioni successive sono efficaci in seguito all'approvazione della PMA.

Nel caso in cui la RA dovesse cessare di essere operativa, la RA deve seguire la procedura descritta nel paragrafo 5.8. di presente documento.

9.11. Notifiche individuali e comunicazioni con i partecipanti

La QUICKSIGN fornisce una nuova versione di presente policy di registrazione tramite il suo sito web.

9.12. Modifiche

La QUICKSIGN rivede presente documento la sua certification practices statement almeno una volta l'anno. A discrezione della QUICKSIGN, 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 risolvere le controversie tra la QUICKSIGN e i suoi clienti sono fissate nel contratto applicabile tra le parti.

9.14. Legge Applicabile

Subordinatamente a qualsiasi limitazione presente nella legge applicabile, la legge FRANCESE disciplina l’esecutività, la costruzione e la validità della presente policy, indipendentemente dal contratto o da un'altra scelta di disposizioni legali e senza la pretesa di istituire una qualsivoglia natura commerciale in FRANCIA.

Presente disposizione ai sensi della legge applicabile si applica solo alla policy di registrazione. I contratti con un cliente con riferimento a presente policy possono avere le loro disposizioni di legge applicabile, premesso che questa sezione disciplina l’esecutività, la costruzione e la validità di presente policy, indipendentemente dai termini e dalle condizioni di tali altri accordi.

9.15. Osservanza delle Leggi Applicabili

Presente policy di registrazione è soggetta alle leggi francesi, ai regolamenti, alle normative, alle ordinanze, ai decreti e agli ordini. Il cliente e la QUICKSIGN concordano di osservare le leggi e le normative applicabili nei loro contratti.

9.16. Varie disposizioni

Presente RP 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 RP 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 non costituisce una rinuncia e non preclude una successiva applicazione. Tutte le disposizioni in presente RP che per natura esulano dai termini della performance dei servizi (per esempio le informazioni confidenziali corrispondenti e i diritti di proprietà intellettuale) servono tali termini e si applicano a tutti i successori della parte.

Se una sezione di presente RP non dovesse essere corretta o non valida, le altre sezioni di presente RP rimangono efficaci finché la RP non è stata aggiornata.