Manuale Operativo / CPS
Certification Practice Statement e Certificate Policy

Codice Identificazione CANEXI-CPS-001-01

Tipologia Documento: **CPS**	Data Emissione: **03/11/2017**	Pagine: **1/75**

	Nominativo	Funzione	Data	Firma
Redazione	Nicola Baggini	Analista Funzionale CA	02/11/2017	
Verifica	Andrea Porfirione	Responsabile Ufficio e-Banking	02/11/2017	
Verifica	Luca Biancardi	Responsabile Sicurezza CA	03/11/2017	
Verifica	Serena Barbara	Responsabile Ufficio DCB Operations	03/11/2017	
Approvazione	Renato Martini	Responsabile Servizio CA	03/11/2017	

STORIA DELLE MODIFICHE APPORTATE

Versione	Data applicazione	Descrizione delle modifiche
01	03/11/2017	Prima versione del documento.

LEGENDA DI COPERTINA

Stato del documento

Le firme sulla copertina del presente documento fanno riferimento allo standard interno di Nexi per la gestione della documentazione del Sistema Qualità: hanno lo scopo di permetterne il controllo di configurazione e di indicarne lo stato di lavorazione.

Si segnala che la firma di approvazione autorizza la circolazione del documento limitatamente alla lista di distribuzione e non implica in alcun modo che il documento sia stato revisionato e/o accettato da eventuali Enti esterni.

In particolare, il documento è da intendersi **REDATTO** se provvisto della/e firma/e di chi lo ha redatto; **VERIFICATO** se ha superato con esito positivo la verifica interna e quindi provvisto della/e firma/e di verifica che ne autorizza il rilascio alla GESTIONE DELLA CONFIGURAZIONE. Nel caso in cui la revisione abbia esito negativo il documento viene modificato e verificato, con un nuovo numero di versione e una nuova data di emissione. Il documento è da intendersi **APPROVATO** se provvisto della firma di approvazione che si aggiunge alle altre.

Un documento sprovvisto di firme è in uno stato indefinito, non può essere messo in circolazione.

Distribuzione

La distribuzione di un documento può essere:

- **PUBBLICA**, se il documento può circolare senza restrizioni;
- **INTERNA**, se il documento può circolare solo all'interno di Nexi;
- **RISERVATA,** se il documento è distribuibile ad un numero limitato di destinatari;
- **CONTROLLATA**, se il documento è distribuibile ad un numero limitato di destinatari e ogni copia è controllata.

Nexi

Sommario

1 Introduzione

1.1 Quadro generale

Nexi SpA, un Prestatore di Servizi Fiduciari (Trust Service Provider) accreditato presso l'AgID sino dal 2012, eroga servizi qualificati di certificazione di chiavi pubbliche, oltre a diversi altri servizi fiduciari.

Un certificato lega una chiave pubblica ad un soggetto (individuo od organizzazione). Tale soggetto, titolare del certificato, possiede ed utilizza la corrispondente chiave privata. Il certificato viene generato e fornito al titolare da una terza parte fidata, detta **Certification Authority** (di seguito CA), ed è firmato digitalmente dalla CA.

Nexi svolge il ruolo di CA nell'ambito del servizio qui descritto. Nexi si avvale di due outsourcer come indicato nel piano della sicurezza Paragrafo 2.2.

Nell'ambito di questo documento, i termini "CA", "Prestatore" (di Servizi Fiduciari) e "Certificatore" sono utilizzati come sinonimi e fanno tutti riferimento a Nexi, inteso come il soggetto erogatore del servizio di CA, e/o ai sistemi informativi utilizzati da Nexi per l'erogazione del servizio di CA, salvo dove sia specificato diversamente.

L'affidabilità di un certificato, ovvero la fiducia che si può riporre nell'associazione tra la chiave pubblica e il soggetto specificati nel certificato, dipende sensibilmente dalle procedure operative seguite dalla CA, dagli obblighi e responsabilità che si assumono la CA e il titolare del certificato, e dalle misure di sicurezza fisica, operativa e tecnica poste in atto dalla CA a protezione dei propri sistemi di elaborazione. Tali aspetti, insieme ad altre informazioni necessarie per poter valutare il servizio offerto da una CA, sono descritti in un documento pubblico chiamato **Certification Practice Statement** (di seguito CPS).

Questo documento è il CPS di Nexi relativo all'emissione e gestione di **certificati qualificati** conformi alle norme vigenti, in particolare il Regolamento UE n.910/2014 (in seguito, per brevità, citato anche come "Regolamento eIDAS").

La struttura di questo CPS si basa sulla specifica pubblica RFC 3647.

1.2 Nome identificativo del documento

La versione vigente del CPS è pubblicata sul sito web della CA (https://ca.nexi.it) e sul sito web dell'AgID (www.agid.gov.it). Nel caso di eventuali discrepanze tra le due pubblicazioni, farà fede la versione pubblicata sul sito web della CA.

Questo CPS è pubblicato in formato PDF firmato, in modo tale da assicurarne l'origine e l'integrità.

1.3 Partecipanti alla PKI

1.3.1 Certification Authority

Nell'ambito della PKI a cui fa riferimento questo CPS, il ruolo di Certification Authority (CA) è svolto unicamente dalla società Nexi SpA Di seguito i dati identificativi della società:

Denominazione sociale:	**Nexi SpA**
Indirizzo della sede legale:	**Corso Sempione 55 • 20149 Milano**
Legale rappresentante:	**Dott. Bernabè Franco (Presidente)**
N° iscrizione Registro Imprese di Milano:	**R.E.A. n. 318847**
N° di Partita IVA:	**13212880150**
N° di telefono (centralino):	**+39 02 7705 1**
ISO Object Identifier (OID):	1.3.6.1.4.1.40796
Sito web generale (informativo):	https://www.nexi.it
Sito web del servizio di certificazione:	https://ca.nexi.it
E-mail (informativo):	info@ca.nexi.it
Directory server (registro dei certificati):	ldap://ldap.ca.nexi.it

Come previsto dalle norme italiane, la PKI realizzata da Nexi prevede un solo livello di chiavi di certificazione (chiavi di CA). Pertanto tutte le chiavi di CA sono "root" e sono di conseguenza self-signed.

Le chiavi di CA attualmente in uso da parte di Nexi e coperte dal presente CPS sono elencate nella Appendice A.

1.3.2 Registration Authority

L'identificazione e autenticazione (I&A) dei soggetti che richiedono i certificati possono essere svolte, oltre che direttamente dal personale della CA, anche da terze parti delegate (ovvero "Registration Authorities", RA) sulla base di appositi accordi stipulati con la CA. Le RA sono anche dette Centri di Registrazione Locale (CDRL).

Normalmente, le RA svolgono anche l'attività di "registrazione" che consiste nella trasmissione alla CA, con procedure sicure, dei dati anagrafici dei Richiedenti (futuri Titolari) e altri dati ad essi associati, affinché tali dati siano memorizzati nei sistemi della CA ai fini dell'emissione dei certificati.

Le RA sono responsabili nei confronti della CA della corretta e sicura I&A dei Richiedenti, nonché del trattamento dei loro dati nel pieno rispetto della normativa sulla privacy e altre norme applicabili. La CA rimane comunque pienamente responsabile, nei confronti di chiunque si affidi ai certificati, della I&A dei Richiedenti, sia essa svolta in proprio dalla CA oppure dalle RA.

Le RA sono soggette a ispezioni da parte della CA, finalizzate a verificare il rispetto da parte delle RA degli accordi stipulati con la CA.

La CA rende disponibili alle RA gli opportuni strumenti e procedure per effettuare le operazioni di registrazione degli utenti, nonché per l'emissione e la successiva gestione (es. sospensione o revoca) dei certificati. A tali strumenti possono accedere solo gli operatori di RA espressamente autorizzati dalla CA.

Le RA possono, secondo le circostanze, rivestire anche il ruolo di "terzo interessato" (vedere il decreto [3]) e dunque avere i conseguenti diritti e doveri.

1.3.3 Utenti Finali (titolari)

Il titolare di un certificato emesso secondo questo CPS può essere:

a) una persona fisica;

b) una persona fisica associata ad una persona giuridica;

c) una persona giuridica (es. un'impresa, un ente pubblico o altro tipo di organizzazione).

1.3.4 Relying parties

Le "Relying Parties" sono tutti i soggetti che fanno affidamento sulle informazioni contenute nei certificati. In particolare, per quanto riguarda il servizio di CA qui descritto, sono tutti i soggetti che verificano firme elettroniche attraverso i certificati emessi secondo questo CPS.

1.3.5 Altri partecipanti

Nell'ambito della PKI svolge un ruolo importante l'organismo di supervisione nazionale **AgID** (**Agenzia per l'Italia Digitale**). Ai sensi del regolamento europeo eIDAS, l'AgID pubblica sul proprio sito la Trust Service List (TSL) nazionale che elenca tutte le CA qualificate accreditate.

1.4 Uso previsto dei certificati

I certificati qualificati emessi secondo questo CPS sono da utilizzarsi per la verifica di **sigilli** e **firme elettroniche avanzate e qualificate**. Altri usi dei certificati non sono previsti e sono da evitarsi. La CA si riserva facoltà di revocare i certificati qualora venga a sapere che sono utilizzati in modo improprio.
I certificati emessi secondo questo CPS si differenziano nel profilo secondo che il titolare sia una persona fisica oppure giuridica, che la corrispondente chiave privata risieda o meno in un dispositivo sicuro di firma (QSCD – Qualified Signature Creation Device) e che la firma venga apposta con una procedura remota o meno. Di seguito sono elencati gli **OID** (**Object IDentifier**) **delle policy supportate** da questo CPS. Per ciascuna di esse, c'è la policy di riferimento definita nella norma ETSI EN 319 411-2.

Policy OID specificato nei certificati emessi da NEXI	Policy di riferimento ETSI EN 319 411-2	Persona	Chiavi su QSCD	Firma Remota
1.3.6.1.4.1.40796.3.1	**QCP-n-qscd**	Fisica	SI	NO
1.3.6.1.4.1.40796.3.2	**QCP-n-qscd**	Fisica	SI	SI
1.3.6.1.4.1.40796.3.3 (*)	**QCP-n**	Fisica	NO	NO
1.3.6.1.4.1.40796.3.4 (*)	**QCP-n**	Fisica	NO	SI
1.3.6.1.4.1.40796.4.1 (*)	**QCP-l-qscd**	Giuridica	SI	NO
1.3.6.1.4.1.40796.4.2	**QCP-l-qscd**	Giuridica	SI	SI
1.3.6.1.4.1.40796.4.3 (*)	**QCP-l**	Giuridica	NO	NO
1.3.6.1.4.1.40796.4.4 (*)	**QCP-l**	Giuridica	NO	SI

(*) *Alla data di revisione di questo CPS*, queste policy non sono ancora disponibili.

I certificati contengono normalmente due Policy OID: quello proprietario di Nexi e quello standard definito nella norma ETSI EN 319 411-2.

Può essere presente un terzo Policy OID, nel caso dei certificati per chiavi di “firma digitale verificata”, ai sensi della Determina AgID n.63/2014 (in questo caso, il Policy OID aggiuntivo è **1.3.76.16.3**).

Eventuali **limitazioni d’uso** possono essere specificate nei certificati mediante l’attributo **userNotice** dell’estensione CertificatePolicies. In particolare, i certificati per *firma automatica* sono un caso particolare dei certificati per firma remota, e contengono almeno la specifica limitazione d’uso stabilita dall’AgID (vedere http://www.agid.gov.it/sites/default/files/circolari/limiti_uso_nei_cq_2014_v.1.pdf).

Eventuali **limitazioni sul valore** delle transazioni (nelle quali il certificato può essere usato) possono essere specificate nell’estensione qCStatements dei certificati, attraverso la voce ***QcEuLimitValue***.

1.5 Amministrazione del CPS

1.5.1 Organizzazione responsabile

Questo CPS è redatto, pubblicato ed aggiornato da Nexi SpA.

Richieste di informazioni o chiarimenti sul presente CPS e/o sulle policy di certificato (CP) qui definite possono essere inviate tramite l'apposita funzione presente all'interno del sito web del servizio di certificazione (vedi pagina Contattaci: https://ca.nexi.it/Contact)

1.5.2 Soggetti approvatori

Questo CPS è approvato dalla Direzione aziendale, previa verifica da parte delle funzioni aziendali interessate e tenendo conto di quanto indicato all'art. 6.1 della norma ETSI EN 319 401.

1.5.3 Soggetti approvatori

La redazione e approvazione del CPS segue le procedure previste dal Sistema di Gestione Qualità aziendale. Questo CPS viene riesaminato e, se necessario, aggiornato con frequenza almeno annuale.

1.6 Definizioni ed acronimi

CA	Certification Authority
CAB	Conformity Assessment Body
CAD	Codice dell'Amministrazione Digitale (D.lgs. n.82/2005)
CP	Certificate Policy
CRL	Certificate Revocation List
CSP	Certification Practice Statement
HSM	Hardware Security Module
HTTP	Hyper-Text Transfer Protocol
I&A	Identificazione e Autorizzazione
OCSP	On-line Certificate Status Protocol
OID	Object IDentifier
PKI	Public Key Infrastructure
QSCD	Qualified Signature-Creation Device
RA	Registration Authority
TLS	Transport Layer Security
TSL	Trust-service Status List
TSP	Trust Service Provider

2 Pubblicazioni e repository

2.1 Repository

Con “repository” si intende l’archivio on-line attraverso il quale la CA rende pubbliche e liberamente accessibili le informazioni necessarie ai soggetti che partecipano alla PKI (i Richiedenti, i Titolari, le RA delegate, le RP, ecc.), nel rispetto di questo CPS.

Il repository di Nexi è rappresentato principalmente sul sito web della CA (https://ca.nexi.it) ed altri siti da esso richiamati. Per alcune esigenze può essere utilizzato anche un directory server.

La CA gestisce il repository e ne è direttamente responsabile.

Il repository è normalmente accessibile in modo continuo (7x24).

2.2 Informazioni pubblicate/presenti relative ai certificati

La CA pubblica almeno la seguente documentazione sul proprio sito web:

- Certification Practice Statement (CPS)
- PKI Disclosure Statement (PDS)
- Condizioni Generali di Contratto
- Tariffe dei servizi(*)
- Certificati di CA
- Modulistica utile per l’utilizzo dei servizi fiduciari di Nexi

Sono inoltre pubblicate le liste dei certificati sospesi o revocati (CRL).

(*): alla data del presente documento, Nexi non eroga servizi direttamente ad utenza retail, poiché per i servizi di Nexi affinché ne usufruiscano gli utenti finali, Nexi concorda tariffazioni di servizio con i propri clienti Corporate, e saranno questi ultimi poi che forniranno i servizi fiduciari alla propria clientela finale. Ne consegue che le tariffazioni di servizio, per via di quanto sopra, non possono essere pubblicate perché non note a priori, essendo concordate di volta in volta tra l’Account Manager di Nexi, ed il Cliente Corporate stesso, in funzione di parametri e accordi non definibili a priori.

2.3 Tempi e frequenza delle pubblicazioni

Questo CPS e la documentazione annessa vengono pubblicati sul sito web della CA in occasione di ogni aggiornamento.

Per quanto riguarda la pubblicazione delle CRL si rimanda al paragrafo 4.9.7.

2.4 Controllo degli accessi

- L’accesso al repository in sola lettura (“read-only”) è completamente libero per chiunque.

- L'accesso al repository in "scrittura", ossia per la pubblicazione di informazioni nuove o aggiornate, è consentito solo ad Nexi nei termini delle figure preposte, ed Nexi ne è responsabile.

3 Identificazione & Autenticazione (I&A)

3.1 Denominazione dei titolari

Tipi di nomi

Il Titolare è identificato all'interno del certificato attraverso un Distinguished Name (DN), nel campo Subject, conforme allo standard ITU-T X.500 (ISO/IEC 9594). Le regole di valorizzazione degli attributi del DN rispettano i requisiti e raccomandazioni delle norme ETSI EN applicabili, in merito ai profili di emissione dei certificati per persone fisiche e per persone giuridiche, e le conseguenti specifiche RFC 5280. In particolare, i certificati emessi secondo questo CPS sono conformi ai seguenti standard:

- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates.
- ETSI EN 319 412-1: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures.
- ETSI EN 319 412-2: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons.
- ETSI EN 319 412-3: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons.
- ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

3.1.1 Esigenza di avere nomi significativi

Nel campo Subject sono inseriti dati chiaramente identificativi del Titolare (persona fisica o giuridica) del certificato, salvo quanto precisato nel paragrafo 3.1.2.

Nel caso di certificati emessi a persona fisica, il campo Subject contiene *almeno* gli attributi seguenti:

- countryName (OID: 2.5.4.6)
- givenName (OID: 2.5.4.42)
- surname (OID: 2.5.4.4)
- commonName (OID: 2.5.4.3)

- serialNumber (OID: 2.5.4.5)

In tutti i casi, il campo Subject contiene anche l'attributo dnQualifier (OID 2.5.4.46).

3.1.2 Anonimato e pseudonimia dei titolari

Nel caso in cui sia richiesto di inserire nel certificato uno pseudonimo, in luogo dei dati reali del richiedente, la CA si riserva di valutare caso per caso l'ammissibilità della richiesta.

Qualora sia utilizzato uno pseudonimo, esso è chiaramente identificato come tale nel certificato attraverso lo specifico attributo pseudonym (OID 2.5.4.65) del campo Subject.

In questo caso, nel campo Subject sono omessi gli attributi givenName, surname e serialNumber.

3.1.3 Interpretazione dei nomi

Per le regole di interpretazione dei nomi ci si attiene allo standard ITU-T relativo ai servizi di directory (ITU-T X.500 ovvero ISO/IEC 9594).

3.1.4 Unicità dei nomi

Per garantire l'univocità del campo Subject (identificativo del Titolare) del certificato, in conformità con le direttive ETSI EN 319 412 in merito ai profili di emissione dei certificati, il campo Subject contiene attributi identificativi specifici in base alla natura del Titolare stesso.

- Qualora il titolare sia una persona fisica, l'univocità è garantita grazie all'inserimento dell'attributo **serialNumber** (OID: 2.5.4.5) nel campo Subject del certificato.
    - Normalmente, questo attributo contiene il **codice fiscale (TIN)** della persona fisica ed il codice ISO 3166 del paese che lo ha rilasciato.
        - *Qualora il titolare non disponga di un codice fiscale*, al suo posto può essere utilizzato il numero del **passaporto** o della **carta d'identità** (ID) del titolare.
- Qualora il titolare sia una persona giuridica, l'univocità è garantita grazie all'inserimento dell'attributo **organization Identifier** (OID: 2.5.4.97) nel campo Subject del certificato.
    - Normalmente, questo attributo contiene il **codice fiscale (VAT number)** della persona giuridica ed il codice ISO 3166 del paese che lo ha rilasciato.
        - *Qualora il titolare non disponga di un codice fiscale*, al suo posto può essere utilizzato un diverso codice identificativo univoco dell'organizzazione.

Il formato degli attributi:

- serialNumber
- organizationNumber

È conforme, ove possibile, allo standard ETSI EN 319 412-1

3.1.5 Riconoscimento, autenticazione e ruolo dei marchi registrati

Si fa presente che la CA *non* svolge verifiche sull'utilizzo di marchi e marchi registrati, i quali sono di proprietà esclusiva dei rispettivi titolari.

I richiedenti del certificato rappresentano e garantiscono che la loro presentazione alla CA e l'utilizzo delle informazioni relative alla richiesta del certificato non interferiscano e né danneggino i diritti di una qualsiasi terza parte, di qualunque giurisdizione, in merito a marchi, marchi di identificazione di servizio, nomi commerciali, denominazioni societarie e ogni altro diritto di proprietà intellettuale, e che non tenteranno di utilizzare il certificato (e le informazioni in esso contenute) per scopi illegali, ivi compresi interferenze illecite su vantaggi contrattuali o potenziali vantaggi aziendali, concorrenza sleale, azioni volte a ledere la reputazione di altra persona, pubblicità ingannevole, e ingenerare confusione su persone fisiche o giuridiche.

I titolari e i richiedenti del certificato si obbligano a manlevare e indennizzare la CA contro qualunque perdita o danno, derivanti da una tale interferenza o infrazione.

3.2 Verifica iniziale dell'identità

Questa sezione descrive le modalità di identificazione del richiedente (validazione dell'identità del richiedente e del suo possesso della chiave privata) al momento della richiesta di rilascio del certificato qualificato. Il processo di validazione iniziale dell'identità è relativo alla verifica da parte della CA dell'identità del Titolare o dell'identità della persona fisica che rappresenta un'organizzazione.

3.2.1 Possesso chiave privata (evidenza)

La dimostrazione del possesso, da parte del Richiedente, della chiave privata (corrispondente alla chiave pubblica da inserire nel certificato) si basa sulla verifica della CSR (Certificate Signing Request). La chiave pubblica del Richiedente, infatti, dev'essere inviata alla CA sotto forma di CSR in formato PKCS#10 (RFC 2314). Si veda anche il paragrafo "Richiesta del certificato" (a seguire nel presente documento).

3.2.2 Validazione identità delle organizzazioni

La richiesta di emissione di un certificato qualificato per persona giuridica (certificato per sigillo elettronico) è a carico della persona fisica che rappresenta la persona giuridica, la quale è identificata secondo le stesse procedure individuate per le persone fisiche (vedere il paragrafo 3.2.3).

3.2.3 Validazione delle identità individuali

Prima di procedere al rilascio del certificato richiesto, la CA deve verificare con certezza l'identità del richiedente. Per consentire una più ampia diffusione sul territorio del servizio di CA ed una

semplificazione dello stesso, ove possibile, tramite meccanismi di riconoscimento a distanza, le funzioni di identificazione e autenticazione possono essere svolte con varie modalità:

- Identificazione “de visu” (o “in presenza”) svolta direttamente dalla CA, dai soggetti esterni incaricati (RA) o da un Pubblico Ufficiale (**Modalità 1**);
- Identificazione a distanza, nel rispetto delle norme antiriciclaggio, basata sul riconoscimento effettuato da un Intermediario finanziario o da altro Soggetto Esercente Attività Finanziaria (**Modalità 2**);
- Identificazione a distanza tramite firma elettronica qualificata, ovvero basata sul riconoscimento effettuato da altro Prestatore di Servizi Fiduciari Qualificato (**Modalità 3**);
- Identificazione a distanza tramite utilizzo di un dispositivo TS-CNS, CNS o CIE, ovvero basata sul riconoscimento effettuato da corrispondente Ente Emettitore (**Modalità 4**);
- Identificazione a distanza tramite videoconferenza, svolta dalla CA o dai soggetti incaricati (**Modalità 5**);
- Identificazione a distanza tramite bonifico bancario eseguito mediante l’utilizzo di MyBank o in alternativa, tramite bonifico bancario eseguito direttamente dall’Home Banking dell’utente finale (**Modalità 6**).

Di seguito si descrivono con maggiori dettagli le varie modalità di I&A sopra richiamate. Nelle descrizioni che seguono, il termine “Richiedente” si riferisce al soggetto (persona fisica) che sta richiedendo il certificato per se o per l’organizzazione che egli/ella rappresenta.

Modalità 1

L’identificazione prevede la presenza fisica del Richiedente che dovrà essere maggiorenne, dinnanzi ad un soggetto abilitato a eseguire il riconoscimento, che provvede ad accertare la sua identità attraverso la verifica formale/sostanziale del documento d’identificazione, presentato in stato integro e in corso di validità, esibito in originale dal soggetto stesso.

Secondo quanto previsto dall’art. 35 del D.P.R. 28 Dicembre 2000, n. 445 e s.m.i., sono ammessi almeno i seguenti documenti di identità e di riconoscimento:

- Carta d’identità
- Passaporto
- Patente di guida/nautica
- Libretto di pensione
- Porto d’armi

Sono ammesse anche altri documenti di riconoscimento, purché ognuno sia munito di fotografia e di timbro, e sia stato rilasciato da un’Amministrazione dello Stato.

I Richiedenti con cittadinanza diversa da quella italiana, *ai fini dell'identificazione*, devono esibire in originale uno dei seguenti documenti di riconoscimento:

- Passaporto
- Carta d'identità italiana (se residenti in Italia)

Le operazioni d'identificazione (e relativa registrazione) dei Richiedenti sono svolte, in base al modello organizzativo di riferimento coinvolto/incaricato, da uno dei seguenti soggetti abilitati al riconoscimento:

- Direttamente dal personale preposto della CA;
- Da una terza parte denominata Centro di Registrazione Locale (CDRL) dinnanzi ad un incaricato del CDRL con incarico di Operatore di Registrazione (OdR);
- Da un soggetto terzo denominato Incaricato alla Registrazione (IR);
- Da un Pubblico Ufficiale in base a quanto disposto dalle normative che disciplinano la loro attività, ivi comprese le disposizioni di cui al D.L. 3 Maggio 1991, n. 143 e s.m.i.

I CDRL possono operare successivamente alla stipula di un mandato con la CA in cui la terza parte indica il proprio personale, che sarà definito Operatore di Registrazione (OdR), che dovrà operare nel contesto delle pratiche operative di registrazione. L'autorizzazione e successivamente la qualificazione degli OdR come abili alle operazioni di identificazione, registrazione e rilascio, avviene:

- Mediante corso di formazione della durata di 1gg. circa eseguito da personale della CA o incaricato dalla CA con adeguate ed idonee conoscenze normative/applicative per l'attività specifica
- Superamento di un verifica scritta a fine corso
- La CA conserva i moduli degli utenti dove è riportato il superamento il corso, la data del corso, chi lo ha tenuto, il dove, il programma di massima seguito durante il corso, e tutto ciò che aiuti ad avere informazioni attestanti quanto avvenuto.

A seguito della firma da parte dei rispettivi legali rappresentanti della CA e del CDRL e previa qualificazione degli OdR, la CA rende disponibili agli OdR stessi gli strumenti telematici sicuri per consentire lo svolgimento delle attività di identificazione, registrazione e rilascio dei certificati.
I privilegi di accesso agli strumenti telematici sicuri e le operazioni degli OdR sono sotto il costante controllo della CA, ed ogni operazione eseguita sugli applicativi di cui sopra viene registrata e archiviata.

Gli IR possono operare successivamente alla stipula di un mandato con la CA, direttamente o tramite nomina di un CDRL; in questo secondo caso la società terza indica il proprio personale, che sarà individuato come Incaricato di Registrazione (IR) e che dovrà operare nel contesto delle pratiche operative di registrazione.

Modalità 2

L'identificazione è demandata ad un Intermediario finanziario o altro Soggetto Esercente Attività Finanziaria che, in ottemperanza con la vigente normativa in materia di Antiriciclaggio, è obbligato al riconoscimento dei propri clienti; i dati identificativi del Richiedente, rilasciati sotto la propria responsabilità ai sensi del D.Lgs. 231/07 e raccolti dal Soggetto esercente all'atto del riconoscimento, vengono utilizzati direttamente per l'emissione dei certificati, previa (da parte del Richiedente):

- accettazione delle condizioni contrattuali per il rilascio del certificato e degli eventuali strumenti per l'apposizione della firma;
- approvazione e conferma dei dati anagrafici registrati.

Modalità 3

L'identificazione si basa sul riconoscimento (già) effettuato da altro Prestatore di Servizi Fiduciari Qualificato per il rilascio di un certificato qualificato a norma del Regolamento eIDAS. L'identità del Richiedente è accertata attraverso procedure di identificazione informatica basate sull'acquisizione di un modulo di adesione o di altro insieme di dati in forma elettronica (comunque fornito dalla CA), firmato elettronicamente con il certificato qualificato, *ancora in corso di validità*, contenuto nel dispositivo sicuro (QSCD) in possesso del Soggetto stesso.

Modalità 4

L'identificazione si basa sul riconoscimento (già) effettuato dall'Ente preposto all'emissione di uno dei seguenti strumenti di identificazione in rete:

- TS-CNS (Tessera Sanitaria – Carta Nazionale dei Servizi);
- CNS (Carta Nazionale dei Servizi);
- CIE (Carta di Identità Elettronica).

L'identità del Richiedente è accertata attraverso procedure di identificazione informatica basate sull'utilizzo dei suddetti strumenti di autenticazione on-line e presuppone che il certificato contenuto nel dispositivo sicuro, in possesso del Soggetto stesso, sia ancora in corso di validità.

Modalità 5

In tale modalità l'identificazione viene effettuata mediante l'ausilio di un sistema di videoconferenza e prevede che il Richiedente, che dev'essere maggiorenne, sia dotato di una webcam correttamente collegata ad un PC con sistema audio funzionante, e con risoluzione del video oggettivamente sufficiente a permettere l'identificazione certa.

Le operazioni d'identificazione (e relativa registrazione) dei Richiedenti sono svolte, in base al modello organizzativo di riferimento, da uno dei seguenti soggetti abilitati al riconoscimento (d'ora in poi Operatore):

- direttamente dalla CA;
- da un soggetto incaricato dalla CA, denominato Centro di Registrazione Locale (CDRL);
- da un soggetto incaricato dalla CA, denominato Incaricato alla Registrazione (IR).

L'Operatore segue particolari procedure – che per ragioni di sicurezza sono riservate – volte a garantire l'autenticità della richiesta del corso della sessione in videoconferenza. L'Operatore, tra l'altro, richiede al Richiedente di esibire un documento di riconoscimento in corso di validità tra quelli indicati nella Modalità 1. L'Operatore può escludere l'ammissibilità del documento presentato dal Richiedente se ritenuto carente delle caratteristiche elencate. L'Operatore può inoltre sospendere, o non avviare, il processo di identificazione nel caso in cui la qualità audio/video sia di scarsa qualità o ritenuta non adeguata a soddisfare i requisiti dii cui all'Art. 24 del Regolamento UE n.910/2014 o dell'art 32 comma 3, lettera a) del CAD.

Al momento dell'identificazione il Richiedente deve confermare:

- l'accettazione delle condizioni contrattuali e del trattamento dei dati personali per l'attivazione del servizio di firma e per il rilascio del certificato digitale;
- i dati identificativi ed anagrafici registrati che verranno utilizzati anche per l'emissione dei certificati.

La sessione di videoconferenza è interamente registrata (audio+video). Per garantire la tutela e la gestione dei propri dati personali in piena aderenza alla normativa applicabile in materia di protezione dei dati personali, la sessione (audio+video) viene anche cifrata con opportuno certificato di cifratura, e resa "in chiaro" su richiesta formale degli organi preposti alla vigilanza, o per ulteriori approfondimenti legati all'operatività puntuale.

I dati di registrazione, costituiti dal file audio-video e metadati strutturati in formato elettronico, sono conservati come precisato al paragrafo 5.5.

Modalità 6

In tale modalità l'identificazione viene effettuata mediante un bonifico bancario*, il quale una volta verificato, in forze alle procedure anti-riciclaggio ed altri controlli che attuano tutti gli istituti bancari, potrà rappresentare un'alternativa al riconoscimento "de visu".

(*) L'Istituto bancario da cui viene fatto il bonifico, deve essere tale da rispondere alle vigenti normative italiane per gli istituti bancari, specificatamente ai controlli inerenti e svolti in fase di apertura di conto corrente.

3.2.4 Informazioni che la CA non verifica

Alcune informazioni accessorie a procedure di attivazione e di gestione dell'account, come l'indirizzo di posta elettronica ed il numero di telefono cellulare, generalmente non sono verificate dalla CA, che non si assume responsabilità nel caso in cui tali informazioni siano fornite in modo errato o risultino comunque errate.

3.2.5 Verifica autorizzazione delle richieste

Tutte le informazioni ritenute dalla CA come imprescindibili, possono essere soggette ad ulteriore verifica da parte della CA (vedi paragrafo seguente a titolo di esempio non esaustivo, 3.2.6), la quale si riserva il diritto - qualora la documentazione presentata sia affetta da irregolarità - di rigettare la richiesta. Nel caso di rigetto della richiesta, la CA ne informa tempestivamente il Richiedente indicando la motivazione del rigetto. Il Richiedente del quale sia stata rigettata la richiesta può formulare una nuova richiesta. La CA resta comunque esente da qualsiasi responsabilità, pregiudizio e/o danno, diretto e/o indiretto che possa derivare da tale rigetto.

3.2.6 Abilitazioni professionali, ruolo e organizzazione

Ai sensi dell'art. 28 del CAD, il Titolare può ottenere, in autonomia o con il consenso dell'eventuale "Terzo Interessato" se presente, l'inserimento nel certificato di informazioni sulle proprie qualifiche, quali l'appartenenza ad ordini o collegi professionali, la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, oppure i poteri di rappresentanza. Queste informazioni, se del caso, sono inserite nell'attributo **title** del campo Subject del certificato (vedere il paragrafo 2.2).

In questo caso il Richiedente, salvo diversi accordi tra la CA e l'Ordine di appartenenza (ove applicabile), oltre alla documentazione e alle necessarie informazioni identificative, dovrà produrre anche documentazione idonea a dimostrare l'effettiva sussistenza dello specifico ruolo (o abilitazione professionale), eventualmente attestandolo mediante *autocertificazione* ai sensi dell'art. 46 del DPR n.445/2000 e s.m.i. Tale documentazione non dovrà essere anteriore di oltre 10 (dieci) giorni alla data di registrazione.

Ai sensi della Deliberazione CNIPA n. 45/2009 e s.m.i., nel caso in cui il ruolo sia *autocertificato* da parte del Richiedente, nel certificato non saranno inserite informazioni sull'organizzazione a cui potrebbe essere associato il Richiedente; la CA, in tal caso, non assume alcuna responsabilità, salvo nei casi di dolo o colpa grave, per l'inserimento del ruolo nel certificato. La denominazione ed il codice identificativo (es. Partita IVA) dell'organizzazione saranno invece inserite nel certificato se tale organizzazione ha espressamente richiesto o autorizzato il rilascio del certificato, anche senza l'esplicita indicazione di un ruolo. *In tal caso, la CA effettua un controllo sulla regolarità formale della documentazione presentata dal Richiedente.*

La CA si riserva di subordinare l'inserimento nel certificato delle informazioni che rientrano in questa categoria alla stipula di appositi accordi con i singoli enti, cui compete la gestione e tenuta degli albi, elenchi e/o registri professionali, per la disciplina delle modalità di attestazione del Ruolo del Titolare e l'adempimento di quanto previsto a loro carico in qualità di "Terzo Interessato".

3.2.7 Limiti d'uso e/o di valore nel certificato

Ai sensi dell'art. 28 del CAD e dell'Art. 13 del Regolamento eiDAS, il Titolare può richiedere alla CA l'inserimento nel certificato del limite di valore degli atti unilaterali e dei contratti per i quali tale certificato può essere usato. Questa informazione è inserita nell'estensione **QcStatements** del certificato. Il valore-limite desiderato dev'essere espresso come numero intero, e con indicazione della valuta (es. "EUR").

Ai sensi del CAD, la CA non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.

Per quanto riguarda i limiti d'uso, ai sensi dell'art. 28 del CAD, la CA garantisce il rilascio di certificati con le seguenti limitazioni d'uso (a titolo di esempio non esaustivo):

- <<I titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato. The certificate holder must use the certificate only for the purposes for which it is issued.>>
- <<Il presente certificato è valido solo per firme apposte con procedura automatica. The certificate may only be used for unattended/automatic digital signature.>>
- <<L'utilizzo del certificato è limitato ai rapporti con (indicare il soggetto). The certificate may be used only for relations with the (declare the subject).>>

Anche in questo caso, la CA non è responsabile dei danni derivanti dall'uso di un certificato che non rispetti i limiti d'uso indicati nel certificato stesso.

La richiesta di inserire limitazioni d'uso diverse da quelle sopra indicate sarà valutata caso per caso dalla CA sotto l'aspetto legale, tecnico e di interoperabilità.

In ogni caso, il testo della limitazione d'uso non può eccedere i 200 caratteri (spazi e punteggiatura inclusi) e deve essere espresso in lingua sia italiana che inglese (è ammesso il solo inglese nel caso di gruppi chiusi di utenti che utilizzano la sola lingua inglese).

3.3 Identificazione/autenticazione richieste di rinnovo

3.3.1 Identificazione e autenticazione per il rinnovo ordinario delle chiavi

La procedura seguita per il rinnovo del certificato (vedere paragrafo 4.6) è sostanzialmente identica a quella seguita per il rilascio del primo certificato. Essendo tuttavia il titolare già registrato, non è richiesta una nuova registrazione a meno che non siano intervenute variazioni dei suoi dati (variazioni che il Titolare è comunque tenuto a segnalare tempestivamente alla CA) oppure che il certificato emesso a nome del titolare, sia stato emesso precedentemente ed è alla data della richiesta di rinnovo, oltre i propri termini temporali di validità (vedere paragrafo 3.3.2).

A partire da 6 mesi prima della scadenza del certificato, il Titolare riceve (all'indirizzo di posta elettronica fornito alla CA o RA in fase di registrazione), un'email di avviso di scadenza, contenente le istruzioni per avviare la procedura di rinnovo del certificato.

La procedura di rinnovo, basata su strumenti messi a disposizione dalla CA, richiede tra l'altro che il titolare sottoscriva digitalmente un modulo di richiesta rinnovo mediante la chiave privata corrispondente al certificato da rinnovare.

3.3.2 Identificazione e autenticazione per il rinnovo delle chiavi a seguito di revoca

Dopo la revoca o la scadenza del certificato non è possibile il rinnovo del certificato: è necessaria una emissione ex novo con le modalità descritte per l'emissione il primo certificato.

3.4 Identificazione e autenticazione per le richieste di revoca

La sospensione o revoca del certificato avviene con le modalità e le procedure descritte nel paragrafo 4.9.

La revoca (o sospensione) del certificato può essere richiesta nei seguenti modi:

1. Attraverso una procedura on-line
2. Mediante inoltro alla CA (o ad una sua RA) di una richiesta formale via email (richiesta off-line).

Nel primo caso, Il Titolare si identifica inserendo il proprio codice fiscale (o altro codice identificativo personale per i cittadini stranieri non dotati di codice fiscale) e si autentica inserendo il codice riservato di emergenza ("codice utente") che gli è stato fornito in fase di registrazione o di emissione del certificato.

Nel secondo caso, è necessario che la richiesta sia sottoscritta con firma digitale o autografa del Richiedente e (nel caso di firma autografa) accompagnata da una scansione del documento di identità; nel caso di sottoscrizione digitale si accetta sia la firma elettronica avanzata sia la firma elettronica qualificata ai sensi del Regolamento eiDAS.

4 Requisiti Operativi gestione certificati

4.1 Richiesta del certificato

4.1.1 Chi può richiedere certificati

Un certificato qualificato per una persona fisica può essere richiesto dal soggetto interessato (futuro Titolare) rivolgendosi direttamente alla CA lì dove sussistano le condizioni ovvero per quei servizi di cui Nexi se ne occupa direttamente (Clienti Corporate Banche, che necessitano degli opportuni strumenti per il circuito Si.tra.d.) o ad una sua RA (CDRL) se già presente. In ogni caso, il cliente Corporate si rivolgerà all'Account Manager Nexi che lo segue, per attivare l'iter di

richiesta (Nexi alla data del presente documento, non eroga servizi direttamente a Clientela retail).

La richiesta può prevedere anche un "terzo interessato", ovvero il soggetto che acconsente all'inserimento di un ruolo nel certificato (come previsto dall'art. 32 del CAD) oppure l'organizzazione che richiede o autorizza il rilascio del certificato del titolare (cfr. la Deliberazione CNIPA n. 45/2009).

Un certificato qualificato per una persona giuridica può essere richiesto dalla persona fisica che rappresenta la persona giuridica, nelle modalità indicate già sopra.

4.1.2 Processo di richiesta e responsabilità

In generale, la richiesta di un certificato qualificato prevede sempre i seguenti passi:

- La richiesta formale del Richiedente (previo accordo Cliente Corporate – Account Nexi), con contestuale accettazione delle Condizioni Generali di contratto della CA e del presente CPS;
- L'identificazione e autenticazione (I&A) del Richiedente a cura dell'operatore di RA (può trattarsi di una RA esterna, ossia di un CDRL);
- La registrazione della richiesta sui sistemi della CA, a cura dell'operatore di RA;
- La generazione della coppia di chiavi del Richiedente (futuro Titolare); (questa operazione può avvenire anche in un momento precedente)
- L'invio della chiave pubblica alla CA nel formato previsto, a cura del Richiedente stesso oppure della RA, attraverso canali sicuri predisposti dalla CA.

I dettagli tecnico-operativi possono variare secondo la modalità di I&A (vedere il cap. 4), secondo i canali trasmissivi e strumenti informatici utilizzati per la registrazione e secondo il contesto d'uso dei certificati che vengono richiesti.

In tutti i casi, in fase di richiesta è necessario che il Richiedente:

a) Dichiari di aver preso visione del presente CPS e di averlo compreso ed accettato;

b) Si assuma esplicitamente gli obblighi previsti dalle norme vigenti e dal contratto con la CA;

c) Acconsenta al trattamento dei propri dati personali nel rispetto della normativa vigente.

Al fine di ampliare le possibilità operative, le funzioni di registrazione possono essere svolte anche da terze parti delegate, con sedi distribuite sul territorio, sulla base di appositi accordi stipulati con la CA. Tali terze parti (CDRL) operano secondo procedure concordate con la CA.

I CDRL sono responsabili nei confronti della CA della corretta e sicura identificazione dei richiedenti, nonché del trattamento dei loro dati nel pieno rispetto della normativa sulla privacy e della normativa sulla firma digitale. *La CA rimane a sua volta pienamente responsabile, nei*

confronti di chiunque si affidi ai certificati, delle operazioni di identificazione e registrazione dei richiedenti, siano esse svolte in proprio oppure dai CDRL.

4.1.2.1 Informazioni che il Richiedente deve fornire

La richiesta di registrazione ed emissione certificato viene formalizzata attraverso un "Modulo di Registrazione e Richiesta del Certificato" (il nome esatto del modulo può variare) il quale è in possesso del personale della CA, dei CDRL, o generato applicativamente nei processi online.

In seguito, per brevità, si fa riferimento al suddetto documento con il termine "modulo di richiesta".

In certi casi il modulo di richiesta viene generato in formato PDF dal sistema informativo di RA e pre-compilato coi dati anagrafici del Richiedente, quindi reso disponibile al Richiedente e all'operatore di RA per essere da entrambi sottoscritto.

Durante la registrazione, il Richiedente deve fornire alla RA almeno la seguente documentazione:

a) Il modulo di richiesta compilato in ogni sua parte obbligatoria;

b) Solo nel caso di richiesta di certificato destinato a contenere anche il ruolo o qualifica professionale del titolare (per es. avvocato, ingegnere, medico, ecc.), ovvero la carica rivestita presso organizzazioni terze, la documentazione atta a comprovare il possesso della qualifica professionale o della carica rivestita, poteri di rappresentanza, ecc.;

c) Solo nel caso di richiesta di certificato per sigillo elettronico, la documentazione necessaria a comprovare l'identità della persona giuridica (che diventerà Titolare del certificato) e quella relativa alla sussistenza dei poteri di rappresentanza della persona fisica che richiede il rilascio dello stesso.

Il modulo di richiesta dev'essere sottoscritto dal Richiedente, con firma autografa oppure elettronica, dinnanzi all'incaricato della CA (o altro operatore OdR/IR secondo il modello organizzativo adottato nel caso specifico, e secondo le modalità di I&A descritte precedentemente). Nel caso di sottoscrizione elettronica, la CA accetta i seguenti tipi di firma elettronica:

1) firma elettronica avanzata o qualificata ai sensi del Regolamento eIDAS (con certificato non necessariamente emesso dalla presente CA, ma emesso comunque da un TSP qualificato eIDAS);

2) firma elettronica avanzata apposta mediante il certificato di autenticazione presente sulla carta CNS/CRS (Carta Nazionale o Regionale dei Servizi) del Richiedente;

3) firma elettronica basata su un dato riservato conosciuto solo dal Richiedente, oltre che dalla CA (per esempio una password dinamica (OTP) che la CA invia al telefono cellulare del Richiedente (mediante SMS o con altre modalità);

4) firma elettronica apposta mediante tecniche grafometriche;

5) altre forme di firma elettronica semplice o avanzata ai sensi delle norme vigenti.

Le firme elettroniche semplici (ossia non avanzate) sono accettate solo nel caso di identificazione de visu del Richiedente da parte dell'incaricato e di firma elettronica del modulo di richiesta in presenza dell'incaricato stesso, il quale appone al modulo la propria controfirma digitale. In questo caso, il modulo include anche la dichiarazione dell'incaricato che la firma elettronica del Richiedente è avvenuta in sua presenza.
Nel caso di richiesta di un certificato qualificato per **persona fisica**, il Richiedente deve fornire le seguenti informazioni:

- Nome e cognome (*)
- Data di nascita
- Comune, provincia e stato di nascita
- Codice fiscale o analogo codice identificativo (vedere il paragrafo 3.1.5)
- Indirizzo di residenza, eventualmente all'estero
- Indirizzo di posta elettronica (*)
- Estremi del documento di riconoscimento presentato per l'identificazione: tipo, numero, ente emittente e data di rilascio dello stesso
- Numero di telefono cellulare (obbligatorio solo nel caso di certificato per firma remota e nel caso di identità accertata da un Pubblico Ufficiale)
- Eventuali abilitazioni professionali (*)
- Eventuali poteri di rappresentanza (*)
- Eventuale pseudonimo, da inserire nel certificato in luogo del nome e cognome

(*) Tutti i dati contrassegnati con l'asterisco sono inseriti nel certificato, tranne nel caso di utilizzo dello pseudonimo (vedere il paragrafo 3.1.2).

Nel caso di richiesta di un certificato qualificato per **persona giuridica**, il Richiedente (legale rappresentante o dotato di procura della persona giuridica) deve fornire le seguenti informazioni tramite PEC:

- Denominazione della persona giuridica (*)
- Paese dove ha sede la persona giuridica (*)
- Partita IVA o Codice Fiscale (*) per le organizzazioni italiane, ovvero VAT code o altro codice identificativo univoco dell'organizzazione per i Soggetti stranieri (*) (vedere il paragrafo 3.1.5)
- Nome e cognome del richiedente
- Codice fiscale o analogo codice identificativo del richiedente (vedere il paragrafo 3.1.4)

- Indirizzo di posta elettronica del richiedente (per l'invio delle comunicazioni)
- Estremi del documento di riconoscimento del richiedente: tipo, numero, ente emittente e data di rilascio dello stesso;
- Numero di telefono cellulare (obbligatorio solo nel caso di certificato per firma remota e nel caso di identità accertata da un Pubblico Ufficiale).

(*) Tutti i dati contrassegnati con l'asterisco sono inseriti nel certificato.

4.2 Elaborazione della richiesta

4.2.1 Svolgimento delle funzioni di identificazione e autenticazione

Per le modalità di svolgimento delle funzioni di I&A si rimanda ai paragrafi 3.2 e 4.1.2

Durante la fase di registrazione e richiesta del certificato, *possono* essere consegnati al Richiedente, da parte dell'operatore di RA, alcuni codici personali riservati necessari per:

- L'attivazione e sblocco del dispositivo di firma (codici PIN e PUK)
- L'attivazione della procedura di firma remota (es. password, OTP)
- Richiedere la sospensione o revoca del certificato ("codice utente")

Questi codici possono essere consegnati al Titolare in forma fisica (es. stampati su carta retinata in busta chiusa, oppure come scratch-card), separatamente dal dispositivo di firma, oppure elettronica (per es. inviati mediante SMS o e-mail).

In certi casi (es. firma remota) alcuni di questi codici possono essere impostati dal Titolare stesso. Secondo i casi, il codice di sospensione o revoca del certificato può essere fornito al Titolare anche nella fase di generazione del certificato.

4.2.2 Approvazione o rifiuto delle richieste

La CA o la terza parte delegata (RA/CDRL) può rigettare la richiesta, nel caso in cui le informazioni fornire dal Richiedente siano giudicate non affidabili, inesatte, incomplete o incoerenti; o ancora nel caso di dubbi sull'identità del Richiedente (o della persona giuridica da questi presumibilmente rappresentata) o per qualsiasi altra ragione che configuri una non conformità al presente CPS.

4.2.3 Tempi di elaborazione delle richieste

I tempi di elaborazione della richiesta, dalla registrazione del Richiedente all'emissione del certificato, dipendono dalla modalità di richiesta seguita e dalla eventuale necessità di approfondimenti sulle informazioni fornite dal Richiedente, dalla necessità di consegnare fisicamente il dispositivo di firma (ove previsto, e secondo il tipo di dispositivo) e/o di attivare lo stesso.

4.3 Emissione del certificato

4.3.1 Azioni della CA durante l'emissione del certificato

L'emissione del certificato fa seguito ad un'appropriata richiesta effettuata con la modalità ad es. descritta nel par. 3.2 e 4.1.

La generazione del certificato avviene nel rispetto dell'art. 18 del DPCM 22 febbraio 2013, del regolamento UE n. 910/2014 e degli standard ETSI di riferimento (in part. ETSI EN 319 412), utilizzando un processo articolato in diverse fasi e basato su canali di comunicazione sicuri.

Durante il processo di emissione del certificato, successivamente alla identificazione ed autenticazione (I&A) del Richiedente, la CA svolge le seguenti azioni (dove con "CA" si intende non solo il sistema di generazione certificati ma anche i sistemi e/o siti web che interfacciano le RA e/o i Richiedenti):

1) Ove previsto, attiva una procedura che genera una coppia di chiavi all'interno del dispositivo di firma del Richiedente (oppure all'interno di un HSM nel caso di richiesta certificato per firma remota) e la corrispondente CSR che viene automaticamente inviata alla CA;
2) Riceve, attraverso un canale sicuro (*cifrato ed autenticato*), la CSR del Richiedente;
3) Verifica il possesso della chiave privata, da parte del Richiedente, ed il corretto funzionamento della coppia di chiavi, mediante verifica crittografica della CSR;
4) Genera un codice identificativo univoco[1], nell'ambito del proprio database, che verrà inserito nell'attributo dnQualifier (OID: 2.5.4.46) del campo Subject del certificato (vedere il paragrafo 3.1.4);
5) Genera il certificato (*) utilizzando la chiave pubblica estratta dalla CSR e i dati identificativi del Titolare (precedentemente raccolti e memorizzati in fase di registrazione);
6) Memorizza il certificato nel proprio database, registrando l'evento nel giornale di controllo;
7) Se richiesto, pubblica il certificato nel proprio repository, registrando l'evento nel giornale di controllo;
8) invia il certificato al Titolare (o alla RA) o direttamente al dispositivo di firma (se previsto) attraverso un canale sicuro (cifrato ed autenticato); se la chiave privata del Titolare si trova su un dispositivo di firma, contestualmente si attiva una procedura che provvede ad installare il certificato all'interno del dispositivo (oppure all'interno del HSM nel caso di certificato per firma remota); viene così completata la personalizzazione del dispositivo (evento registrato nel giornale di controllo); questa procedura può inoltre provvedere, nel caso di dispositivo di firma personale (es. Smart card), a modificare i codici PIN e PUK del dispositivo impostandoli ai valori previsti;

[1] Nel caso che un medesimo richiedente possieda più certificati (ad esempio per diversi ruoli o per motivi di affidabilità del servizio), questo codice sarà diverso per ogni certificato.

9) Nel caso di chiavi di sottoscrizione generate dal titolare all'interno di HSM, associa al Titolare la credenziale di autenticazione forte (ad esempio OTP o dato biometrico) già in possesso del Titolare ed utilizzata in fase di generazione della coppia di chiavi. L'accesso alla coppia di chiavi è inoltre assoggettato alla conoscenza di uno username e di una password precedentemente scelte dal titolare stesso (nel caso dell'OTP) o alla presenza fisica del titolare dinnanzi ad un incaricato della CA (nel caso del riconoscimento basato su tecniche biometriche);

10) Se necessario (ovvero se non è già stato fatto in fase di registrazione), genera un codice riservato di emergenza da utilizzare per l'autenticazione dell'eventuale richiesta di sospensione o revoca del certificato (ai sensi dell'Art 21 del DPCM 22/2/2013);

11) Rende disponibili al Titolare i codici personali ed il codice di emergenza attraverso procedure sicure che dipendono dal tipo di dispositivo di firma utilizzato (ove previsto), dalla modalità di generazione delle chiavi del Titolare e dalla modalità di registrazione del Titolare:

    a) Nel caso di chiavi generate dalla CA, i codici personali ed il codice di emergenza sono forniti al Titolare attraverso l'invio di una busta chiusa e sigillata (o scratch-card) contenente tali informazioni;

    b) Nel caso di chiavi generate dal CDRL, i codici personali ed il codice di emergenza sono forniti al Titolare attraverso la consegna di una busta chiusa e sigillata (o scratch-card) contenente tali informazioni;

    c) Nel caso di chiavi generate, sotto il controllo del Titolare, all'interno di un HSM, sono previste due possibilità:

        – I codici personali di attivazione del dispositivo sicuro ed il codice di emergenza sono già in possesso del Titolare. La username e la password vengono impostati dal Titolare in fase di generazione della coppia di chiavi. La credenziale OTP ed il codice di emergenza sono già stati consegnati al Titolare al momento della sua identificazione. Nel caso di chiavi di sottoscrizione il cui utilizzo è assoggettato a meccanismi di autenticazione/autorizzazione di tipo biometrico (ad es. grafometria), il codice di emergenza è consegnato al titolare al momento della sua identificazione;

        – I codici personali di attivazione del dispositivo di firma non vengono modificati (cfr. il passo 8). Il codice di emergenza viene altresì notificato al titolare attraverso procedure sicure.

(*) Nel caso di chiavi di firma generate dalla CA in modalità massiva (bulk) il certificato è rilasciato in stato sospeso ed è necessario attivarlo successivamente attraverso un codice OTP temporaneo inviato al telefono cellulare del Titolare.

Qualora si verifichino condizioni che impediscano la generazione del certificato, il sistema rigetta la richiesta e segnala l'evento all'operatore di RA, ovvero al Richiedente.

4.3.2 Notifica di emissione certificato al titolare

L'emissione del certificato viene notificata all'operatore di registrazione (incaricato della CA oppure OdR) oppure direttamente al Titolare, secondo le modalità di richiesta; nel primo caso, l'operatore provvede a segnalare l'emissione al Titolare all'atto della consegna del dispositivo di firma personalizzato (ossia contenente il certificato). In alcuni casi il Titolare può ricevere una notifica via email, all'indirizzo di posta elettronica che ha fornito al momento della registrazione.

4.4 Accettazione del certificato

4.4.1 Comportamenti che costituiscono accettazione del certificato

L'uso della chiave privata costituisce accettazione del certificato. Inoltre, il certificato si considera accettato al momento della sua installazione sul dispositivo di firma del Titolare nel caso in cui il contratto lo preveda espressamente.

4.4.2 Pubblicazione del certificato da parte della CA

La pubblicazione del certificato, se espressamente richiesta, prevede i seguenti passi:

- Il certificato è pubblicato nel repository dei certificati; il momento (data/ora) della pubblicazione è attestato da un riferimento temporale affidabile;
- La pubblicazione del certificato è registrata nel giornale di controllo.

Nota: La pubblicazione del certificato non è una componente standard del servizio di CA qui descritto e non avviene "per default". Il mero consenso alla pubblicazione, da parte del richiedente, non comporta necessariamente la pubblicazione del certificato, a meno che questa non sia prevista negli accordi specifici con un particolare cliente.

4.4.3 Notifica di emissione certificato ad altri soggetti

Nessuna stipula.

4.5 Uso della coppia di chiavi e del certificato

4.5.1 Uso della chiave privata e del certificato da parte del titolare

Il Titolare del certificato di firma è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri e a custodire ed utilizzare la propria chiave privata ed il proprio dispositivo di firma (ove previsto) con la diligenza del buon padre di famiglia. Il Titolare è pertanto tenuto a proteggere la segretezza della propria chiave privata, evitando di divulgare a terzi il codice personale identificativo (es. PIN) di attivazione della stessa, provvedendo a digitarlo con modalità che non ne consentano la visione da parte di altri soggetti e conservandolo in un luogo sicuro e diverso da quello in cui è custodito il dispositivo di firma (ove previsto). La stessa cura deve essere dedicata ai dispositivi di autenticazione forte (es. generatori di codici OTP) nel caso di chiavi di firma custodite all'interno di un HSM (ossia chiavi per firma remota). La chiave privata, per cui è stato rilasciato il certificato, è strettamente personale e non può mai, per nessuna ragione, essere ceduta o concessa in uso a terzi. Verso la fine del documento, c'è un apposito paragrafo sugli obblighi del titolare, per maggiori informazioni vedere paragrafo 9.6).

4.5.2 Uso della chiave pubblica e del certificato da parte delle RP

Tutti coloro che fanno affidamento sulle informazioni contente nei certificati (in breve ci si riferisce a tali soggetti con “Relying Parties”: RP) hanno l’obbligo di verificare che il certificato non sia scaduto, sospeso o revocato. La verifica dev’essere svolta sullo stato del certificato alla data-ora rilevante per la RP, secondo il particolare contesto (per es. la data-ora corrente, o meglio la data-ora di apposizione della firma *se questa può essere accertata o inferita*).

Le RP possono esimersi dallo svolgere le verifiche sopra citate *solo* nel caso di certificato per “firma verificata”, ai sensi della Determinazione AgID n.63/2014; l’esame dell’estensione CertificatePolicies del certificato consente alla RP di determinare se si tratta di un tale tipo di certificato.

4.6 Rinnovo del certificato

Il rinnovo del certificato si applica ai certificati non ancora scaduti (e non revocati) e consiste nella generazione di una nuova coppia di chiavi (da parte del Richiedente) ed emissione di un nuovo certificato (da parte della CA) con periodo di validità normalmente uguale al periodo di validità del certificato in scadenza e con gli stessi dati identificativi del Titolare.

4.6.1 Circostanze per il rinnovo del certificato

La procedura di rinnovo deve essere avviata almeno 30 giorni prima della data di scadenza del certificato corrente. Il mancato rispetto di tale termine richiede l’avvio di procedure non standard con conseguenti possibili ritardi non quantificabili a priori.

4.6.2 Chi può richiedere il rinnovo

Il rinnovo può essere richiesto dal Titolare del certificato in scadenza (o dal suo rappresentante, nel caso in cui il Titolare sia una persona giuridica). Sono rinnovabili, sulla base del presente CPS, solo i certificati emessi dalla presente CA.

4.6.3 Elaborazione delle richieste di rinnovo

La procedura seguita per il rinnovo è molto simile a quella seguita per il rilascio del primo certificato; il soggetto Titolare (o Richiedente, nel caso di certificati emessi a persona giuridica) deve prendere comunque contatto con la RA (CDRL) di riferimento o con la CA.

I passi principali della procedura di rinnovo sono:

1) compilazione del modulo di richiesta certificato e successiva firma digitale dello stesso, a cura del Titolare o del Richiedente, tramite il certificato in scadenza che non deve essere sospeso né revocato;
2) trasmissione del suddetto modulo alla CA o alla RA (CDRL) di riferimento;
3) verifica, da parte della CA, della correttezza dei dati contenuti nel modulo e della validità della firma digitale associata;
4) generazione di una nuova coppia di chiavi del Titolare ed invio della CSR alla CA;

5) emissione di un corrispondente nuovo certificato da parte della CA;
6) invio del nuovo certificato al Titolare, da parte della CA, e sua installazione sul dispositivo di firma del Titolare (se previsto).

4.6.4 Notifica al titolare di nuova emissione del certificato

Si applica quanto descritto nel paragrafo 4.2.2

4.6.5 Comportamenti che costituiscono accettazione del certificato rinnovato

Si applica quanto descritto nel paragrafo 4.4.1.

4.6.6 Pubblicazione del certificato rinnovato da parte della CA

Si applica quanto descritto nel paragrafo 4.4.2.

4.6.7 Notifica ad altri soggetti della nuova emissione del certificato

Si applica quanto descritto nel paragrafo 4.4.3.

4.7 Rigenerazione della chiave

La rigenerazione della chiave, non intesa come rinnovo (ossia sostituzione delle chiavi prima della loro naturale scadenza) bensì applicabile a seguito della scadenza o revoca del certificato, è gestita come un'emissione ex novo.

4.8 Modifica del certificato

La modifica del certificato, non intesa come rinnovo (ossia sostituzione delle chiavi prima della loro naturale scadenza) bensì applicabile nei casi in cui cambiano le informazioni identificative del Titolare quali nome, ruolo oppure organizzazione, ecc., è gestita come un'emissione ex novo.

4.9 Sospensione e revoca del certificato

La sospensione e la revoca del certificato avvengono nel rispetto del DPCM 22/02/2013, del Regolamento eiDAS, e dell'ulteriore normativa, anche tecnica, applicabile, con le modalità e le procedure descritte di seguito.

La revoca di un certificato causa la cessazione anticipata e *definitiva* della sua validità.

La sospensione interrompe temporaneamente la validità di un certificato e consente il successivo ripristino (riattivazione) oppure la revoca definitiva dopo un periodo di tempo predefinito che può variare secondo gli accordi della CA con il Cliente.

La revoca o sospensione del certificato si concretano con l'inserimento del numero di serie del certificato in una nuova Lista dei Certificati Revocati (**CRL**), la quale viene pubblicata in modo tale che tutti gli interessati possano, scaricandola e consultandola, rilevare lo stato del certificato. La stessa informazione viene resa disponibile anche col protocollo **OCSP**.

4.9.1 Circostanze per la revoca

La CA revoca il certificato nelle seguenti circostanze:

- Richiesta esplicita da parte dal Titolare e o del suo rappresentante, per qualsiasi motivo;
- Richiesta esplicita da parte del "terzo interessato" nei casi previsti (vedere più oltre);
- Il certificato non è stato rilasciato nel rispetto del presente CPS e delle norme vigenti; (*)
- Le informazioni identificative del Titolare contenute nel certificato non sono più valide; (*)
- Cessazione anticipata del contratto tra CA e Titolare;
- Violazione degli obblighi contrattuali a carico del Titolare del certificato;
- Evidenza di errori materiali o abusi o falsificazioni in fase di registrazione; (*)
- Compromissione della segretezza della chiave privata del titolare oppure dei dati di attivazione della stessa (es. PIN, password, OTP o altri codici analoghi); (*)
- Smarrimento, furto o danneggiamento del dispositivo di firma; (*)
- Perdita non recuperabile della chiave privata; (*)
- Uso improprio del certificato da parte del Titolare;
- Richiesta da parte dell'Autorità Giudiziaria.

(*) In questi casi, quando la circostanza viene rilevata dal Titolare, il Titolare deve richiedere la revoca del certificato di propria iniziativa e nel più breve tempo possibile.

Il "terzo Interessato" può richiedere la revoca del certificato solamente quando il suo rapporto col Titolare cessa o si modifica in modo tale da invalidare le informazioni contenute nel certificato.

Per esempio, nel caso in cui il "terzo interessato" sia un'organizzazione (ente, società, associazione, etc.) che ha acquistato certificati destinati ai propri dipendenti, tale organizzazione può richiedere la revoca di un certificato quando (elenco non esaustivo):

- Siano cambiati o terminati i rapporti tra l'organizzazione e il Titolare del certificato;
- Si siano verificati casi di dolo e/o infedeltà del dipendente titolare del certificato;
- Sia decaduto il titolo o la carica od il ruolo aziendale del titolare (es. poteri di rappresentanza o qualifica professionale) indicato nel certificato stesso.

4.9.2 Chi può richiedere la revoca

La revoca del certificato può essere richiesta:

- Dal Titolare del certificato (nel caso di certificato intestato a persona fisica);
- Dalla persona fisica che rappresenta il Titolare (nel caso di certificati di sigillo);
- Dal "terzo interessato" (ai sensi dell'Art. 25 del DPCM 22/2/2013);

- Dalla CA stessa, se ne ravvisa la necessità;
- Dall'Autorità Giudiziaria.

4.9.3 Procedura per la revoca

La revoca del certificato può essere richiesta con le modalità di seguito descritte

Modalità 1: on-line

La modalità di richiesta revoca on-line, disponibile 7x24, prevede i seguenti passi:

- il Titolare si collega al sito https://cms.nexi.it/CMSNEXI/titolari/NEXI e si autentica inserendo il proprio codice fiscale (o altro analogo codice identificativo personale per i cittadini stranieri non dotati di codice fiscale italiano) ed il codice riservato di emergenza (*);
- se l'autenticazione viene superata, il sito mostra i dati salienti dei certificati attivi del Titolare e consente di selezionarne uno per richiederne la revoca (o la sospensione);
- previa conferma dell'operazione e inserimento della motivazione (opzionale), la richiesta di sospensione o revoca viene immediatamente presa in carico ed eseguita (in automatico) nel più breve tempo possibile, comunque nei tempi massimi previsti (vedere il paragrafo 4.9.5).

(*) Si tratta del "codice utente" consegnato al Titolare, generalmente, in fase di registrazione o di consegna del dispositivo di firma, ai sensi delle norme vigenti.

- **Modalità 2: off-line**

La revoca del certificato può essere richiesta anche attraverso una richiesta formale inviata alla CA mediante posta elettronica (semplice o PEC), che deve contenere:

- dati identificativi del richiedente (nome, cognome, codice fiscale, telefono, indirizzo di email, indirizzo postale, eventuale organizzazione di appartenenza e/o poteri di rappresentanza);
- dati sufficienti per l'individuazione del certificato che si chiede di revocare (per es. numero di serie e data di inizio validità);
- la motivazione della richiesta di revoca (vedere il paragrafo 4.9.1);
- data e firma del richiedente (vedere il paragrafo 3.4 per le forme di sottoscrizione accettate);
- scansione del documento di identità del richiedente, a meno che la richiesta non sia firmata digitalmente (vedere il paragrafo 3.4).

Le richieste di revoca effettuate con questa modalità non saranno prese in carico se non contengono tutte le necessarie informazioni, sopra elencate.

4.9.4 Periodo di grazia per la richiesta di revoca

Nel caso di accertata o anche solo sospetta compromissione della propria chiave privata o del proprio dispositivo di firma, il Titolare deve darne notizia alla CA (o alla RA) nel più breve tempo possibile, richiedendo la sospensione o revoca del certificato.

4.9.5 Tempo entro cui la CA deve effettuare la revoca

La richiesta di revoca viene evasa entro 24 ore dalla ricezione, a condizione che la richiesta sia fatta con le modalità previste e che non emergano dubbi sull'autenticità della stessa.

Nel caso in cui la richiesta di revoca (o di sospensione) sia motivata da sospetta o accertata compromissione della chiave privata, la CA evade la richiesta nel più breve tempo possibile.

4.9.6 Requisiti di verifica revoca per le Relying Parties

Si rimanda ai par. 4.5.2 e 9.6.4.

4.9.7 Frequenza di emissione della CRL

La CRL viene rigenerata e pubblicata periodicamente ogni 24 ore, anche in assenza di nuove richieste di sospensione o revoca. A fronte di nuove richieste di sospensione o revoca, la CRL viene rigenerata e ripubblicata nel più breve tempo possibile, normalmente entro pochi minuti e in ogni caso entro un massimo di 60 minuti.

4.9.8 Massima latenza delle CRL

Le CRL vengono pubblicate subito dopo essere state generate. La latenza tra il momento della generazione ed il momento di pubblicazione dipende dal carico degli elaboratori. Normalmente la latenza è di pochi minuti, e in ogni caso non supera i 60 minuti a meno di imprevisti.

4.9.9 Disponibilità di servizi on-line per la verifica della revoca

Oltre alla pubblicazione delle CRL, la CA rende disponibile anche un servizio di verifica on-line dello stato dei certificati basato sul protocollo OCSP (RFC 6960). Il servizio OCSP è liberamente accessibile da chiunque ne abbia necessità ed è disponibile 7x24.

4.9.10 Requisiti per la verifica on-line della revoca

Non vi sono requisiti particolari per la verifica on-line della revoca. È richiesto solamente l'utilizzo di un client OCSP conforme allo standard RFC 6960.

4.9.11 Altre forme di pubblicizzazione della revoca

Nessuna stipula.

4.9.12 Requisiti speciali nel caso di chiave compromessa

Nel caso di accertata compromissione della chiave privata o del dispositivo che la contiene (es. nel caso di furto accertato), il Titolare è tenuto a darne immediata notizia alla CA, la quale provvederà a sospendere il certificato qualora il Titolare non sia in grado di dimostrare la propria identità e/o non sia in possesso degli opportuni codici di emergenza.

4.9.13 Circostanze per la sospensione

La sospensione può avvenire nelle seguenti circostanze:

- Richiesta esplicita da parte del Titolare del certificato o del suo rappresentante (nel caso di Titolare persona giuridica);
- Richiesta di revoca non autenticata (per es. a causa del fatto che il richiedente non è in grado di fornire il necessario codice riservato: vedere il paragrafo 4.2.1);
- Richiesta esplicita da parte del "terzo interessato";
- Sono insorti dubbi sulla sicurezza del dispositivo di firma o dei dati riservati necessari per l'attivazione della chiave (es. PIN, password, OTP);
- Sono insorti dubbi sulla correttezza dei dati contenuti nel certificato.

Vedere anche i paragrafi successivi per ulteriori dettagli.

4.9.14 Chi può richiedere la sospensione

La sospensione del certificato può essere richiesta:

- dal Titolare del certificato (nel caso di Titolare persona fisica);
- dalla persona fisica che ha richiesto il certificato (nel caso di Titolare persona giuridica);
- dal "terzo Interessato" (ove applicabile);
- dalla CA stessa che agisce d'ufficio.

4.9.15 Procedura per la sospensione

La procedura per la sospensione si svolge con le stesse modalità descritte per la revoca al paragrafo 4.9.3.

4.9.16 Limiti sul periodo di sospensione

Allo scadere di un intervallo di tempo predefinito (normalmente 60 giorni) a partire dalla data di sospensione, un certificato sospeso viene automaticamente revocato dalla CA. Anche in questo caso, la CA invia notifica al Titolare dell'avvenuta revoca.

4.10 Servizi informativi sullo stato del certificato

4.10.1 Caratteristiche operative

Lo stato dei certificati (attivo, sospeso, revocato) è reso disponibile a tutti gli interessati mediante pubblicazione della Certificate Revocation List (**CRL**) col formato definito nella specifica RFC 5280. La CRL è liberamente accessibile almeno con protocollo HTTP. L'indirizzo (URL) della CRL è contenuto nell'estensione CRLDistributionPoints (CDP) del certificato stesso. I numeri di serie dei certificati revocati *restano nella CRL anche dopo la scadenza* dei certificati.

Oltre alla CRL, è disponibile anche un servizio di verifica on-line basato sul protocollo **OCSP** (On-line Certificate Status Protocol) e conforme alla specifica RFC 6960. L'indirizzo (URL) del

risponditore OCSP è contenuto nell'estensione AuthorityInformationAccess (AIA) del certificato stesso.

4.10.2 Disponibilità del servizio

L'accesso alla CRL e al servizio OCSP è disponibile in modo continuo (24 x 7).

4.10.3 Funzionalità opzionali

Nessuna stipula.

4.11 Cessazione del contratto

Il contratto tra la CA ed il titolare si intende cessato quando il certificato scade o viene revocato, salvo condizioni diverse che possono essere previste nei contratti con determinati clienti.

4.12 Deposito in garanzia e recupero della chiave privata

Nell'ambito del servizio di certificazione qui descritto, il deposito in garanzia ("key escrow") delle chiavi dei Titolari non è previsto. **Pertanto, non è possibile il recupero della chiave privata ("key recovery") del Titolare.** Per quanto riguarda le chiavi di CA, allo scopo di garantire la continuità del servizio, Nexi mantiene copie di sicurezza (backup) delle proprie chiavi private di certificazione (chiavi di CA), in forma cifrata, e le suddette copie di backup sono conservate in luogo sicuro, come verrà maggiormente illustrato ed approfondito nel capitolo 7.

5 Misure di sicurezza fisica ed operativa

5.1 Sicurezza fisica

Nexi si avvale dei servizi di gestione data center (certificati ISO/IEC 27001) erogati principalmente da un fornitore qualificato, il quale è responsabile dell'housing, della connettività ad Internet e della sicurezza fisica dei sistemi di elaborazione "core" utilizzati a supporto del servizio di CA (dove Nexi rimane comunque la CA e ne ha la responsabilità; sul fornitore di cui sopra Nexi esegue delle ispezioni di Audit a tutto campo ad intervalli di tempo periodici). Il fornitore garantisce:

- Controllo accessi fisici;
- Continuità di alimentazione elettrica;
- Sistemi antincendio ed antiallagamento;
- Ventilazione e condizionamento ottimali;
- Connettività ad Internet ridondata e di capacità almeno doppia del minimo necessario;
- Un Network Operation Center (NOC), presidiato H24 per 365 giorni/anno da personale sistemistico qualificato, che assicura il costante monitoraggio dell'infrastruttura e dei servizi ed il tempestivo intervento in caso di necessità.

5.1.1 Ubicazione e caratteristiche costruttive del sito operativo

I servizi di CA, come altri servizi fiduciari erogati da NEXI attraverso il fornitore di cui si avvale, sono basati su infrastrutture di elaborazione ridondate, progettate e realizzate in modo da garantire alta affidabilità e continuità di servizio; sono pertanto utilizzati diversi data center rispettivamente identificabili in un data center primario, uno secondario ed uno di disaster recovery.

Il data center primario è progettato e realizzato secondo le specifiche di livello Rating 4 (ex Tier 4) dello standard ANSI/TIA 942-A.

Il Data center secondario ha caratteristiche funzionali simili, ed il Data center per il disaster recovery è anch'esso progettato e realizzato secondo le specifiche di livello Rating 4 (ex Tier 4) dello standard ANSI/TIA 942-A.

I data center primario e secondario distano oltre 300km tra loro; inoltre, presso il Data center di disaster recovery, vi è inoltre vigilanza armata.

5.1.2 Accessi fisici

Presso tutti i data center sono in opera:

- un sistema di controllo accessi fisici, in modo che l'accesso all'edificio sia possibile solo a chi ne ha effettiva necessità, previa registrazione alla reception, e che l'accesso alle sale tecniche sia consentito solo agli addetti autorizzati, previa identificazione mediante badge e relativo PIN;
- sistemi antintrusione passivi quali grate, vetrate antiproiettile, porte blindate, cancelli motorizzati e sistemi antintrusione attivi quali TVCC e VMD.

5.1.3 Alimentazione elettrica e condizionamento

Tutti i data center sono dotati di:

- sistemi di alimentazione elettrica ridondati a tutti i livelli (gruppi di trasformazione, power center, UPS, gruppi elettrogeni, quadri di distribuzione, ecc.) a garanzia della continuità di alimentazione elettrica in ogni prevedibile condizione;
- sistemi di ventilazione e di condizionamento (HVAC) atti a garantire condizioni climatiche ottimali per il regolare funzionamento dei server ospitati nel data center.

5.1.4 Prevenzione e protezione dagli allagamenti

Tutti i data center sono dotati di sistemi di rilevazione allagamenti.

5.1.5 Prevenzione e protezione dagli incendi

Presso tutti i data center è in opera un sistema antincendio realizzato nel rispetto delle norme di legge e degli standard tecnici di riferimento; sensori per la rilevazione incendio sono inoltre presenti in tutti i piani dell'edificio.

5.1.6 Conservazione dei supporti di memorizzazione

Sul tema della conservazione dei supporti di memorizzazione, si applicano le procedure previste dal sistema aziendale di gestione della sicurezza delle informazioni (SGSI).

5.1.7 Smaltimento dei rifiuti

Sul tema dello smaltimento dei rifiuti, la CA applica quanto previsto dalle norme vigenti.

5.1.8 Off-site backup

In generale, i backup sono conservati presso un sito diverso da quello di origine dei dati, garantendo così la possibilità di ripristino in ogni prevedibile condizione.

5.2 Sicurezza operativa

5.2.1 Ruoli di fiducia

La struttura organizzativa è definita nel rispetto degli standard ETSI EN 319 401 e ETSI EN 319 411-1 ed in conformità al DPCM 22 febbraio 2013 e comprende pertanto sia i “ruoli di fiducia” previsti dagli standard ETSI citati che le “figure professionali” definite all’art. 38 del suddetto DCPM.

I ruoli di fiducia e le relative responsabilità sono assegnate formalmente dalla Direzione/Servizio HR mediante lettere di incarico. I requisiti per il mantenimento dell’incarico vengono rivalutati con cadenza almeno annuale e a fronte di cambiamenti nella struttura organizzativa dell’azienda. Gli incaricati possono avvalersi, per lo svolgimento delle proprie attività, di addetti e collaboratori, nel rispetto delle disposizioni generali stabilite dall’azienda.

Le funzioni e le mansioni del personale sono distribuite in modo che una sola persona non sia in grado di eludere le misure di sicurezza a tutela dei sistemi di CA; inoltre, i soggetti designati sono liberi da conflitti di interesse che potrebbero pregiudicare l’imparzialità delle attività loro assegnate.

Nexi ha definito i seguenti ruoli di fiducia / figure di responsabilità nell’ambito del servizio di CA:

- Security Officer: responsabile nel complesso per l’implementazione e la gestione delle procedure di sicurezza. Questa figura corrisponde al “Responsabile per la Sicurezza” di cui all’art. 38 DPCM 22 febbraio 2013.
- System Administrator: responsabile per l’installazione, la configurazione e il mantenimento dei sistemi della CA. Tra i System Administrator è ricompresa la figura del “Responsabile della Conduzione Tecnica dei Sistemi” di cui all’art. 38 DCPM 22 febbraio 2013.
- System Operator: responsabile per l’operatività quotidiana dei sistemi della CA.
- System Auditor: responsabile della verifica degli archivi e dei log di audit dei sistemi di CA.

- Registration & Revocation Officer: responsabile della verifica delle informazioni necessarie per l'emissione dei certificati e dell'approvazione delle richieste di certificato; responsabile inoltre per la modifica dello stato dei certificati (es. sospensione/revoca).

In conformità all'art. 38 del DPCM 22 febbraio 2013, in NEXI sono inoltre designate le seguenti figure di responsabilità in aggiunta a quelle sopra citate:

- Responsabile del servizio di certificazione e validazione temporale;
- Responsabile dei servizi tecnici e logistici;
- Responsabile delle verifiche e delle ispezioni (auditing).

5.2.2 Numero di persone richieste per lo svolgimento delle procedure

Per la gestione delle chiavi private della CA (generazione delle chiavi, backup, ripristino, cancellazione, ecc.) sono necessari almeno due soggetti designati in ruoli di fiducia ("dual control").

Le altre procedure possono essere svolte da una singola persona.

5.2.3 Identificazione ed autenticazione per ciascun ruolo

Tutti i ruoli di fiducia definiti nella sezione 6.2.1 e in generale il personale di Nexi utilizzano appropriati sistemi di identificazione e autenticazione prima dell'accesso ai sistemi informatici di Nexi.

Per quanto riguarda l'accesso fisico alle sale dati e agli armadi che contengono i sistemi di CA, l'identificazione ed autenticazione avviene tramite badge personale con PIN per il personale dell'outsourcer secondo accordi contrattuali tra Nexi e quest'ultimo, e nelle ispezioni che esegue Nexi verso l'outsourcer si fa riferimento alle normative vigenti ed alle policy di gestione accessi.

Per quanto riguarda invece gli accessi logici ai sistemi di CA, l'identificazione avviene attraverso l'utilizzo dell'account personale e relativa password oppure tramite autenticazione a due fattori (es. smartcard con PIN) per le attività o i sistemi che ne necessitano.

5.2.4 Ruoli che richiedono la separazione dei compiti

Il personale che ricopre uno dei ruoli di fiducia di cui al paragrafo 5.2.1 non può ricoprire ulteriori ruoli nell'ambito del servizio di CA.

5.3 Sicurezza del personale

5.3.1 Qualifiche, esperienze e autorizzazioni richieste

Nexi, si assicura che il personale adibito al servizio di CA sia adeguatamente competente per le mansioni assegnategli, sulla base di istruzione, formazione, addestramento, abilità ed esperienza appropriati, e che sia libero da conflitti di interesse che possono compromettere la necessaria imparzialità e il rispetto delle procedure.

Le attività previste per i team coinvolti sulla gestione del Servizio CA sono previsti all'interno del Fascicolo Regolamentare di riferimento

Nel caso di nuove assunzioni, Nexi si riserva sempre di valutare quale tipo di formazione sia necessaria in relazione alle mansioni da assegnare, alle qualifiche esistenti e all'esperienza, e provvede ove necessario all'inserimento della risorsa in un piano di formazione.

5.3.2 Controllo dei precedenti

Per la definizione della rosa dei candidati, Nexi si avvale, sia in ambito tecnico che amministrativo, tanto dei curricula ricevuti tramite gli appositi canali quanto della eventuale collaborazione di società specializzate nel recruitment. Per ogni candidato viene verificata la veridicità delle informazioni contenute nei c.v. (titoli di studio, master, diplomi, corsi di qualifica specifica, ecc.). Inoltre per tutti i candidati, una volta superata la fase di selezione, si eseguono verifiche per eventuali cariche pendenti e presenza nelle liste antiterrorismo.

5.3.3 Requisiti di formazione

Il personale addetto ai servizi di CA viene adeguatamente formato, secondo le mansioni che svolge. Anche attraverso corsi svolti da docenti esterni quando lo si reputa necessario, e un addestramento sul posto di lavoro ("training on the job").

5.3.4 Frequenza di aggiornamento della formazione

Per tutto il personale che opera nell'ambito del servizio di CA viene valutata la necessità di nuova formazione almeno una volta all'anno (oppure anticipatamente a fronte di nuovi sviluppi / servizi), in modo da garantire che tutto il personale sia sempre in grado di eseguire le proprie mansioni in modo soddisfacente e con competenza.

5.3.5 Rotazione delle mansioni

Nessuna stipula.

5.3.6 Sanzioni per le azioni non autorizzate

Nel caso di azioni non autorizzate e/o violazioni delle policy e/o delle procedure aziendali o di Gruppo, Nexi si riserva la facoltà di attivare il procedimento disciplinare previsto dal contratto collettivo e dalle policy interne, previa valutazione della natura e della gravità della violazione e del suo impatto sulle attività aziendali, se si è trattato del primo caso, se l'addetto era stato adeguatamente formato, ecc.

5.3.7 Documentazione fornita al personale

Nexi assicura, a tutto il personale impiegato nell'ambito del servizio di CA, la disponibilità di tutta la documentazione necessaria per il corretto svolgimento delle loro mansioni (questo CPS, le procedure operative, la modulistica, le guide, le policy di sicurezza, ecc.).

5.4 Gestione del giornale di controllo

Il Giornale di Controllo (Audit Log) è l'archivio sicuro nel quale vengono conservate le registrazioni degli eventi più rilevanti per la sicurezza del servizio di CA.

5.4.1 Tipi di eventi registrati

Vengono registrati almeno i seguenti eventi:

- gli eventi relativi alla gestione del ciclo di vita dei certificati, in particolare le richieste di emissione certificato e le richieste di sospensione, riattivazione e revoca;
- gli eventi relativi alla personalizzazione dei dispositivi di firma;
- gli accessi al sistema di emissione e gestione dei certificati;
- l'entrata e l'uscita dai locali protetti della CA.

Di ogni evento viene registrata:

- la tipologia
- la data
- l'ora di occorrenza
- se disponibili, altre informazioni utili ad individuare gli attori coinvolti nell'evento, i sistemi coinvolti, e l'esito delle operazioni

5.4.2 Frequenza di elaborazione del giornale di controllo

Gli eventi rilevanti vengono raccolti dai sistemi che li generano e vengono trasmessi al sistema di gestione centralizzato entro pochi minuti.

Presso il sistema di gestione del Giornale di Controllo, gli eventi vengono automaticamente classificati e memorizzati localmente in modo tale da consentirne la consultazione.

Con frequenza giornaliera, i dati locali vengono copiati sul sistema di memorizzazione a lungo termine (vedere il paragrafo 5.4.4).

5.4.3 Periodo di conservazione del giornale di controllo

Il Giornale di Controllo viene conservato per 20 anni.

5.4.4 Protezione del giornale di controllo

Il Giornale di Controllo è memorizzato su storage di tipo WORM (Write-Once-Read-Many).

5.4.5 Procedure di backup del giornale di controllo

Lo storage WORM sul quale si memorizza il Giornale di Controllo è replicato su due data center.

5.4.6 Sistema di memorizzazione del giornale di controllo

Si rimanda al par. 5.4.4

5.4.7 Notifiche in caso di rilevazione di eventi sospetti

Nessuna stipula.

5.4.8 Verifiche di vulnerabilità

Nessuna stipula.

5.5 Archiviazione delle registrazioni

5.5.1 Tipi di informazioni archiviate

Ai sensi dell'Art. 32 del CAD, la CA conserva, almeno per 20 anni, tutte le informazioni relative ai certificati qualificati emessi, dal momento della loro emissione, anche al fine di poter fornire prova della certificazione in eventuali procedimenti giudiziari. Sono inoltre conservate le informazioni relative alle richieste di sospensione o revoca dei certificati.

In particolare vengono archiviati:

- I moduli di richiesta certificato, inclusivi dell'accettazione delle condizioni di contratto della CA e degli eventuali allegati (es. documento d'identità del richiedente ove previsto, ecc.);
- I moduli di richiesta sospensione o revoca dei certificati.
- Le registrazioni audio-video in formato mp4 cifrate (descrivere il processo o rimando alla procedura)

I contratti stipulati con le Registration Authority (RA) sono conservati dalle strutture della C.A. Nexi preposte.

Per quanto riguarda i log dei sistemi di elaborazione della CA, si rimanda al paragrafo 5.4.

5.5.2 Periodo di conservazione degli archivi

Gli archivi sono conservati per almeno 20 anni, ai sensi del CAD.

5.5.3 Protezione degli archivi

Le registrazioni sono archiviate e protette con diverse modalità, a seconda che siano in origine cartacee o digitali, come descritto di seguito:

5.5.3.1 Archivi cartacei

Gli archivi sono allocati presso gli uffici preposti e non accessibili se non al personale incaricato. (si rimanda al paragrafo 5.5.6)

5.5.3.2 Archivi digitali

Al momento non è presente un archivio completo di documentazione *digitalizzata*.

5.5.4 Procedure di backup degli archivi

Una parte dei documenti cartacei sono già presenti nel sistema di conservazione digitale.

Per i documenti non ancora digitalizzati è in fase di analisi il processo di acquisizione dei dati del modulo di adesione e generazione automatica del file indice necessario alla conservazione digitale.

5.5.5 Marcatura temporale degli archivi

La marcatura temporale è utilizzata esclusivamente per la documentazione digitale prodotta attraverso procedure automatiche: in questo caso, ogni documento viene marcato temporalmente come ultimo atto del processo applicativo.

Nel caso della documentazione conservata a norma, il riferimento temporale è garantito dal processo di conservazione stesso.

5.5.6 Sistema di archiviazione

La gestione dell'archiviazione dei documenti della CA (moduli di registrazione e di revoca) avviene in modalità cartacea.

A seguire la documentazione conservata:

- Certificati di firma digitale emessi da RAO Nexi (comprendono tutti i certificati gestiti dai RAO Nexi verso i clienti finali);
- Certificati di firma digitale emessi da RAO delegati (suddivisi per cliente banca)
- Certificati di firma digitale emessi da RAO Nexi Personale Interno;
- Certificati di firma digitale automatica emessi da RAO Delegati (suddivisi per cliente Banca)
- Certificati di firma digitale automatica emessi da RAO Nexi verso Aziende
- Moduli di sospensione/revoca
- Documenti d'identità dei titolari

5.5.7 Procedura di recupero e verifica delle informazioni archiviate

Allo stato attuale le informazioni relative ai documenti della CA possono essere recuperare in qualsiasi momento accedendo all'archivio cartaceo.

5.6 Rinnovo della chiave della CA

Almeno 5 anni prima della fine del periodo di validità della corrente chiave di certificazione (chiave di CA), Nexi genera una nuova coppia di chiavi di CA e trasmette il corrispondente certificato self-signed all'AgID (in quanto organismo nazionale deputato alla supervisione dei Prestatori di Servizi Fiduciari).

Dopo l'inserimento del nuovo certificato di CA nell'elenco di fiducia (TSL) pubblicato dall'AgID, Nexi inizia a firmare i nuovi certificati e le corrispondenti CRL con la nuova chiave di CA.

5.7 Compromissione e disaster recovery

5.7.1 Procedure di gestione degli incidenti e delle compromissioni

Il Sistema aziendale prevede un processo interno di registrazione e gestione degli incident come da fascicolo regolamentare interno Nexi. In caso pertanto di malfunzionamenti sono registrati le anomalie, categorizzate in base a dei criteri di impatto/ priorità e laddove sono considerati rilevanti si procede ad informare la banca /cliente.

Nel caso in cui l'incidente, alla ricezione o nel corso della gestione, si configuri come "possibile grave incidente di sicurezza", è previsto dal Sistema aziendale una ulteriore gestione della Sicurezza delle Informazioni (SGSI) che segue specifiche procedure di gestione degli incidenti e delle compromissioni.

La gestione di un incidente di sicurezza delle informazioni è gestita dalla struttura aziendale Computer Security Incident Response Team, in seguito CSIRT, tramite una procedura in più fasi, ciascuna delle quali ha uno scopo ben preciso.

- Rilevazione e segnalazione: è la fase in cui il CSIRT ha lo scopo di intercettare gli eventi anomali tramite gli appositi strumenti di sicurezza e di raccogliere le segnalazioni da parte delle diverse fonti e punti di contatto, attraverso i canali disponibili.
- Triage: è la fase essenziale in cui il CSIRT stabilisce la corretta priorità di gestione dell'incidente, in funzione dell'impatto potenziale e della severità della minaccia.
- Risposta: è la fase in cui il CSIRT effettua le seguenti attività:
    - Identificazione delle azioni di contenimento necessarie;
    - Identificazione e ingaggio delle strutture operative preposte al contenimento dell'incidente;
    - Attivazione del CSIRT "esteso", qualora necessario;
    - Gestione della comunicazione interna, durante le varie fasi di risposta, in funzione della tipologia e della priorità dell'incidente;
    - Coordinamento e monitoraggio delle azioni effettuate per la risoluzione;
    - Risoluzione dell'incidente di sicurezza.
- Chiusura e ripristino del servizio: una volta implementate le azioni di ripristino, il CSIRT deve coordinare e/o eseguire le seguenti attività:
    - Verifica della corretta risoluzione dell'incidente, dell'eliminazione delle cause e del ripristino delle condizioni normali di esercizio;
    - Raccolta e tracciamento delle evidenze e delle attività svolte, qualora non sia già stato fatto durante la fase di risposta;
    - Chiusura del ticket;
    - Produzione della reportistica.
- Follow-up: è la fase in cui il CSIRT effettua l'analisi degli incidenti occorsi e redige un documento, ad esclusivo uso interno, sulle conoscenze acquisite da trasmettere e condividere con le strutture interessate raccordandosi inoltre con il monitoraggio degli

accessi, operazioni e sistemi, con la gestione dei malfunzionamenti e delle segnalazioni in modo da favorire l'assunzione di iniziative di prevenzione allo scopo di non incorrere in incidenti analoghi.

5.7.2 Corruzione o perdita degli elaboratori, del software e/o dei dati

Nexi si assicura che l'outsourcer implementi un piano di Business Continuity per il servizio di CA al fine di garantire che anche un caso di corruzione o perdita di uno o più elaboratori non possa arrecare alcun disservizio alla piattaforma di CA.

In particolare, tutti i componenti critici del sistema sono ridondati sia localmente nel singolo data center che tra i due data center primario e secondario. Inoltre Nexi riceve anche tramite Audit sul fornitore ad intervalli di tempo regolari, la garanzia che il fornitore implementi degli appositi piani di backup a garanzia che non ci sia perdita di software e/o dati.

5.7.3 Procedure nel caso di compromissione della chiave della CA

La chiave della CA è la singola più critica risorsa della CA e come tale è protetta da un insieme di misure di sicurezza a più strati concentrici (multi-layered), così come altre risorse critiche della CA.

Nel caso di compromissione (perdita di confidenzialità) della chiave della CA, dopo l'accertamento dell'incidente Nexi attuerà il seguente piano:

- invio di un'informativa all'organismo nazionale di supervisione (AgID);
- invio di un'informativa all'organismo di valutazione conformità (CAB);
- pubblicazione di una nota informativa in evidenza sul sito web della CA;
- invio di una nota informativa a tutte le RA e altri soggetti interessati;
- revoca di tutti i certificati emessi con la chiave compromessa.

Infine, a meno che la CA non debba essere cessata, saranno generate nuove chiavi di CA e la chiave pubblica sarà disseminata con le modalità previste indicate nel proseguo del documento.

5.7.4 Continuità operativa a fronte di un disastro

La continuità operativa a fronte di un disastro è garantita dal sito di DR a circa 300 km di distanza dai data centers primario e secondario.

5.8 Cessazione della CA o delle RA

Di seguito si descrivono le attività che saranno svolte qualora Nexi decida, per qualsiasi ragione, di cessare il proprio servizio di certificazione.

Nexi valutata e pianificata l'azione da intraprendere, prima della effettiva cessazione, provvede ad eseguire :

- Almeno 60 giorni prima della data pianificata di cessazione del servizio, sarà inviata una informativa a tutti i clienti del servizio di CA (e di altri servizi che includono i servizi di CA), nonché all'organismo di supervisione (AgID) e all'organismo di verifica della conformità (CAB);
- Con preavviso minimo di 60 giorni, sarà pubblicata in modo evidente una nota informativa sul sito web della CA, al fine di rendere disponibile l'informazione anche alle Relying Parties;
- Con preavviso minimo di 60 giorni, la CA invierà una comunicazione a tutti gli eventuali subappaltatori e terze parti delegate (RA, informandoli che alla scadenza del termine non saranno più autorizzati ad eseguire attività collegate al servizio di emissione dei certificati);
- La responsabilità della conservazione delle evidenze (richieste di certificati, giornale di controllo, ecc.) sarà trasferita ad un altro soggetto affidabile che ne possa garantire la conservazione per un tempo adeguato. Sarà inoltre trasferita a tale soggetto la responsabilità di pubblicare sul proprio sito la chiave pubblica della CA cessata;
- Sì pianificherà la distruzione delle chiavi private di certificazione nonché del materiale critto-grafico annesso che ne consente il ripristino.

Alla data di cessazione:

- Saranno distrutte (mediante cancellazione logica) le chiavi private di certificazione nonché il materiale annesso (se presente) che ne consente il ripristino, verbalizzando l'operazione.

6 Misure di sicurezza tecnica

6.1 Generazione e installazione delle chiavi

6.1.1 Generazione della coppia di chiavi

6.1.1.1 Chiavi della CA

La generazione delle chiavi di certificazione (chiavi di CA) avviene in un ambiente protetto, all'interno di un apparato crittografico sicuro, seguendo una procedura che richiede l'intervento congiunto di almeno due persone ("dual control"). L'esecuzione della procedura avviene in presenza del Responsabile delle Ispezioni Interne ed è tracciata in un verbale conservato dal Responsabile della Sicurezza della CA.

6.1.1.2 Chiavi dei Titolari

Nel caso delle chiavi che devono risiedere in un dispositivo sicuro, la coppia di chiavi viene generata all'interno del dispositivo con modalità compatibili col traguardo di sicurezza (security target) del dispositivo stesso, generalmente attraverso le librerie software fornite dal produttore del dispositivo.

Nel caso delle chiavi che non devono risiedere in un dispositivo sicuro, la coppia di chiavi viene generata mediante procedure software approvate dalla CA.

6.1.2 Consegna della chiave privata al titolare

6.1.2.1 Chiavi che devono risiedere in un dispositivo sicuro

Nel caso dei certificati relativi a chiavi che devono risiedere in un dispositivo sicuro, il dispositivo viene generalmente fornito al titolare dalla CA o dalla RA ed è già personalizzato (ossia contiene già la chiave privata ed il corrispondente certificato); pertanto, la consegna del dispositivo implica la consegna della chiave privata. La chiave privata è protetta dal PIN del dispositivo. Nel caso in cui il dispositivo non sia consegnato direttamente al titolare, ma sia spedito al titolare per posta, *i codici riservati PIN e PUK vengono trasmessi separatamente*.

Nel caso di chiavi per firma remota, la chiave privata non viene consegnata al titolare (poiché si trova all'interno di un apparato crittografico remoto gestito dalla CA) bensì posta sotto il suo esclusivo controllo attraverso un sistema di autenticazione forte (a due fattori).

6.1.2.2 Chiavi che non devono risiedere in un dispositivo remoto

In questo caso le chiavi sono generate dal titolare stesso, con procedure approvate dalla CA, e dunque non devono essere consegnate.

6.1.3 Consegna della chiave pubblica alla CA

La chiave pubblica del soggetto che richiede il certificato (futuro Titolare) viene fornita alla CA sotto forma di Certificate Signing Request (CSR) conforme allo standard PKCS#10 (RFC 2986).

6.1.4 Disseminazione della chiave pubblica della CA

La chiave pubblica della CA, necessaria per la verifica di tutti i certificati da essa emessi, viene disseminata sotto forma di certificato auto-firmato (self-signed) almeno con le seguenti modalità:

- Mediante pubblicazione sul sito web della CA;
- Mediante pubblicazione sul directory server della CA;
- Attraverso la Trust-service Status List (TSL) pubblicata sul sito dell'AgID.

6.1.5 Lunghezza delle chiavi

Per quanto riguarda la lunghezza delle chiavi, in generale Nexi applica le raccomandazioni della specifica ETSI TS 119 312 ("Electronic Signatures and Infrastructures - ESI; Cryptographic Suites").

6.1.5.1 Chiave della CA

La chiave (di tipo RSA) della CA ha una lunghezza di 4096 bit.

6.1.5.2 Chiavi dei Titolari

Le chiavi (di tipo RSA) dei Titolari devono avere una lunghezza di 2048 bit.

6.1.6 Generazione dei parametri e qualità delle chiavi

6.1.6.1 Chiave della CA

La CA usa una coppia di chiavi crittografiche generate con algoritmo RSA, con esponente pubblico pari a 65537 (esadecimale 0x10001).

6.1.6.2 Chiavi dei Titolari

Le chiavi dei Titolari devono essere generate con algoritmo RSA, con esponente pubblico pari a 65537 (esadecimale 0x10001).

6.1.7 Key Usage (estensione X.509 v3)

6.1.7.1 Chiave della CA

La chiave della CA viene utilizzata unicamente per firmare i certificati dei Titolari e per firmare le Liste dei Certificati Revocati (CRL). Pertanto, nel certificato della CA, l'estensione KeyUsage contiene:

- keyCertSign (firma certificati)
- cRLSign (firma di CRL)

6.1.7.2 Chiavi dei Titolari

Le chiavi dei titolari sono utilizzate unicamente per firma elettronica e/o sigillo elettronico, dunque per attestare la paternità e/o l'autenticità ed origine di un documento.

Pertanto, nel certificato del titolare, l'estensione KeyUsage contiene:

- nonRepudiation.

6.2 Protezione della chiave privata e sicurezza dei moduli crittografici

6.2.1 Requisiti di sicurezza dei moduli crittografici

Le chiavi private della CA sono generate ed utilizzate all'interno di apparati crittografici hardware (HSM) di elevata qualità e sicurezza, dotati di certificazione FIPS PUB 140-2 a Livello 3 e di certificazione ISO 15408 (Common Criteria) a livello EAL4 o superiore.

La chiave privata del titolare, nel caso in cui sia richiesto l'uso di un dispositivo sicuro di firma (si rimanda al par.1.4), risiede all'interno di un dispositivo crittografico hardware dotato di certificazione ISO 15408 (Common Criteria) a livello EAL4 o superiore, sulla base di un traguardo di sicurezza (Security Target) appropriato per l'uso previsto delle chiavi, nel rispetto delle norme vigenti.

6.2.2 Controllo multi-persona (N di M) della chiave privata

Nessuna stipula.

6.2.3 Deposito in garanzia della chiave privata

Non applicabile.

6.2.4 Backup della chiave privata

Allo scopo di garantire la continuità del servizio Nexi mantiene copie di sicurezza (backup) delle proprie chiavi private di certificazione (chiavi di CA), in forma cifrata.

6.2.5 Archiviazione della chiave privata

Le copie di backup delle chiavi private della CA sono conservate in luogo sicuro.

6.2.6 Trasferimento della chiave privata dal/al modulo crittografico

Le operazioni di backup e di ripristino delle chiavi di CA richiedono l'intervento congiunto di almeno due persone diverse ("dual control").

6.2.7 Memorizzazione della chiave privata sul modulo crittografico

La chiave privata della CA viene generata esclusivamente all'interno del modulo crittografico (HSM), dove essa rimane, ed è protetta dai rischi di perdita, alterazione, uso non autorizzato, esportazione non sicura, ecc. grazie ai meccanismi di sicurezza specifici del HSM (vedere anche il paragrafo 6.2.1).

6.2.8 Modalità di attivazione della chiave privata

L'attivazione della chiave privata avviene nel rispetto delle procedure previste dal fornitore del HSM ed in coerenza con la relativa certificazione di sicurezza (vedere anche il paragrafo 6.2.1).

6.2.9 Modalità di disattivazione della chiave privata

Nessuna stipula.

6.2.10 Modalità per la distruzione della chiave privata

Per la distruzione della chiave privata della CA, qualora fosse necessaria (per es. nel caso di cessazione in toto del servizio o di dismissione di una singola chiave di CA), si segue la procedura raccomandata dal fornitore del HSM.

6.2.11 Classificazione dei moduli crittografici

Vedere il paragrafo 6.2.1.

6.3 Altri aspetti di gestione delle coppie di chiavi

6.3.1 Archiviazione della chiave pubblica

Nessuna stipula.

6.3.2 Durata operativa dei certificati e delle chiavi

Ai sensi dell'art. 19 del DPCM 22/02/2013, la CA determina il termine di scadenza del certificato e il periodo di validità delle chiavi in funzione della lunghezza delle chiavi e dei servizi cui esse

sono destinate, tenendo conto anche delle raccomandazioni contenute nella specifica tecnica ETSI TS 119 312.

I certificati emessi secondo questo CPS hanno normalmente una durata di 3 anni*. La CA valuta caso per caso l'opportunità di emettere certificati con durata diversa*, tenendo conto di quanto sopra. In ogni caso, la durata massima del certificato è di 10 anni.

Il periodo di validità delle chiavi si considera coincidere col periodo di validità dei corrispondenti certificati.

6.4 Dati di attivazione

6.4.1 Generazione dei dati di attivazione

La generazione dei dati di attivazione delle chiavi avviene nel rispetto delle best practice di sicurezza nonché (ove applicabile) delle procedure raccomandate dai fornitori dei dispositivi.

6.4.2 Protezione dei dati di attivazione

6.4.2.1 Chiave della CA

I dati di attivazione delle chiavi di CA sono protetti con modalità coerenti con la policy di sicurezza aziendale e col requisito del "dual control" di cui al paragrafo 6.1.1.1.

6.4.2.2 Chiavi dei titolari

I dati di attivazione della chiave privata del titolare sono protetti, a cura del titolare stesso, in modo tale da prevenire la loro rivelazione a terzi non autorizzati. Per ulteriori importanti precisazioni a questo riguardo si rimanda all'opportuno paragrafo nel proseguo del presente documento.

6.4.3 Altri aspetti relativi ai dati di attivazione

Nessuna stipula

6.5 Sicurezza degli elaboratori

6.5.1 Requisiti di sicurezza degli elaboratori

Gli elaboratori utilizzati nell'ambito del servizi di CA utilizzano sistemi operativi di comprovata qualità e affidabilità, configurati in modo tale da impedire l'uso non autorizzato e/o con modalità non previste delle risorse (dati, applicazioni, canali di comunicazione, ecc.).

Ove possibile e laddove tale funzionalità non sia già insita nel sistema operativo, vengono installati sistemi anti-malware al fine di mitigare il rischio di "infezioni" ed attacchi di sicurezza.

Inoltre, per la stessa ragione vengono installate le "patch" di sicurezza raccomandate di volta in volta dai fornitori.

Gli elaboratori sono sottoposti ad una procedura di “hardening” finalizzata alla rimozione o disabilitazione delle funzionalità non richieste, in modo specifico su ciascun elaboratore, secondo il ruolo che esso ricopre nell’ambito della infrastruttura.

L'accesso privilegiato agli elaboratori (ossia come “Amministratore” del sistema) è limitato al personale che ne ha effettivamente necessità *e che sia stato nominato “amministratore di sistema” nel rispetto normativa vigente*.

6.5.2 Rating di sicurezza degli elaboratori

Nessuna stipula.

6.6 Sicurezza del ciclo di vita

6.6.1 Sicurezza nello sviluppo dei sistemi

Lo sviluppo dei sistemi software a supporto dei servizi fiduciari erogati da Nexi, incluso il servizio di CA, svolto da Nexi o per conto di Nexi, avviene nel rispetto del Sistema di Gestione Qualità (SGQ) aziendale, conforme alla norma UNI EN ISO 9001.

6.6.2 Sistema di gestione della sicurezza

Nexi ha definito ed utilizza un SGSI (Sistema di Gestione della Sicurezza delle Informazioni) per la C.A., conforme alla norma ISO/IEC 27001:2013, incluse quelle coinvolte nello sviluppo ed erogazione del servizio di CA. (demandato come outsourcing dei sistemi ad un fornitore esterno già Qualified TSP eIDAS compliant).

6.6.3 Gestione del ciclo di vita

Il ciclo di vita dei sistemi è soggetto alle procedure aziendali di change management.

6.7 Sicurezza di rete

L’accesso agli host on-line della CA è protetto da firewall di alta qualità che garantiscono un adeguato filtraggio delle connessioni. Prima dei firewall, una batteria di router che implementano opportune ACL (Access Control List) costituisce un’ulteriore barriera di protezione. Sui server del servizio di CA, tutte le porte di comunicazione non necessarie sono disattivate. Sono attivi esclusivamente quegli agenti che supportano i protocolli e le funzioni necessarie per il funzionamento del servizio.

Per irrobustire il filtraggio delle comunicazioni tutto il sistema di certificazione è suddiviso in un’area esterna, una interna ed una DMZ.

NEXI commissiona almeno annualmente un Vulnerability Assessment (VA) per verificare l’eventuale presenza di vulnerabilità di rete, avvalendosi di specialisti indipendenti, per i sistemi posti in outsourcing presso il fornitore che ha il facility management delle macchine.

6.8 Riferimento temporale

Il riferimento temporale usato da Nexi, col quale vengono mantenuti sincronizzati i sistemi di elaborazione della CA, è ottenuto da un dispositivo di alta precisione che garantisce una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC.

7 Profilo dei certificati, CRL, OCSP

7.1 Profilo dei certificati

I certificati emessi secondo questo CPS sono conformi alla specifica pubblica RFC 5280, basata sullo standard ITU-T X.509 v3 (ovvero ISO/IEC 9594-8:2005), nonché alle norme europee ETSI EN 319 411 ed ETSI EN 391 412 (parti 1-4).

7.1.1 Numeri di versione

La versione del certificato è v3 (2).

7.1.2 Estensioni inserite nei certificati

I certificati emessi secondo questo CPS contengono le seguenti estensioni:

- **KeyUsage** (OID 2.5.29.15) marcata come **critica**
- **CertificatePolicies** (OID 2.5.29.32)
- **CRLDistributionPoints** (OID 2.5.29.31)
- **AuthorityKeyIdentifier** (OID 2.5.29.35)
- **SubjectKeyIdentifier** (OID 2.5.29.14)
- **AuthorityInformationAccess** (OID 1.3.6.1.5.5.7.1.1)
- **qCStatements** (OID 1.3.6.1.5.5.7.1.3)

L'estensione **CertificatePolicies** contiene gli identificativi delle policy di riferimento del certificato ed eventuali qualificatori delle stesse.

L'estensione **CRLDistributionPoints** contiene l'indirizzo della **CRL** (per ulteriori informazioni si rimanda ai paragrafo 8.2 riportato di seguito).

L'estensione **AuthorityInformationAccess** contiene:

- l'indirizzo del servizio OCSP (per ulteriori informazioni si rimanda ai paragrafi 8.3 di seguito);
- l'indirizzo (URL) dal quale si può scaricare il certificato della CA emittente.

L'estensione **qCStatements** contiene i seguenti elementi:

- **QcCompliance** (OID 0.4.0.1862.1.1)
- **QcRetentionPeriod** (OID 0.4.0.1862.1.3)

- **QcSSCD** (0.4.0.1862.1.4) – presente solo nei certificati relativi a chiavi che risiedono su dispositivo sicuro
- **QcPDS** (OID 0.4.0.1862.1.5)

Nel caso in cui l'uso del certificato sia limitato alle transazioni che non superano un determinato valore, l'estensione **QcStatements** include anche l'elemento **QcLimitValue** (OID 0.4.0.1862.1.2).

7.1.3 Identificatori degli algoritmi

Tutti i certificati emessi secondo questo CPS sono firmati con algoritmo **sha256WithRSAEncryption** identificato dall'OID 1.2.840.113549.1.1.11.

7.1.4 Forme dei nomi

il campo Subject (titolare) del certificato contiene un **Distinguished Name** composto da attributi definiti nella specifica pubblica RFC 5280 ed è conforme alla norma ETSI EN 319 412 (parti 1-4).

7.1.5 Limitazioni sui nomi

Non applicabile.

7.1.6 Identificativi delle policy

Per l'elenco delle policy supportate e dei relativi identificativi (OID), si rimanda al paragrafo 1.4

7.1.7 Limitazioni sulle policy

L'estensione PolicyConstraints non è utilizzata.

7.1.8 Sintassi e significato dei qualificatori delle policy

Nella estensione **CertificatePolicies** viene sempre inserito il qualificatore **cPSuri** contenente l'indirizzo (URL) del presente CPS pubblicato sul sito web della CA.

Può inoltre essere presente il qualificatore **userNotice**, contenente un testo che descrive eventuali limitazioni d'uso del certificato.

7.1.9 Trattamento previsto delle policy critiche

Non applicabile.

7.2 Profilo delle CRL

Le CRL emesse dalla CA sono conformi alla specifica pubblica RFC 5280.

Nei campi-base, oltre ai dati obbligatori, viene inserito anche il campo **nextUpdate** (data prevista per la prossima emissione della CRL).

La CRL è firmata con algoritmo **sha256WithRSAEncryption** (OID 1.2.840.113549.1.1.11).

7.2.1 Numeri di versione

Il campo Version della CRL contiene il valore 2 come richiesto dalla specifica RFC 5280.

7.2.2 Estensioni della CRL

La CRL contiene l'estensione **cRLNumber** (numero progressivo della CRL).

Le singole voce (entry) della CRL contengono inoltre l'estensione **reasonCode** che indica la motivazione della sospensione o revoca.

7.3 Profilo OCSP

Il servizio OCSP erogato da Nexi è conforme alla specifica pubblica RFC 6960. In particolare, la risposta OCSP è conforme al profilo "pkix-ocsp-basic" (OID 1.3.6.1.5.5.7.48.1.1).

7.3.1 Numeri di versione

La versione della risposta OCSP è v1 (0).

7.3.2 Estensioni OCSP

La risposta OCSP contiene l'estensione Nonce (OID OID 1.3.6.1.5.5.7.48.1.2).

8 Verifiche di conformità

8.1 Frequenza e circostanze delle verifiche

La conformità dei servizi CA di Nexi al presente CPS, al Regolamento (UE) n.910/2014 ("eIDAS") e agli standard ETSI applicabili viene verificata su base annuale da un Organismo di Valutazione accreditato (Conformity Assessment Body, CAB).

Inoltre, sempre su base almeno annuale, viene svolta un'attività di auditing sul fornitore per i servizi di CA che tiene conto anche di aspetti inerenti la sicurezza delle informazioni, le norme applicabili sulla protezione dei dati e le politiche e procedure interne.

Nexi può demandare a società esterne lo svolgimento di audit verso soggetti che eventualmente svolgono attività per conto di Nexi nell'ambito dei servizi di CA, per esempio le RA esterne (CDRL). Per tali audit di seconda parte non vi è una cadenza predefinita a priori.

8.1.1 Verifiche sulla CA

Lo scopo delle verifiche (audit) è di accertare che le attività della CA sono conformi a tutti i requisiti degli standard ETSI EN applicabili e al regolamento eIDAS e che sono implementate in modo efficace.

8.1.2 Verifiche sulle RA

Lo scopo delle verifiche (audit) è di accertare che le attività delle RA esterne sono conformi a tutti i requisiti degli standard ETSI EN applicabili e al Regolamento eiDAS e che sono implementate in modo efficace. Nel caso delle RA esterne ciò si realizza generalmente con la conformità agli obblighi contrattuali, pertanto la verifica può riguardare in particolar modo tali aspetti.

8.2 Identità e qualificazione degli auditor

Le verifiche di conformità (audit) sulla CA sono svolte da un Organismo di Valutazione (CAB) accreditato in conformità al Regolamento (CE) n. 765/2008, attraverso personale qualificato e competente sul tema delle valutazioni di conformità, secondo la norma ETSI EN 319 403, dei Prestatori di Servizi Fiduciari e dei relativi servizi fiduciari forniti ai sensi del Regolamento eiDAS.

Eventuali audit di seconda parte vengono eseguiti sempre da organismi accreditati in conformità al Regolamento (CE) n. 765/2008.

8.3 Relazioni tra la CA e gli auditor

Gli Organismi di Valutazione (CAB) che svolgono audit sul servizio di CA, ed eventualmente sulle RA esterne che collaborano con la CA, non hanno alcuna relazione con Nexi.

L'auditor interno non appartiene alla struttura che si occupa delle attività di CA.

8.4 Argomenti coperti dalle verifiche

Le verifiche riguardano in particolare la corretta operatività della CA in riferimento alle attività di: identificazione e autenticazione dei soggetti che richiedono i certificati; gestione della relativa documentazione; emissione del certificato; gestione delle chiavi; sospensione, riattivazione e revoca dei certificati; aggiornamento della lista dei certificati revocati (CRL). Viene inoltre verificata l'implementazione delle previste misure di sicurezza fisica, tecnica ed operativa; la sicurezza del personale. Più in generale, viene verificato il rispetto del presente CPS e degli altri documenti applicabili al servizio di CA (per es. le procedure operative interne).

8.5 Azioni conseguenti alle non-conformità

Le azioni conseguenti alle eventuali non-conformità riscontrate durante gli audit (mancato soddisfacimento dei requisiti definiti nei regolamenti, standard, procedure applicabili) dipendono dalla natura e dalla severità della non-conformità rilevata, dalle regole di gestione delle non-conformità definite dall'Organismo di Valutazione e/o dalle procedure interne di gestione delle non-conformità.

8.6 Comunicazione dei risultati delle verifiche

Il risultato dell'audit svolto dall'Organismo di Valutazione (OdV) viene comunicato alla Direzione aziendale e ai responsabili della struttura organizzativa preposta all'erogazione del servizio di CA. Il risultato dell'audit viene inoltre comunicato all'Organismo nazionale di Supervisione (AgID) attraverso l'invio del report prodotto dall'OdV.

Il risultato dell'audit interno o dell'audit di seconda parte viene comunicato alla Direzione aziendale, ai responsabili della struttura organizzativa preposta all'erogazione del servizio di CA e, ove applicabile, all'entità/organizzazione esterna coinvolta.

9 Condizioni generali

9.1 Tariffe del servizio

9.1.1 Tariffe per l'emissione o rinnovo del certificato

Le tariffe massime del servizio seguono quanto indicato nel paragrafo 2.2.

Diverse condizioni economiche possono essere negoziate su base personalizzata, a seconda dei volumi richiesti.

9.1.2 Tariffe per l'accesso ai certificati

L'accesso ai certificati pubblicati è libero e gratuito.

9.1.3 Tariffe per l'accesso alle informazioni di stato dei certificati

L'accesso ai servizi informativi (CRL, OCSP) sullo stato dei certificati è libero e gratuito.

9.1.4 Tariffe per altri servizi

Nessuna stipula.

9.2 Responsabilità finanziaria

9.2.1 Copertura assicurativa

Nexi ha stipulato un'apposita assicurazione a copertura dei rischi dell'attività e degli eventuali danni derivanti dall'erogazione del servizio di certificazione.
Nel caso in cui i certificati rilasciati da Nexi prevedano limitazioni all'utilizzo - tra cui limitazioni nel valore delle transazioni per le quali il certificato è valido, ovvero limitazioni negli scopi per i quali il certificato può essere utilizzato - Nexi non sarà responsabile per i danni conseguenti ad un utilizzo non conforme.
In ogni caso, il risarcimento di danni a terzi non potrà superare l'importo massimo annuo di €10.000.000,00 (dieci milioni di Euro).

9.2.2 Altri asset

Nessuna stipula.

9.2.3 Garanzia o copertura assicurativa per gli utenti finali

Si rimanda al paragrafo 9.2.1.

9.3 Confidenzialità delle informazioni trattate

9.3.1 Ambito di applicazione delle informazioni confidenziali

Le seguenti informazioni sono trattate come confidenziali:

- In generale, tutti i dati ottenuti dai Richiedenti (futuri Titolari dei certificati) ad eccezione delle informazioni che devono essere inserite nei certificati o che per altre ragioni sono considerate non confidenziali (si veda il paragrafo successivo);
- Le richieste di emissione certificati, che siano in forma cartacea od elettronica;
- Le richieste di sospensione o revoca dei certificati, che siano in forma cartacea od elettronica;
- Le comunicazioni scambiate tra la CA e le RA, e tra la CA e i Richiedenti o Titolari, indipendentemente dal canale di comunicazione utilizzato (email, telefono, web, ecc.);
- I codici riservati dei Richiedenti o Titolari (es. credenziali di accesso a siti web della CA, dati di attivazione delle chiavi private, ecc.) qualora siano generati dalla CA o transitino attraverso i sistemi della CA;
- Le chiavi private dei Titolari qualora siano generate dalla CA;
- I log dei sistemi di elaborazione della CA;
- I contratti con le RA esterne.

9.3.2 Informazioni considerate non confidenziali

Non sono considerate confidenziali tutte le informazioni che devono essere pubbliche per rispetto delle norme di legge (si veda il par. 9.15) o degli standard tecnici di riferimento dei servizi di certificazione (es. RFC 5280) o per esplicita richiesta del Titolare. In particolare, le seguenti informazioni non sono considerate confidenziali:

- i certificati e le informazioni in essi contenute
- le liste dei certificati sospesi o revocati (CRL) le informazioni in esse contenute
- le informazioni sullo stato dei certificati erogate on-line dalla CA (es. via OCSP)
- le informazioni sui Titolari ottenibili dalla consultazione di fonti pubbliche
- le informazioni che il Titolare stesso ha chiesto alla CA di rendere pubbliche

9.3.3 Responsabilità di protezione delle informazioni confidenziali

La CA assicura che le informazioni confidenziali siano adeguatamente protette fisicamente e/o logicamente dagli accessi non autorizzati (anche se per sola lettura) nonché dal rischio di perdita a seguito di disastri.

Tutte le informazioni confidenziali sono trattate dalla CA nel rispetto delle norme applicabili, in particolare del D.lgs. 196/03 e del Regolamento (UE) 2016/679.

9.4 Trattamento e protezione dei dati personali

Nexi è titolare dei dati personali raccolti in fase di identificazione e registrazione degli utenti che richiedono certificati e si obbliga quindi a trattare tali dati con la massima riservatezza e nel rispetto di quanto previsto dal D.lgs. 196/03 nonché dal Regolamento (UE) 2016/679.

Nel caso in cui l'attività di identificazione e registrazione degli utenti avvenga presso una struttura delegata (RA), quest'ultima è qualificata come "titolare di trattamento autonomo correlato".

9.4.1 Programma sulla privacy

Per quanto riguarda la privacy, la CA rispetta le norme vigenti, in particolare il D.Lgs. 196/03 ed il Regolamento (UE) 2016/679. La protezione dei dati personali rientra nel Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di Nexi.

9.4.2 Dati che sono considerati personali

Si rimanda alla definizione di dati personali di cui alle norme vigenti, in particolare il D.Lgs. 196/03.

9.4.3 Dati che non sono considerati personali

Sono considerati dati non personali quelli che non rientrano nella definizione di cui al paragrafo precedente. Si rimanda inoltre al paragrafo 9.3.2.

9.4.4 Responsabilità di protezione dei dati personali

Nexi è il "titolare del trattamento" dei dati personali ai sensi del D.lgs. 196/03.

9.4.5 Informativa e consenso al trattamento dei dati personali

L'informativa sul trattamento dei dati personali, ai sensi del D.Lgs. 196/03, è pubblicata sul sito web della CA. La richiesta del certificato richiede il consenso, da parte del Richiedente, al trattamento dei propri dati personali da parte della CA, in coerenza con tale informativa.

9.4.6 Divulgazione dei dati a seguito di richiesta dell'autorità giudiziaria

I dati personali del Titolare potranno essere comunicati alle forze di polizia, all'autorità giudiziaria, agli organismi di informazione e sicurezza o ad altri soggetti pubblici, ai sensi del D.Lgs. 196/2003, nel caso in cui ciò sia richiesto per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

9.4.7 Altre circostanze di possibile divulgazione dei dati personali

Non applicabile.

9.5 Diritti di proprietà intellettuale

Questo CPS è proprietà intellettuale di Nexi. Tutti i diritti sono riservati.

9.6 Dichiarazioni e garanzie

9.6.1 Dichiarazioni e garanzie della CA

Con l'emissione del certificato, la CA attesta e garantisce che:

- I dati identificativi del Titolare contenuti nel certificato erano, alla data di emissione del certificato, esatti e veritieri;
- Il Titolare possedeva, alla data di emissione del certificato, la corrispondente chiave privata.

La CA si impegna a:

- Erogare il servizio di certificazione in conformità a questo CPS;
- Fornire un efficiente servizio di sospensione o revoca dei certificati;
- Fornire un servizio informativo efficiente ed affidabile sullo stato dei certificati.
- Fornire informazioni chiare e complete sui requisiti e condizioni del servizio;
- Rendere disponibile una copia di questo CPS a chiunque ne faccia richiesta;
- Trattare i dati personali conformemente alle norme vigenti.

9.6.2 Dichiarazioni e garanzie delle RA

Le RA sono tenute al pieno rispetto del contratto stipulato con la CA, in particolare (ma non solo) alla:

- Corretta e sicura I&A (identificazione a autenticazione) dei richiedenti;
- Diligente conservazione di tutte le evidenze raccolte (salvo che non sia a cura della CA, secondo lo specifico contratto stipulato con la RA), per tutto il tempo previsto dal contratto e comunque in caso di cessazione/fine contratto, le evidenze dovranno essere inviate alla C.A. che provvederà alla conservazione delle stesse, secondo le tempistiche di legge e le normative vigenti;
- Corretto utilizzo degli strumenti e canali trasmissivi che la CA mette a loro disposizione.

9.6.3 Dichiarazioni e garanzie dei Titolari

Il Titolare del certificato deve:

- Leggere ed accettare integralmente questo CPS prima di richiedere il certificato;
- Fornire alla CA informazioni esatte, complete e veritiere in fase di richiesta del certificato;
- Utilizzare la propria chiave privata unicamente per gli scopi previsti da questo CPS;

- Adottare misure di sicurezza atte a prevenire l'uso non autorizzato della propria chiave privata (per es. custodendo i dati di attivazione del proprio dispositivo di firma, come PIN o password, in luogo sicuro);
- (Per i certificati che richiedono l'uso di un dispositivo di firma) nel caso in cui generi da sé la propria coppia di chiavi, generarla all'interno di un dispositivo di firma approvato dalla CA;
- Fino alla data di scadenza o di eventuale revoca del proprio certificato, informare prontamente la CA nel caso in cui:
  - Il proprio dispositivo di firma sia andato perso, sia stato sottratto o si sia danneggiato;
  - Abbia perso il controllo esclusivo della propria chiave privata, per esempio a causa della compromissione dei dati di attivazione (PIN o password) del proprio dispositivo di firma;
  - Alcune informazioni contenute nel certificato siano inesatte o non più valide;
- Nel caso di compromissione della propria chiave privata (per es. a causa dello smarrimento del PIN del dispositivo di firma o della sua rivelazione a terzi non autorizzata), cessare immediatamente l'utilizzo della stessa ed assicurarsi che non venga più utilizzata.

Inoltre il titolare deve:

- Assicurare la confidenzialità dei codici riservati ricevuti dalla CA, per esempio i dati di attivazione dei dispositivi di firma (PIN o password), i codici riservati per l'accesso ai servizi on-line della CA (es. il codice di sospensione in emergenza), ecc.;
- Richiedere tempestivamente alla CA la sospensione del certificato nel caso di sospetta compromissione della propria chiave privata;
- Nel caso di accertata compromissione della propria chiave privata, richiedere tempestivamente alla CA la revoca del certificato;
- Prima di cominciare ad utilizzare la chiave privata, controllare attentamente che il corrispondente certificato ottenuto da NEXI abbia il profilo previsto e contenga informazioni corrette, incluse le eventuali limitazioni d'uso;
- Astenersi dall'uso della chiave privata nel caso in cui il corrispondente certificato ottenuto da Nexi presenti qualsiasi difformità rispetto alle attese.

9.6.4 Dichiarazioni e garanzie delle Relying party

Tutti coloro che devono fare affidamento sulle informazioni contente nei certificati (in breve ci si riferisce a tali soggetti con "Relying Parties": RP) hanno l'obbligo, prima di accettare un certificato, di:

- Verificare che il certificato in esame sia integro ed autentico;

- Verificare che il certificato in esame non sia sospeso, revocato o scaduto alla data di riferimento della verifica (*);
- Tenere nella debita considerazione le seguenti informazioni, se presenti nel certificato: ruolo o qualifica del titolare, organizzazione di appartenenza del titolare, limiti d'uso, limiti di valore;
- Verificare che il certificato in esame sia un certificato qualificato (ove richiesto).

(*) La verifica può essere fatta mediante consultazione della CRL pubblicata dalla CA o mediante interrogazione del servizio OCSP erogato dalla CA, agli indirizzi (URL) contenuti nei certificati stessi. La verifica può essere omessa solo nel caso di certificato per "firma verificata" (vedere il paragrafo 4.5.2).

Le RP sono inoltre tenute a conoscere il presente CPS; in particolare, per quanto concerne le limitazioni di responsabilità e le politiche di indennizzo.

Nel caso di contenzioso con Nexi, le RP non potranno avanzare alcuna pretesa se non adempiono agli obblighi sopra esposti.

9.6.5 Dichiarazioni e garanzie di altri soggetti

Ai sensi delle norme vigenti, il "Terzo Interessato" è la persona fisica o giuridica che acconsente all'inserimento di un ruolo nel certificato oppure l'organizzazione che richiede o autorizza il rilascio del certificato del titolare. Nel secondo caso, si tratta dell'organizzazione che compare nel certificato nel campo **organizationName** (se presente).

Il Terzo Interessato è tenuto a:

- Conoscere il presente CPS;
- Informare tempestivamente la CA nel caso in cui le condizioni in essere al momento della emissione del certificato (per es. il possedere, da parte del Titolare, determinate qualifiche professionali o il suo appartenere alla suddetta organizzazione o il suo ricoprire in essa determinate cariche) vengano meno, richiedendo in tal caso la revoca del certificato.

9.7 Esclusione di garanzie

La CA non ha ulteriori obblighi e non garantisce nulla più di quanto espressamente indicato in questo CPS (si rimanda al paragrafo 9.6.1) e nelle Condizioni Generali di Fornitura e/o previsto dalle norme vigenti.

9.8 Limitazioni di responsabilità

Si rimanda alle Condizioni Generali di fornitura *pubblicate sul sito web della CA*.

9.9 Indennizzi

9.9.1 Indennizzi ai contraenti

Nexi ha stipulato un'apposita assicurazione a copertura dei rischi dell'attività e degli eventuali danni derivanti dall'erogazione del servizio di certificazione (si rimanda al par. 9.2.1.)

Nel caso in cui i certificati rilasciati da Nexi prevedano limitazioni all'utilizzo - tra cui limitazioni nel valore delle transazioni per le quali il certificato è valido, ovvero limitazioni negli scopi per i quali il certificato può essere utilizzato - Nexi non sarà responsabile per i danni conseguenti ad un utilizzo non conforme.

In caso di reclami è disponibile sul portale CA Nexi (https://ca.nexi.it/Contact) la compilazione del form per la richiesta di risarcimento che sarà presa in carico dall'ufficio Reclami di Nexi per l'esecuzione della procedura di gestione come da regolamento interno.

9.9.2 Indennizzi ad NEXI

Fermo quanto previsto dalle Condizioni Generali di Fornitura, i Contraenti sono obbligati al risarcimento dei danni eventualmente sofferti da Nexi nei seguenti casi:

- Falsa dichiarazione (es. circa l'identità del Richiedente) nella richiesta del certificato;
- Omessa informazione su atti o fatti essenziali, sia per negligenza che intenzionale;
- Omessa custodia dei dati di attivazione (es. PIN) della propria chiave privata;
- Utilizzo di nomi in violazione dei diritti di proprietà intellettuale di altri soggetti.

9.10 Durata e risoluzione del contratto

9.10.1 Durata del contratto

Il Contratto ha inizio dalla data dell'adesione da parte del Contraente ed ha termine alla data di scadenza del certificato emesso da Nexi; in caso di rinnovo del certificato medesimo, la validità del Contratto è differita sino alla data di scadenza del certificato rinnovato. In ogni caso la validità del Contratto cesserà in conseguenza della revoca, per qualunque motivo effettuata, del certificato.

9.10.2 Risoluzione del contratto

Si rimanda alle Condizioni Generali pubblicate sul sito web della CA.

9.10.3 Effetti della risoluzione

Nel caso di risoluzione del contratto, il certificato del Titolare viene revocato dalla CA.

9.11 Avvisi e comunicazioni

Si rimanda al paragrafo 2.1.

9.12 Revisioni del CPS

9.12.1 Procedura per le revisioni

La CA si riserva di apportare modifiche a questo CPS in qualsiasi momento, senza preavviso, per esigenze tecniche od organizzative proprie oppure a seguito di variazioni normative. Ogni nuova versione del CPS annulla e sostituisce le versioni precedenti.

Le variazioni significative al CPS, per es. che interessano le procedure operative, il profilo dei certificati, ecc., vengono concordate con l'organismo di supervisione (AgID) prima di essere pubblicate.

9.12.2 Periodo e meccanismo di notifica

Questo CPS viene riesaminato dalla CA e, se necessario, aggiornato almeno una volta ogni anno anche in assenza di variazioni normative.

Le nuove versioni del CPS sono pubblicate sul sito web del CA.

9.12.3 Circostanze che richiedono la modifica dell'OID

Questo CPS si applica a varie policy di certificato (vedere il par. 1.4), ciascuna identificata da uno specifico OID. La revisione del CPS non implica, di per sé, la modifica di tali OID.

9.13 Risoluzione delle dispute

Qualora il Titolare o il Richiedente del certificato sia un Professionista ai sensi del D.Lgs. n.206/2005 ("Codice del Consumo"), qualsiasi controversia derivante dal Contratto sarà deferita al giudizio di un Collegio Arbitrale composto da tre membri, di cui uno nominato da Nexi, uno nominato dal Contraente, ed il terzo, che fungerà da Presidente, dai primi due.

Qualora una delle Parti non provveda a nominare il proprio Arbitro entro 20 giorni dal ricevimento della comunicazione di nomina di Arbitro inviata dall'altra Parte, tale secondo Arbitro sarà nominato, a richiesta di quest'ultima Parte, dal Presidente del Tribunale di Milano.

Analogamente, qualora i due Arbitri nominati dalle Parti non raggiungano un accordo sulla nomina del terzo Arbitro entro 20 giorni dalla nomina del secondo Arbitro, il terzo Arbitro sarà nominato dal Presidente del Tribunale di Milano su istanza della Parte più diligente.

L'arbitrato avrà natura rituale e gli Arbitri giudicheranno secondo diritto in conformità a quanto previsto dagli articoli 806 e seguenti del Codice di Procedura Civile.

La sede dell'Arbitrato sarà in Milano.

9.14 Legge applicabile

Il contratto è soggetto alla Legge Italiana ed Europea e come tale sarà interpretato ed eseguito. Per quanto non espressamente previsto dal contratto, il servizio di CA sarà regolato dalle norme vigenti.

9.15 Conformità alle norme applicabili

9.15.1 Riferimenti normativi

Si riportano di seguito i principali riferimenti normativi applicabili:

[1] Regolamento (UE) 2014/910 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (anche “eIDAS”).

[2] Decreto Legislativo 7 marzo 2005, n.82: “Codice dell’Amministrazione Digitale”, G.U. n.112 del 16 maggio 2005, e s.m.i.

[3] Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013: “Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali…”, G.U. n.117 del 21 maggio 2013.

[4] Decreto Legislativo 30 giugno 2003, n. 196: “Codice in materia di protezione dei dati personali”, G.U. n. 174 del 29 luglio 2003, e s.m.i.

[5] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

9.16 Disposizioni varie

9.16.1 Intero accordo

Il presente CPS, che può essere integrato o meno da Condizioni Generali o particolari di contratto sottoscritte specificamente dal Richiedente, costituisce la disciplina che regola l’utilizzo del certificato da parte del Titolare e regola inoltre i rapporti tra Titolare e CA. La richiesta del certificato implica l’accettazione integrale e incondizionata del presente CPS da parte del Titolare.

9.16.2 Cessione del contratto

Si rimanda alle Condizioni Generali pubblicate sul sito web della CA.

9.16.3 Separabilità

Si rimanda alle Condizioni Generali pubblicate sul sito web della CA.

9.16.4 Applicazione (spese legali e rinuncia ai diritti)

Si rimanda alle Condizioni Generali pubblicate sul sito web della CA.

9.16.5 Forza maggiore

Nexi non sarà responsabile della mancata esecuzione delle obbligazioni qui assunte qualora tale mancata esecuzione sia dovuta a cause non imputabili ad Nexi, quali - a scopo esemplificativo e senza intento limitativo - caso fortuito, disfunzioni di ordine tecnico assolutamente imprevedibili e poste al di fuori di ogni controllo, interventi dell'autorità, cause di forza maggiore, calamità naturali, scioperi anche aziendali - ivi compresi quelli presso soggetti di cui le parti si avvalgano nell'esecuzione delle attività connesse al servizio qui descritto - ed altre cause imputabili a terzi.

9.17 Altre disposizioni

9.17.1 Orari di accesso ai servizi

Per l'accesso ai servizi della CA si garantiscono gli orari riportati di seguito, a meno di situazioni ostative impreviste e nel caso dei fermi per manutenzione programmata:

Servizio	Orario di accessibilità
Registrazione utenti ed emissione certificati	Dalle ore 09:00 alle ore 17:00 dal Lunedì al Venerdì esclusi i festivi
Sospensione o revoca dei certificati	24h x 7gg
Accesso alle CRL e al servizio OCSP	24h x 7gg

Livelli di servizio specifici possono essere stipulati attraverso contratti personalizzati.

Appendice A – Chiavi di certificazione

Di seguito si elencano le chiavi di certificazione attualmente in uso da NEXI e coperte dal presente CPS. Per ogni chiave, si riportano il **Subject** DN, il **Subject Key Identifier** (SKI) e le date di inizio e fine validità. Si tratta in tutti i casi di Root CA (dunque self-signed) come previsto dalle norme Italiane.

Subject DN	CN = NEXI EU Qualified Certificates CA OU = Qualified Trust Service Provider 2.5.4.97 = VATIT-13212880150 O = NEXI S.p.A. L = Milano C = IT
Subject Key Identifier	6f 8e 5d 75 28 4a 4f e1 92 fc d4 c2 b3 12 3f f9 3a 20 c8 22
Inizio validità	25/10/2017
Fine validità	20/10/2037

Si riportano di seguito le chiavi di certificazione usate nel passato ed ancora attualmente valide

Subject DN	CN = ICBPI EU Qualified Certificates CA OU = Qualified Trust Service Provider 2.5.4.97 = VATIT-13212880150 O = ICBPI S.p.A. L = Milano C = IT
Subject Key Identifier	95 5b 7a 60 85 e6 5b 59 26 9d c6 c2 6d 55 f5 c8 34 c3 47 24
Inizio validità	29/05/2017
Fine validità	24/05/2037

Subject DN	CN = Certification Authority ICBPI OU = Qualified Certification Service Provider O = ICBPI S.p.A./13212880150 C = IT
Subject Key Identifier	74 a5 23 f0 c1 50 a2 28 66 c8 44 d9 46 83 34 42 a1 10 05 af
Inizio validità	21/12/2012
Fine validità	21/12/2037

FINE DOCUMENTO