Certificati Qualificati

Manuale Operativo / Certification Practice Statement e Certificate Policy

Versione 1.11

(06 dicembre 2024)

Andrea Sassetti
Firmato digitalmente il 06/12/2024 15:30:05 CET

STORIA DELLE MODIFICHE APPORTATE

Versione	Data	Modifiche
1.0	9 maggio 2017	Prima versione del documento.
1.1	20 novembre 2017	P.1.1 – inseriti riferimenti a certificatori sostituiti
		P.1.5.1 – inseriti riferimenti a versione documento e responsabile CPS
		P.9.1.1 – inserito url sito web certificatore
		P.9.6.1 e 9.6.3 - specificati obblighi art. 32 CAD
		P.9.17.2 – inserito paragrafo con raccomandazioni sui formati dei documenti P.9.8 – esplicitate le limitazioni di responsabilità
		Appendice A – aggiornati riferimenti a chiavi di certificazione
		Appendice B – inserita nuova appendice contenente le modalità operative per la generazione e la verifica delle firme
1.2	26 aprile 2018	Tutto il documento – Aggiornato logo P.1.2 – modificato link sito AgID P.9.8 – modificata formula limitazioni di responsabilità P.9.16.3 – corretto refuso nel titolo del paragrafo
		P.1.4 – Aggiornata la disponibilità di alcune policy
		Appendice A – Aggiunta nuova chiave di CA per Modello ATe
1.3	28 febbraio 2019	P.1.3.1 aggiornati riferimenti Legale Rappresentante
		P.3.2.3 inserita modalità di identificazione a distanza tramite schema e-ID nazionale (Modalità 4) e dettagliata Modalità 2
		P.3.2.5.2 inseriti dettagli su OID 1.3.76.16.5
		P.4.9.3 modificato link per procedura per la revoca (modalità online), inserito indirizzo mail per invio modalità offline e specificato link online con moduli richieste di revoca
1.4	23 maggio 2019	P.1.3.1 aggiornati riferimenti Legale Rappresentante
		P.1.1, p.1.4, p.1.6, p.1.7 (aggiunto), cap.3, p.4.1.2, p.6.1.7.2, p.6.3.2, p.7.1, p.7.1.2, p.7.1.6, Appendice A: varie integrazioni e precisazioni relative ai certificati per l'autenticazione di siti web (QWAC) P.9.4, 9.6.1 Aggiornati riferimenti trattamento dati personali. P.9.13 indicato Foro competente
1.5	16 dicembre 2019	P.1.6 e p.3.2.3 – aggiornato acronimo e definizione IR
		P. 4.3.1 – aggiunte modalità di invio codici personali e di emergenza
		P.3.2.5.1 e 9.8 – rimosse le limitazioni di responsabilità relativamente alla colpa lieve
		P.3.1.2, 3.2.5.1, 4.1.1, 4.1.2.1, 4.8, 4.9.1, 9.6.4 e 9.6.5 – sostituito il termine 'ruolo' con 'qualifica' nei riferimenti a certificati che contengono informazioni sulla qualifica professionale o la carica rivestita dal Titolare presso organizzazioni terze
		P.3.2.5.1 e 4.1.1 – sostituiti riferimenti Deliberazione CNIPA n. 45/2009 (abrogata) P.7.1 – inserite indicazioni sull'applicazione delle raccomandazioni emanate dall'Agenzia con Det. AgID n.121/2019
		P.4.9.16 – modificato limite sul periodo di sospensione
		P.4.3.1 – aggiornata la lista dei canali di trasmissione dei codici personali e del codice di emergenza

		P.1.3.2 e 4.1.2 – riformulata la responsabilità di I&A dei Richiedenti
		P.4.9.3 – precisate le modalità di consegna del codice utente
		Aggiornata lista dei redattori e dei verificatori del presente documento
		P.1.3.1 – modificato il ruolo del legale rappresentante
		P.5.1.1 – aggiornata la certificazione dei data center
		P.5.2.1 – inserita la figura autonoma di "Responsabile della Sicurezza"
		P.8.2 – rimosso l'inciso sull'identità degli auditor di seconda parte
1.6	28 febbraio 2020	P.4.1.2.1 – miglioramenti nella descrizione per la compilazione del modulo richiesta
		P. 5.3.2 – eliminati i riferimenti ai carichi pendenti per i dipendenti
		P. 9.8 – aggiunte ulteriori precisazioni sulla responsabilità della CA
1.7	31 luglio 2020	P.1.4 e 7 – Aggiornata la descrizione delle policy OID tenendo anche conto della "Firma con SPID"
		P. 3.1.2 – Aggiunta una specifica per il SAN a seguito della Determinazione n. 157/2020
		P. 3.2.3 – Aggiunta la modalità 6 per consentire l'identificazione mediante datore di lavoro. Spostati alcuni paragrafi dalla modalità 1 al par. 3.2.3. Aggiornata la lista dei documenti di riconoscimento accettabili. Aggiunta sub "Modalità 6" la descrizione del nuovo modello di identificazione. Aggiunto il riferimento all'allegato "Documenti di riconoscimento consentiti".
		P. 6.1.7.2. – Aggiunta specifica per la "Firma con SPID"
		P. 7.1.2 – Aggiunte specifiche conseguenti alla Determinazione n. 157/2020
		Aggiunta lista allegati con "Documenti di riconoscimento consentiti"
1.8	3 marzo 2021	P. 1.6: Aggiunti i paragrafi relativi alle definizioni ed acronimi 1.6.1 e 1.6.2; P. 3.2.3: inserita una descrizione ulteriore per l'autenticazione nella modalità 2; P.4.1.2.1: piccole modifiche; Aggiunte le appendici C e D.
1.9	16 marzo 2023	P.1.3.1: modificato indirizzo email generale
		P. 1.4: introdotto riferimento articoli Reg. eIDAS; eliminata nota a fine tabella.
		P.3.1.2: introdotta interpretazione attributo CountryName (certificati di sigillo)
		P.3.1.5.: introdotti chiarimenti a seguito Avviso n.18/2021 AgID
		P.3.2.3: modificato passaggio relativo alla Modalità 2; piccola modifica alla Modalità 5
		P. 4.1.2.1: modifica casistiche di accettazione firme elettroniche e eliminazione obbligatorietà indirizzo posta elettronica
		P 4.2.1: aggiunta eccezione Appendice D
		P. 4.3.1: modifica al punto 11) relativo all'invio di codici personali e codice di emergenza
		P. 4.6.1, 4.6.2, 4.6.3: introdotti riferimenti al rinnovo tacito del certificato;

		P. 4.9.1: introdotti chiarimenti in caso di perdita della certificazione del QSCD.
		P. 6.7: aggiornamento periodicità VA.
		P. 8.6: piccola correzione acronimo Organismo di Vigilanza (CAB).
		P. 8 Appendice D: modificato ultimo passaggio del paragrafo relativo al limite d'uso per la sottoscrizione dei documenti
1.10	5 aprile 2024	P. 1.6.2 Introdotto nuovo acronimo per Operatore Supervisore
		P. 3.2.3 Specificato il ruolo di verifica degli Operatori Supervisore per la Modalità 1 di identificazione ("de-visu" o "in presenza").
		P. 4.2.2 Specificato il ruolo di verifica da parte degli Operatori Supervisore.
		Correzione di alcuni refusi nei sommari dell'Appendice C e dell'Appendice D.
1.11	06 dicembre 2024	P 3.1.2 Introdotta interpretazione dell'attributo *CountryName* per certificati di firma.
		P 3.1.5 Correzione refusi.
		P 3.4 Allineamento delle definizioni.
		P 4.1.2.1 Integrazioni delle informazioni per la richiesta del servizio.
		P 4.1.2.1 Semplificazione dei dati obbligatori per la richiesta del servizio.
		P 4.2 Integrazione del paragrafo.
		P 4.3.1 Integrazione per emissione in modalità *bulk,* revisione del bullet 9) per maggiore chiarezza sulle modalità di autenticazione a due fattori del Titolare.
		P 4.5.1 Integrazione per maggiore chiarezza ed esaustività del paragrafo.
		P 4.9.1 Integrazione modalità di sospensione e revoca in caso di richiesta del Terzo Interessato.
		P 4.9.3 Modifica delle informazioni richieste in caso di sospensione e revoca dei certificati e aggiornamento del link per la sospensione e revoca online.
		P. 4.9.13 Integrazione del paragrafo.
		P. 5.1, 5.2, 5.3, 5.5, 5.7, 6.5, 6.6, 6.7 riformulazione delle informazioni per garantire sicurezza e riservatezza di dati sensibili.
		P. 5.8 Introdotta specifica per l'informazione sullo stato dei certificati in caso di cessazione della CA.
		P. 7.1 Correzione dell'OID relativi ai certificati QWAC utilizzati in ambito PSD2.

Approvato da:	Andrea Sassetti

SOMMARIO

1. INTRODUZIONE

1.1 Quadro generale

Aruba PEC S.p.A., un Prestatore di Servizi Fiduciari (Trust Service Provider) accreditato presso l'AgID sino dal 2007, eroga servizi qualificati di certificazione di chiavi pubbliche, oltre a diversi altri servizi fiduciari (per maggiori informazioni si rimanda al sito web https://www.pec.it).

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** (**CA**), ed è firmato digitalmente dalla CA.

Aruba PEC svolge il ruolo di CA nell'ambito del servizio qui descritto. Nell'ambito di questo documento, i termini "CA", "Prestatore" (di Servizi Fiduciari) e "Certificatore" sono utilizzati come sinonimi e fanno tutti riferimento ad Aruba PEC, inteso come il soggetto erogatore del servizio di CA, e/o ai sistemi informativi utilizzati da Aruba PEC 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** (**CPS**).

Questo documento è il CPS di Aruba PEC 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").

Aruba PEC S.p.A. è il CSP sostitutivo e conservatore della documentazione del seguente CSP non più attivo:

- Trust Italia S.p.A. (cessato il 20/02/2008)

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

Per quanto riguarda i certificati qualificati per siti web (Qualified Website Authentication Certificates, in sigla QWAC), Aruba PEC rispetta la versione corrente delle "Guidelines for Issuance and Management of Extended Validation Certificates" del CA/Browser Forum, pubblicata su http://www.cabforum.org. In caso di conflitto tra il presente CPS e tali Linee Guida, queste ultime hanno la precedenza.

1.2 Nome e Identificativo del documento

La versione del presente CPS è indicata sul frontespizio.

La versione vigente del CPS è pubblicata sul sito web della CA (https://www.pec.it) e sul sito web dell'AgID (http://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 Aruba PEC S.p.A. Di seguito i dati identificativi della società:

Denominazione sociale:	**Aruba PEC S.p.A.**
Indirizzo della sede legale ed operativa:	**Via S. Clemente, 53** **24036 Ponte San Pietro (BG)**
Legale rappresentante:	**Giorgio Cecconi** (Presidente del Consiglio di Amministrazione)
N° di iscrizione al Registro Imprese di Bergamo:	**01879020517 (REA n. 445886)**
Codice Fiscale e Partita IVA:	**01879020517**
N° di telefono (centralino):	**+39 0575 050.350**
ISO Object Identifier (OID):	**1.3.6.1.4.1.29741**
Sito web principale:	**https://www.pec.it**
E-mail (generale):	**CPS-requests@ca.arubapec.it**

Come previsto dalle norme italiane, la PKI realizzata da Aruba PEC 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 Aruba PEC 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, ma non necessariamente, 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 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 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 e sigilli elettronici 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** oppure per l'**autenticazione di siti web**, secondo il tipo di certificato considerato. 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) e che la firma venga apposta con una procedura remota o meno. Nel caso dei QSCD, ci si riferisce a quelli certificati ai sensi degli artt. 31 e 39 del Regolamento eIDAS, o per i quali si applicano le disposizioni transitorie cui l'art. 51 eIDAS.
Di seguito sono elencati gli **OID** (**Object Identifier**) **delle policy supportate** da questo CPS e, per ciascuna, la policy di riferimento definita nella norma ETSI EN 319 411-2.

Policy OID specificato nei certificati emessi da Aruba PEC	Policy di riferimento ETSI EN 319 411-2	Persona	Chiavi su QSCD	Firma Remota
1.3.6.1.4.1.29741.1.7.1	**QCP-n-qscd**	Fisica	SI	NO
1.3.6.1.4.1.29741.1.7.2	**QCP-n-qscd**	Fisica	SI	SI
1.3.6.1.4.1.29741.1.7.3	**QCP-n**	Fisica	NO	NO
1.3.6.1.4.1.29741.1.7.4	**QCP-n**	Fisica	NO	SI
1.3.6.1.4.1.29741.1.7.5	**QCP-l-qscd**	Giuridica	SI	NO
1.3.6.1.4.1.29741.1.7.6	**QCP-l-qscd**	Giuridica	SI	SI
1.3.6.1.4.1.29741.1.7.7	**QCP-l**	Giuridica	NO	NO
1.3.6.1.4.1.29741.1.7.8	**QCP-l**	Giuridica	NO	SI
1.3.6.1.4.1.29741.1.7.9	**QCP-w**	Giuridica	NO	NO

Inoltre, ulteriori OID, possono essere indicati nelle Appendici al presente documento.

I certificati contengono normalmente i seguenti Policy OID, fermo restando quanto previsto al cap. 7:

- il Policy OID proprietario di Aruba PEC;
- il Policy OID standard definito nella norma ETSI EN 319 411-2;
- il Policy OID con valore agIDcert (OID **1.3.76.16.6**) che dichiara la piena applicazione delle raccomandazioni emanate dall'AgID per la generazione di certificati elettronici qualificati (DT DG n. 121 del 17 maggio 2019 e s.m.i.).

Può essere presente un ulteriore Policy OID:

- nel caso dei certificati per chiavi di "firma digitale verificata" ai sensi della Determinazione AgID n.63/2014 (in questo caso, il Policy OID aggiuntivo è **1.3.76.16.3**);
- nel caso dei certificati di sigillo per la "Firma con SPID" ai sensi della Determinazione AgID n.157/2020 (in questo caso, il Policy OID aggiuntivo è **1.3.76.16.4.11** = "spidSignature").

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 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);
- i certificati di sigillo per la "Firma con SPID" contengono la specifica limitazione d'uso stabilita nella Determinazione AgID n.157/2020.

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 Versione del CPS e organizzazione responsabile

Questo documento è la versione 1.11 del CPS di Aruba PEC S.p.A. e viene redatto, pubblicato ed aggiornato da Aruba PEC S.p.A.

Il soggetto responsabile del presente manuale operativo all'interno di Aruba PEC è:

Andrea Sassetti
Direttore dei Servizi di certificazione
Aruba PEC S.p.A.

Richieste di informazioni o chiarimenti sul presente CPS e/o sulle policy di certificato (CP) qui definite possono essere inviate tramite posta elettronica all'indirizzo CPS-requests@ca.arubapec.it.

1.5.2 Soggetti approvatori

Questo CPS è approvato dalla Direzione dei servizi di CA, previa verifica da parte delle funzioni aziendali interessate e tenendo conto di quanto indicato al §6.1 della norma ETSI EN 319 401.

1.5.3 Procedura di approvazione

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 e acronimi

1.6.1 Definizioni

Agenzia per l'Italia Digitale (AgID)	Ente Nazionale per la digitalizzazione della Pubblica Amministrazione (già DIGITPA e CNIPA).
Certificato elettronico qualificato di sigillo	Un certificato di sigillo elettronico che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato III del Regolamento eIDAS.
Certificato qualificato di firma elettronica	Un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I del Regolamento eIDAS.
Chiave privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dal Titolare, mediante la quale si appone la firma elettronica qualificata sul documento informatico.
Chiave pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma elettronica qualificata apposta sul documento informatico dal Titolare.
Codice di emergenza	Codice di sicurezza consegnato al Titolare per richiedere la sospensione o la revoca del certificato.
Firma digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al Titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Firma elettronica	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare.
Firma elettronica qualificata	Una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche.
OTP - One Time Password	Una One-Time Password (password usata una sola volta) è una password che è valida solo per una singola transazione. L'OTP viene generata e resa disponibile al Titolare in un momento immediatamente antecedente all'apposizione della firma elettronica qualificata. Può essere basato su dispositivi hardware o su procedure software.
Revoca o sospensione di un certificato	È l'operazione con cui la CA annulla la validità del certificato prima della naturale scadenza.
Richiedente	E' il soggetto che sta richiedendo ad Aruba PEC S.p.A. l'emissione di un certificato.
Sigillo elettronico qualificato	Un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici
Titolare	È il soggetto intestatario del servizio.

1.6.2 Acronimi

CA	Certification Authority
CAB	Conformity Assessment Body
CAD	Codice dell'Amministrazione Digitale (D.lgs. n.82/2005)
CDRL	Centro di Registrazione Locale
CP	Certificate Policy
CRL	Certificate Revocation List
CSP	Certification Practice Statement
FQDN	Fully-Qualified Domain Name
HSM	Hardware Security Module
HTTP	Hyper-Text Transfer Protocol
I&A	Identificazione e Autorizzazione
IR	Incaricato al Riconoscimento
OdR	Operatore di Registrazione
OS	Operatore Supervisore
OCSP	On-line Certificate Status Protocol
OID	Object IDentifier
PKI	Public Key Infrastructure
PSD2	Payment Services Directive (Direttiva (EU) 2015/2366)
QSCD	Qualified Signature-Creation Device
QSealC	Qualified Electronic Seal Certificate
QWAC	Qualified Website Authentication Certificate
RA	Registration Authority
TLS	Transport Layer Security
TSL	Trust-service Status List
TSP	Trust Service Provider

1.7 Riferimenti normativi

[BR] CA/Browser Forum, "Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates". (https://cabforum.org/baseline-requirements-documents/)

[EVGL] CA/Browser Forum, "Guidelines For The Issuance And Management Of Extended Validation Certificates". (https://cabforum.org/extended-validation/)

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 Aruba PEC è rappresentato principalmente sul sito web della CA (https://www.pec.it) ed altri siti da esso richiamati. Per alcune esigenze può essere utilizzato anche un directory server.

La CA gestisce in proprio il repository e ne è direttamente responsabile.

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

2.2 Informazioni pubblicate sui certificati

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

- Certification Practice Statement (CPS)
- PKI Disclosure Statement (PDS)
- Condizioni Generali di Contratto
- Certificati di CA
- Modulistica

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

2.3 Tempi o 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 §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 Aruba PEC.

3. IDENTIFICAZIONE E AUTENTICAZIONE (I&A)

3.1 Denominazione dei titolari

3.1.1 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 319 412-4: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates.
- ETSI EN 319 412-5: Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements.

3.1.2 Necessità che il nome sia significativo

Nel campo Subject sono inseriti dati chiaramente identificativi del Titolare (persona fisica o giuridica) del certificato, salvo quanto precisato nel §3.1.3.

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)

L'attributo countryName (OID: 2.5.4.6), valorizzato in conformità allo standard ISO 3166-1 Alpha-2, specifica il Paese in cui il serialNumber (OID: 2.5.4.5) della persona fisica è registrato.

Può inoltre essere presente l'attributo title (OID 2.5.4.12), usato per specificare il titolo o qualifica professionale del Titolare.

Nel caso di certificati emessi ad una persona fisica associata ad un'organizzazione, il campo Subject contiene sempre anche gli attributi seguenti, in aggiunta a quelli sopraindicati:

- organizationName (OID: 2.5.4.10)
- organizationIdentifier (OID: 2.5.4.97)

Se è presente anche l'attributo title, quest'ultimo può indicare la qualifica, le mansioni o la carica societaria ricoperta dal Titolare nell'ambito dell'organizzazione.

Nei certificati emessi a persona giuridica, il campo Subject contiene almeno gli attributi seguenti:

- countryName (OID: 2.5.4.6)
- organizationName (OID: 2.5.4.10)
- organizationIdentifier (OID: 2.5.4.97)
- commonName (OID: 2.5.4.3)

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

Inoltre, per i certificati di tipo QWAC, devono essere soddisfatti tutti i requisiti stabiliti nei [BR] e nelle [EVGL]. In particolare, i certificati devono contenere uno o più elementi nell'estensione Subject Alternative Name (SAN), nella quale ciascun elemento dev'essere un nome di dominio completo (FQDN).

Nei certificati di sigillo da utilizzarsi per le finalità di cui alla Determinazione AgID n.157/2020, è sempre presente anche l'estensione Subject Alternative Name (SAN), popolata come previsto dalla suddetta determinazione.

Nei certificati di sigillo, l'attributo countryName (OID: 2.5.4.6) specifica il Paese in cui è stabilita la persona giuridica (sede legale).

3.1.3 Anonimato e pseudonimia dei titolari

Nel caso in cui le 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.

Gli pseudonimi non sono ammessi e per quelli di tipo QWAC i quali per conformità ai [BR] e alle [EVGL] devono contenere il nome ufficiale (ossia registrato) dell'organizzazione Titolare oppure un suo DBA ("Doing Business As") verificato.

3.1.4 Regole di 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), tenendo conto anche dei [BR] e delle [EVGL] per quanto concerne i certificati di tipo QWAC.

3.1.5 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. 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. In ogni caso, l'attributo **serialNumber** viene codificato in conformità alla norma ETSI EN 319 412-1.

Qualora il titolare sia una persona giuridica o sia associato ad una persona giuridica, l'univocità di quest'ultima è garantita attraverso l'inserimento dell'attributo **organizationIdentifier** (OID: 2.5.4.97) nel campo Subject. L'attributo **organizationIdentifier** contiene la **Partita IVA (VAT number)** della persona giuridica ed il codice ISO 3166 del paese che lo ha rilasciato. Qualora la persona giuridica non disponga di un codice fiscale, al suo posto può essere utilizzato un diverso codice identificativo univoco dell'organizzazione. In ogni caso, l'attributo **organizationIdentifier** viene codificato in conformità allo standard ETSI EN 319 412-1, ovvero come previsto dall'Avviso AgID n.18/2021.

Nel caso particolare dei certificati QWAC, che sono emessi a favore di persone giuridiche, l'univocità del nome dell'organizzazione titolare è ottenuta con l'inserimento dell'attributo **serialNumber** del Subject nel rispetto delle [EVGL], mentre l'**organizationIdentifier** è codificato come previsto dall'Avviso AgID n.18/2021, salvo i casi in cui diversamente disposto da altri regolamenti.

Nel caso dei certificati per sigillo elettronico (QSealC) o per siti web (QWAC) destinati a prestatori di servizi di pagamento ai sensi della direttiva PSD2, l'attributo **organizationIdentifier** è sempre presente e viene popolato nel rispetto della specifica ETSI TS 119 495.

3.1.6 Riconoscimento, autenticazione e ruolo dei marchi registrati

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 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 Validazione iniziale dell'identità

Questa sezione descrive le modalità di identificazione iniziale dell'identità del soggetto richiedente (persona fisica o giuridica) al momento della richiesta del certificato qualificato.

Alcuni dei paragrafi seguenti si applicano solamente ai *certificati qualificati per siti web* (QWAC), nel qual caso la CA rispetta i requisiti della norma ETSI EN 319 411-2, con particolare riferimento a quanto previsto dalle [EVGL] richiamate nella stessa norma.

3.2.1 Dimostrazione del possesso della chiave privata

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 4.1. La CA verifica che la firma elettronica contenuta nella CSR sia valida, prima di accettare la CSR.

3.2.2 Validazione dell'identità delle organizzazioni

3.2.2.1 Identità

Nel caso dei certificati per firma elettronica o per sigillo elettronico si applica quanto segue:

- 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 § 3.2.3).
- I poteri di rappresentanza della persona giuridica, dichiarati dalla persona fisica richiedente, devono essere dimostrati fornendo alla CA (o alla RA) appropriata documentazione emessa da una banca dati ufficiale (es. Registro delle Imprese).

Nel caso dei certificati per siti web (QWAC) si applica quanto segue:

- La CA verifica l'identità dell'organizzazione richiedente, la sua corretta denominazione ed il suo codice identificativo univoco (es. Partita IVA ove applicabile, il numero di iscrizione dell'impresa nel pertinente registro delle imprese negli altri casi), nonché l'indirizzo fisico della sua sede principale, mediante consultazione di fonti indipendenti affidabili.
- La richiesta di emissione del certificato dev'essere sottoscritta da un "Contract Signer" (firmatario della richiesta) autorizzato dall'organizzazione Richiedente; tale autorizzazione può essere auto-dichiarata dal firmatario ai sensi delle [EVGL]. Non è necessario che il firmatario sia un legale rappresentante dall'organizzazione Richiedente. L'identità individuale del firmatario della richiesta viene verificata con le modalità descritte nel §3.2.3.

3.2.2.2 DBA o Tradename

Nel caso dei certificati per siti web (QWAC), se il Subject del certificato deve includere un DBA ("Doing Business As") o un nome fittizio (trade name), la CA verifica il diritto del Richiedente di utilizzare tale DBA o nome depositato con uno dei metodi previsti dalle [EVGL].

3.2.2.3 Verifica del Paese

Nel caso dei certificati per siti web (QWAC), la CA verifica la correttezza del paese dichiarato dal Richiedente con uno dei metodi previsti dalle [EVGL].

3.2.2.4 Verifica del controllo dei domini

Nel caso dei certificati per siti web (QWAC), la CA verifica che tutti gli FQDN da includere nel certificato siano di proprietà o sotto il controllo materiale del Richiedente o di una sua affiliata (ad esempio una società controllante o controllata). Questa verifica viene svolta con almeno uno dei metodi ammessi dai Baseline Requirements del CAB Forum [BR].

3.2.2.5 Ulteriori verifiche

Nel caso dei certificati per siti web (QWAC), prima di emettere il certificato la CA svolge – oltre a quanto richiamato nei paragrafi precedenti – tutte le ulteriori verifiche previste nelle [EVGL], come richiesto dalla norma ETSI EN 319 411-1.

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, o basata sul riconoscimento effettuato da corrispondente Ente Emettitore o tramite uno schema di identificazione elettronica (e-ID) nazionale, ovvero notificato da uno Stato membro ai sensi dell'articolo 9 del regolamento eIDAS (**Modalità 4**);
- identificazione a distanza tramite videoconferenza, svolta dalla CA o dai soggetti incaricati (**Modalità 5**);
- identificazione del dipendente/collaboratore/agente/etc. mediante l'identificazione già svolta dal datore di lavoro in fase di assunzione e stipula del contratto (**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 sé o per l'organizzazione che egli/ella rappresenta.

Per i cittadini italiani e per i cittadini stranieri residenti in Italia, sono ammessi i seguenti documenti di identità e di riconoscimento equipollenti tra di loro, così come previsto dall'art. 35 del DPR 28 dicembre 2000, n. 445 e s.m.i.[1]:

- carta d'identità

[1] Le tipologie documentali riportate di seguito sono tassative in caso di identificazione svolta da Aruba PEC. Ciò non toglie che, in caso di identificazione svolta secondo le modalità 2, 3 e 4, Aruba PEC possa considerare validi le ulteriori tipologie documentali previste dal DPR 445/2000 raccogliendo, se del caso, esclusivamente gli estremi degli stessi ai fini di registrazione.

- passaporto
- patente di guida
- Tessere ATe e BT rilasciate dalla Pubblica Amministrazione.

I Richiedenti con cittadinanza diversa da quella italiana, ai fini dell'identificazione, devono esibire in originale uno dei documenti espressamente consentiti dall'Allegato al presente CPS denominato "Documenti di riconoscimento consentiti".

Modalità 1

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

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:

- direttamente dalla CA;
- da una terza parte denominata Centro di Registrazione Locale (CDRL) dinnanzi ad un incaricato del CDRL definito Operatore di Registrazione (OdR);
- da un soggetto terzo denominato Incaricato al Riconoscimento (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 OdR, IR o Operatori Supervisore (OS), a seconda dei casi, che dovrà operare nel contesto delle pratiche operative di registrazione. L'autorizzazione e successivamente la qualificazione degli OdR e degli OS come abili rispettivamente alle operazioni di identificazione, registrazione e rilascio, e alle operazioni di verifica, avviene mediante corso di formazione e superamento di una verifica scritta. 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 rispettivamente lo svolgimento delle attività di identificazione, registrazione e rilascio dei certificati nonché la verifica della documentazione raccolta. I privilegi di accesso agli strumenti telematici sicuri e le operazioni degli OdR e degli OS sono sotto il costante controllo della CA

Gli IR possono operare successivamente alla stipula di un mandato direttamente con la CA, o tramite nomina di un CDRL, nel contesto delle pratiche operative definite dalla CA stessa e limitatamente allo svolgimento delle attività di identificazione e 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, in recepimento della Direttiva 2005/60/CE, è tenuto al corretto riconoscimento della propria clientela; i dati identificativi del Richiedente, rilasciati sotto la propria responsabilità, ai sensi del D.Lgs. 231/07 e s.m.i. (con

specifico riferimento al contesto italiano) 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.

I Soggetti esercenti, destinatari degli obblighi di identificazione e adeguata verifica, acquisiscono i dati in base alle procedure definite in autonomia nel rispetto delle norme antiriciclaggio vigenti alla data di riconoscimento. Questa modalità di identificazione prevede che il Soggetto esercente operi comunque come terza parte delegata (CDRL) sulla base di appositi accordi stipulati con la CA, nel rispetto del presente CPS e di eventuali istruzioni specifiche contenute nell'incarico.

In particolare i Soggetti richiedenti, già contrattualizzati dal Soggetto destinatario degli obblighi o comunque coinvolti all'interno del processo di contrattualizzazione stesso, devono:

- essere identificati in ottemperanza con la vigente normativa in materia di Antiriciclaggio;
- essere sottoposti a un controllo continuo nel tempo;
- essere dotati di strumenti di autenticazione forte a due o più fattori, per l'accesso ai servizi online erogati dal Soggetto esercente, o comunque dotati di due o più canali di contatto personali e garantiti dal Soggetto esercente, funzionali alle comunicazioni e alle procedure di attivazione e autenticazione al Servizio di firma, e verificati dal Soggetto esercente nell'ambito delle suddette fasi di identificazione e controllo;

allora, per la registrazione della richiesta di rilascio del certificato qualificato, possono essere usati i dati identificati già acquisiti dallo stesso Soggetto esercente durante la suddetta fase di riconoscimento del Richiedente.

Infatti il Soggetto esercente, in conformità a quanto previsto dalle procedure interne e dalla normativa antiriciclaggio vigente, svolge tutte le operazioni necessarie alla corretta identificazione e registrazione del Richiedente, verificandone l'identità tramite controlli sui documenti e sui dati personali da esso forniti, ed effettuando, su di essi ,accertamenti specifici come, ad esempio verifiche sulle principali banche dati della loro coerenza, autenticità e accettabilità ai fini della prosecuzione dell'intero processo.

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 sottoposto 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 è espletata mediante mezzi di identificazione e autenticazione elettronica rilasciati nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione, a norma dell'articolo 9 del regolamento eIDAS; con specifico riferimento al contesto italiano, tale verifica dell'identità del Soggetto richiedente un certificato qualificato si avvale di un processo di

autenticazione SPID con credenziali di livello 2 o 3, nelle misure e nelle specificità delineate di volta in volta dall'Agenzia (AgID)

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.

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 al Riconoscimento (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 ed il trattamento dei dati personali in conformità alla normativa applicabile in materia, Aruba adotta idonee misure e strumenti a tutela degli interessati e rende disponibile l'informativa che definisce le modalità di trattamento dei dati trattati.

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

Modalità 6

Mediante questa modalità di identificazione la Certification Authority sfrutta la procedura di identificazione già eseguita dal datore di lavoro ai fini della stipula del contratto, previa verifica delle procedure operative di identificazione e di autenticazione utilizzate dall'azienda/organizzazione datrice. Analogamente, è considerata valida in conformità alla seguente modalità di riconoscimento, l'identificazione eseguita dal datore di lavoro nell'ambito della attivazione di rapporti di agenzia, previa verifica delle procedure operative di identificazione e di autenticazione utilizzate della parte datrice. Questa

modalità di identificazione prevede il conferimento da parte della CA di un mandato con rappresentanza al datore di lavoro, che agisce quindi da CDRL. I Certificati emessi secondo questa modalità di identificazione possono essere utilizzati per le finalità specificate dal datore di lavoro e riportate conseguentemente nello specifico limite d'uso del certificato. I dati di registrazione per questa modalità di identificazione sono conservati dalla CA in formato analogico o in formato elettronico.

3.2.4 Informazioni non verificate

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.

3.2.5 Verifica dell'autorizzazione delle richieste

Tutte le informazioni specificate nel §3.2.3 e nel §4.1 possono essere soggette a ulteriore verifica da parte degli Operatori Supervisore (OS) della CA, 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.

Nel caso dei certificati per siti web (QWAC), la CA verifica il nome, il titolo e l'autorità (rappresentanza) del Firmatario del Contratto (Contract Signer) – e dell'Approvatore del Certificato (Certificate Approver) qualora si tratti di una persona diversa – in conformità alle [EVGL]. Ai fini di tale verifica, Aruba PEC richiede normalmente una specifica dichiarazione da parte del Firmatario del Contratto che deve essere firmata con le modalità indicate nel par. 4.1.2.

3.2.5.1 Abilitazioni professionali, qualifica e organizzazione

Ai sensi dell'art. 28 del CAD, il Titolare può ottenere, in autonomia o con il consenso dell'eventuale "Terzo Interessato", 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 §3.1.2).

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 (cfr. §4.2.1), dovrà produrre anche documentazione idonea a dimostrare l'effettiva sussistenza della specifica qualifica (o abilitazione professionale), eventualmente attestandolo mediante *autocertificazione* ai sensi dell'art. 46 del DPR n.445/2000. Tale documentazione non dovrà essere anteriore di oltre 10 (dieci) giorni alla data di registrazione.

Ai sensi della Determinazione AgID n. 121/2019, nel caso in cui la qualifica sia *autocertificata* da parte del Richiedente, nel certificato non saranno inserite informazioni sull'organizzazione a cui potrebbe essere associato il Richiedente. 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 una qualifica. 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 della qualifica del Titolare e l'adempimento di quanto previsto a loro carico in qualità di "Terzo Interessato".

3.2.5.2 Limiti d'uso e limiti di valore

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 (vedere il §7.1.2). Il valore-limite desiderato dev'essere espresso come numero intero, 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:

- «*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).

Il certificato qualificato rilasciato tramite identità digitale SPID contiene l'OID 1.3.76.16.5, registrato a cura dell'Agenzia, con la seguente descrizione: "*Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity*". Eventuali certificati qualificati emessi a seguito di una richiesta sottoscritta con firma elettronica qualificata basata su tali certificati qualificati conterranno, a loro volta, il suddetto OID.

3.2.6 Criteri per l'interoperabilità

Aruba PEC si riserva facoltà di stipulare accordi con altri Prestatori di Servizi Fiduciari, limitati a specifici contesti, a patto che tali Prestatori siano Qualificati ai sensi del Regolamento EU n.910/2014.

3.3 Identificazione e autenticazione delle richieste di rinnovo

3.3.1 Identificazione e autenticazione per il rinnovo ordinario delle chiavi

La procedura seguita per il rinnovo del certificato (vedere §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).

A partire da 2 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.

Per quanto riguarda i certificati per firma elettronica o sigillo elettronico, 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.

Nel caso dei certificati per siti web (QWAC), la CA può richiedere al Titolare di seguire le stesse procedure di identificazione e autenticazione utilizzate per l'emissione iniziale del certificato, secondo l'età dei dati di validazione utilizzati per l'emissione iniziale (nel rispetto delle [EVGL]).

La richiesta di rinnovo di un certificato per sigillo elettronico è a carico della persona fisica che rappresenta la persona giuridica titolare del sigillo (vedere il §3.2.2).

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 sospensione e revoca

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

La revoca (o sospensione) del certificato può essere richiesta attraverso una procedura on-line, o rivolgendosi al CDRL che ha proceduto all'emissione del certificato o mediante inoltro alla CA (o ad un su CDRL) 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. Nel terzo caso il Titolare potrà seguire la procedura definita più nel dettaglio al capitolo 4.9.

4. REQUISITI OPERATIVI DI GESTIONE DEI 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 (https://www.pec.it) o ad una sua RA (CDRL).

La richiesta può prevedere anche un "terzo interessato", ovvero il soggetto che acconsente all'inserimento di una qualifica nel certificato (come previsto dall'art. 32 del CAD) oppure l'organizzazione che richiede o autorizza il rilascio del certificato del titolare (cfr. la Determinazione AgID n. 121/2019).

Un certificato qualificato per una persona giuridica può essere richiesto dalla persona fisica che rappresenta la persona giuridica, rivolgendosi direttamente alla CA oppure ad una RA.

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, 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: vedere più oltre);
- 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 (vedere il §3.2.1), 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. 3), 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 (vedere il §1.3.2). Tali terze parti (anche dette "Centri di Registrazione Locale", abbreviato 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 delle operazioni di identificazione e registrazione dei richiedenti, siano esse svolte in proprio oppure dai CDRL.

Nel caso dei certificati per siti web (QWAC), sono necessari i seguenti ruoli aggiuntivi del Richiedente, come definito in [EVGL], e applicati nell'ambito del processo di richiesta:

- Certificate Requester (la persona fisica che sottopone la richiesta alla CA)

- Certificate Approver (la persona fisica che approva la richiesta per conto del Richiedente)
- Contract Signer (la persona fisica che sottoscrive l'Accordo di Servizio ovvero Subscriber Agreement)

Il Richiedente può autorizzare una persona a ricoprire due o più dei ruoli di cui sopra e/o può autorizzare più di una persona a ricoprire lo stesso ruolo.

Nel caso dei certificati per siti web (QWAC), la richiesta del certificato dev'essere presentata da un Certificate Requester (o "riferimento tecnico") autorizzato e devono essere approvate da un idoneo Certificate Approver, in conformità con le [EVGL]. La richiesta di certificato dev'essere accompagnata da un Accordo di Servizio (ovvero Subscriber Agreement) firmato da un idoneo Contract Signer (firmatario della richiesta) ai sensi delle [EVGL], come anticipato nel capitolo 3. L'Accordo di Servizio dev'essere sottoscritto dal Contract Signer in uno dei seguenti modi:

- mediante firma autografa apposta in presenza di un rappresentante Aruba PEC (che controfirma come testimone);
- mediante firma autografa autenticata da un pubblico ufficiale (per es. un notaio); (*)
- mediante una firma elettronica qualificata valida, conforme alle normative Europee.

(*) In questo caso, la copia autenticata dell'Accordo di Servizio dev'essere inviata alla CA in originale. La richiesta di certificato non verrà presa in carico finché Aruba PEC non abbia ricevuto e verificato tale originale.

4.1.2.1 Informazioni che il Richiedente deve fornire

La richiesta di registrazione ed emissione certificato è formalizzata attraverso un "Modulo di Registrazione e Richiesta del Certificato" (il nome esatto del modulo può variare) reperibile sul sito web della CA o attraverso i suoi canali commerciali. In seguito, per brevità, si fa riferimento a questo documento con "modulo di richiesta".

In certi casi il modulo di richiesta viene generato in formato PDF dal sistema informativo di RA e precompilato 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 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 la 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. Nel caso di sottoscrizione elettronica, la CA accetta i seguenti tipi di firma elettronica:

1) firma elettronica avanzata basata su un certificato qualificato o qualificata ai sensi del Regolamento eIDAS (con certificato non necessariamente emesso dalla presente CA);
2) firma elettronica apposta mediante il certificato di autenticazione presente sulla carta CIE /CNS/CRS (Carta Identità Elettronica, 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 o firma elettronica avanzata ai sensi delle norme vigenti.

Per quanto riguarda il punto 5, la CA si riserva di accettare firme elettroniche solamente per i casi in cui accerti l'integrità e la sicurezza delle specifiche procedure autorizzate e messe in atto all'interno del processo di identificazione, ovvero nei casi in cui la procedura di accettazione o sottoscrizione è messa a disposizione dalla CA stessa.
Nei casi di identificazione de visu del Richiedente, l'incaricato al riconoscimento appone al modulo la propria controfirma digitale (o altra evidenza elettronica affidabile che attesti l'identità dell'operatore che ha effettuato il riconoscimento). 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 almeno le seguenti informazioni:

- nome e cognome (*)
- codice fiscale o analogo codice identificativo (*) (vedere il §3.1.5)
- tipologia ed estremi del documento di identità in corso di validità
- indirizzo di posta elettronica
- numero di telefono cellulare

La CA si riserva la possibilità di richiedere, a seconda delle modalità di identificazione e distribuzione del servizio, ulteriori informazioni necessarie per una identificazione certa e univoca del Richiedente applicando controlli, anche automatici, di coerenza e completezza sui dati e le informazioni raccolte. Inoltre, nel caso in cui debbano essere inserite ulteriori informazioni all'interno del certificato qualificato, la CA potrà richiede informazioni riguardo:

- 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 §3.1.3).

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:

- 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 §3.1.5)
- nome e cognome del richiedente
- codice fiscale o analogo codice identificativo del richiedente (vedere il §3.1.5)
- tipologia ed estremi del documento di identità in corso di validità
- indirizzo di posta elettronica del richiedente (per l'invio delle comunicazioni)
- numero di telefono cellulare (obbligatorio per alcune procedure).

(*) 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 del CDRL, alcuni codici personali e, per la firma remota, strumenti di identificazione e autenticazione 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, token o altri dispositivi di sicurezza)
- richiedere la sospensione o revoca del certificato ("codice utente")

I codici personali 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, ad eccezione di quanto previsto dall'appendice D del presente documento, il codice di sospensione o revoca del certificato può essere fornito al Titolare anche nella fase di generazione del certificato (vedere il §4.3.1).

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, anche a valle dei controlli effettuati da parte degli Operatori Supervisore. 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 (vedere il §3.2.3) 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 descritte nei par. 3.2 e 4.1. La generazione del certificato avviene nel rispetto delle norme vigenti e degli standard ETSI di riferimento, utilizzando un processo articolato in diverse fasi e basato su canali di comunicazione sicuri.

Durante il processo di emissione del certificato, di norma successivo all'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[2], nell'ambito del proprio database, che verrà inserito nell'attributo dnQualifier (OID: 2.5.4.46) del campo Subject del certificato (vedere il §3.1.5);
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. smartcard), a modificare i codici PIN e PUK del dispositivo impostandoli ai valori previsti (vedere il §4.2.1);
9) nel caso di chiavi di sottoscrizione generate dalla CA all'interno di HSM su richiesta del Titolare, associa al Titolare la credenziale di autenticazione, biometrica o di possesso, utilizzata in fase di generazione della coppia di chiavi (ad esempio OTP, impronta biometrica o altro di-

[2] 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.

spositivo fisico di sicurezza). L'accesso alla coppia di chiavi è inoltre assoggettato alla conoscenza di un secondo fattore di autenticazione conosciuto esclusivamente dal Titolare (ad esempio username e password precedentemente scelte dal titolare stesso o altro codice di identificazione personale);

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 delle norme vigenti);

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 oppure attraverso codici trasmessi via SMS e/o email;

    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 oppure attraverso codici trasmessi via SMS e/o email;

    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.

    – i codici personali di attivazione del dispositivo di firma vengono trasmessi all'utente che dovrà modificarli al primo accesso (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), l'identificazione del Richiedente può essere posticipata alla consegna dei dispositivi di firma, inoltre 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 impediscono 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.

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 hardware o software, smartcard) 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. Per ulteriori dettagli sugli obblighi del Titolare, si rimanda al §9.6.

4.5.2 Uso della chiave pubblica e del certificato da parte delle Relying Party

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 (vedere il §1.4).

Per ulteriori dettagli sugli obblighi delle RP, si rimanda al §9.6.

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.
Se in fase di richiesta del certificato ed accettazione delle condizioni di contratto, il Titolare esprime il proprio consenso al rinnovo tacito del certificato, la procedura di rinnovo è avviata in automatico secondo le modalità di seguito descritte:

- a seguito del consenso prestato, il Titolare riceverà comunicazioni (all'indirizzo di posta elettronica fornito alla CA o RA), relative alla gestione del tacito rinnovo (ad es. comunicazioni di tipo informativo in prossimità del rinnovo tacito e di conferma del rinnovo avvenuto). In qualsiasi momento il Titolare può revocare il consenso al rinnovo tacito fornito tramite le procedure messe a disposizione dalla CA, come ad esempio tramite accesso al pannello di gestione del Servizio;
- le chiavi generate sono custodite all'interno dello stesso dispositivo sicuro (§ 1.4) e sono mantenuti i medesimi elementi di sicurezza previsti.

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). Il Titolare può inoltre prestare il proprio consenso al rinnovo tacito del certificato durante la fase di richiesta del certificato ed accettazione delle condizioni di contratto. Sono rinnovabili, sulla base del presente CPS, solo i certificati emessi dalla presente CA.

4.6.3 Elaborazione delle richieste di rinnovo

Come anticipato nel §3.3, 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).

La procedura di rinnovo viene eseguita dal CDRL (come se fosse una nuova emissione) o direttamente dal Titolare attraverso un servizio messo a disposizione dalla CA, nell'ambito dei rapporti commerciali e contrattuali definiti con il Titolare o con la RA (CDRL), ove presente; anche per il rinnovo, l'interazione con il Titolare avviene tramite canali di comunicazione sicuri (cifrati e autenticati).
Nel caso di consenso al rinnovo tacito da parte del Titolare, la CA effettuerà la procedura prevista a partire dal punto 4 del presente paragrafo.

4.6.4 Notifica al titolare di nuova emissione del certificato

Si applica quanto descritto nel §4.3.2.

4.6.5 Comportamenti che costituiscono accettazione del certificato rinnovato

Si applica quanto descritto nel §4.4.1.

4.6.6 Pubblicazione del certificato rinnovato da parte della CA

Si applica quanto descritto nel §4.4.2.

4.6.7 Notifica ad altri soggetti della nuova emissione del certificato

Si applica quanto descritto nel §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; si rimanda pertanto ai paragrafi da 4.1 a 4.5.

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, qualifica oppure organizzazione, ecc., è gestita come un'emissione ex novo; si rimanda pertanto ai paragrafi da 4.1 a 4.5.

4.9 Sospensione e revoca del certificato

La sospensione e la revoca del certificato avvengono nel rispetto delle norme vigenti 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**. Per ulteriori dettagli si rimanda al §4.10.

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 strumenti di autenticazione); (*)
- il QSCD sul quale è conservata la chiave privata del titolare perda la certificazione di cui al par. §1.4. In particolare:

  nel caso in cui la CA venga a conoscenza della perdita dello stato di certificazione QSCD per il certificato recante la dichiarazione esi4-qcStatement-4 e di cui al par. §1.4, prima della fine del periodo di validità del certificato digitale, provvede alla revoca d'ufficio dello stesso ovvero ad adottare misure atte a impedire l'uso previsto del certificato.

  Nello specifico, qualora la CA si accerti della cancellazione fisica delle chiavi, potrà provvedere, ove previsto, a riemettere il certificato su altro QSCD di cui al par. §1.4 e a consegnarlo al titolare, attraverso le procedure di sicurezza disciplinate all'interno del presente Manuale.
- 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; per ulteriori dettagli sugli obblighi del Titolare si rimanda al §9.6.3.

Il "terzo Interessato" può richiedere la revoca del certificato (con modalità online tramite gli strumenti messi a disposizione dalla CA, o con modalità off-line descritta nel §4.9.3) 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 o la qualifica aziendale del titolare (es. poteri di rappresentanza o qualifica professionale) indicato nel certificato stesso.

Nel caso dei certificati di sigillo, il Titolare e le RP prendono atto che la CA non assume alcun obbligo di verificare, dopo l'emissione del certificato, la permanenza nel tempo dei requisiti che ne hanno consentito l'emissione relativi alla persona giuridica.

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 delle norme vigenti);
- dalla CA stessa, se ne ravvisa la necessità. In particolare:

  nel caso di certificato per sigillo, qualora la CA venga resa edotta da terzi della cessazione, per qualsivoglia motivo e/o causa, e/o dell'esistenza di procedure concorsuali e/o altre circostanze relative alla persona giuridica titolare dello stesso, tali da non rendere più attuali le informazioni in esso contenute;

- dall'Autorità Giudiziaria.

4.9.3 Procedura per la revoca

La revoca del certificato può essere richiesta con due 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://tsmp.arubapec.it/CMS/titolari/ArubaGroup/login-titolare 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 §4.9.5).

(*) Si tratta del "codice utente" consegnato al Titolare, ai sensi delle norme vigenti, in fase di registrazione o di consegna del dispositivo di firma, e comunque prima che il Titolare entri in possesso degli strumenti di firma, completamente operativi.

Modalità 2: off-line

La revoca del certificato può essere richiesta attraverso un CDRL oppure attraverso una richiesta formale inviata alla CA mediante posta elettronica (semplice o PEC), da inviare all'indirizzo revoche.firma@arubapec.it. La richiesta deve contenere:

- dati identificativi del richiedente (nome, cognome, codice fiscale, telefono, indirizzo di email, 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 §4.9.1);
- data e firma del richiedente (vedere il §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 §3.4).

Inoltre, è possibile trovare, all'interno delle guide aruba.it dedicate alla Firma digitale, pubblicate on-line all'indirizzo https://guide.pec.it/soluzioni-firma-digitale/firma-digitale.aspx il modulo predisposto per la richiesta di revoca di un certificato di firma.

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

La CA verifica l'autenticità della richiesta e procede alla revoca del certificato inserendolo in una lista di revoca e sospensione (**CRL**) la quale viene poi pubblicata come descritto nel §4.10. Il momento (data e ora) della revoca del certificato e pubblicazione della CRL è registrato nel giornale di controllo. Lo stato del certificato viene reso disponibile anche attraverso il servizio **OCSP** (vedere il §4.10).

In entrambe le modalità di richiesta (on-line ed off-line) viene inviata al Titolare un'email di conferma dell'avvenuta revoca, qualora la richiesta sia stata accolta.

Nel caso di richiesta da parte del "terzo Interessato", la CA comunica al Titolare del certificato l'avvenuta richiesta di revoca effettuata dal "terzo Interessato". La CA può rigettare la richiesta nel caso la giudichi non autentica, inesatta o incompleta e ne darà notifica al "terzo Interessato" richiedente.

Nel caso revoca su iniziativa della CA, la stessa notifica al Titolare le ragioni della revoca, nonché la data e l'ora a partire dalla quale la revoca sarà efficace.

Nel caso in cui sia richiesta una revoca e non sia possibile accertare in tempo utile l'autenticità della richiesta, la CA procede alla sospensione del certificato.

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 (vedere il §4.9.3) 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 paragrafi §4.5.2 e §9.6.4.

4.9.7 Frequenza di emissione della CRL

La CRL viene rigenerata e pubblicata periodicamente almeno ogni 24 ore, anche in assenza di nuove richieste di sospensione o revoca.

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. Per ulteriori dettagli, vedere il §4.10.

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 §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 o altri strumenti di autenticazione);
- sono insorti dubbi sulla correttezza dei dati contenuti nel certificato.

Nel caso dei certificati di Sigillo, il Titolare e le Relying Parties prendono atto che la CA non assume alcun obbligo di verificare, dopo l'emissione del certificato di sigillo elettronico, la permanenza dei requisiti che ne hanno consentito l'emissione relativi alla persona giuridica.

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, se ne ravvisa la necessità.

4.9.15 Procedura per la sospensione

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

4.9.16 Limiti sul periodo di sospensione

Allo scadere di un intervallo di tempo predefinito di 120 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, il recupero è invece previsto (cfr. il §6.2.4).

5. MISURE DI SICUREZZA FISICA ED OPERATIVA

5.1 Sicurezza fisica

Aruba PEC si avvale dei servizi di gestione data center (certificati ISO/IEC 27001) erogati dalla società capo-gruppo Aruba S.p.A., la quale è responsabile dell'housing, della connettività ad Internet e della sicurezza fisica dei sistemi di elaborazione utilizzati a supporto del servizio di CA. Aruba garantisce ad Aruba PEC:

- 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;
- Control Room presidiata 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 Aruba PEC S.p.A., sono basati su infrastrutture di elaborazione ridondate, progettate e realizzate in modo da garantire alta affidabilità e continuità di servizio. Per queste ragioni i tre datacenter di Proprietà del Gruppo Aruba utilizzati per l'erogazione del servizio sono geograficamente distribuiti nel territorio nazionale italiano.

Il data center **primario**, progettato e realizzato secondo le specifiche di livello Rating 4 (ex Tier 4) dello standard ANSI/TIA 942-B presenta le seguenti caratteristiche:

- Dimensioni: 5000 mq
- Capacità: oltre 40.000 server fisici
- Tipo di edificio: cemento armato
- Alta densità
- Carico massimo pavimento (Kg/mq): 1000
- Massima altezza pavimento flottante (mm): 500
- Altezza tra pavimento sopraelevato e controsoffitto (mt): 3
- Stanza disimballaggio
- Locali batterie esterni

Il data center **secondario** presenta le seguenti caratteristiche:

- Dimensioni: 2000 mq
- Capacità: oltre 10.000 server fisici
- Tipo di edificio: cemento armato
- Alta densità
- Carico massimo pavimento (Kg/mq): 500
- Massima altezza pavimento flottante (mm): 500
- Altezza tra pavimento sopraelevato e controsoffitto (mt): 3
- Stanza disimballaggio
- Locali batterie esterni

Il data center di **disaster recovery,** anch'esso progettato e realizzato secondo le specifiche di livello Rating 4 (ex Tier 4) dello standard ANSI/TIA 942-B, presenta le seguenti caratteristiche:

- Dimensioni: 90.000 mq destinati a data center su un'area complessiva di 200.000 mq
- Capacità: 3600 rack (165.000 server fisici)
- Tipo di edificio: cemento armato
- Doppio power center multi-modulare con UPS a ridondanza 2N + 1
- Generatori di emergenza ridondati con autonomia a pieno carico di 48 ore
- Data hall composta integralmente di muri tagliafuoco e tetto con doppia copertura isolante
- Produzione autonomia di energia idroelettrica e fotovoltaica
- Sistema di cooling geotermico ad altissima efficienza
- Aree magazzino ed uffici a disposizione dei clienti

Presso questo data center 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;
- **sistemi antintrusione passivi** quali grate, vetrate antiproiettile, porte blindate, cancelli motorizzati e sistemi **antintrusione attivi** quali TVCC e VMD.

Per le specificità dei singoli data center, si rimanda al paragrafo 5.1.1.

5.1.3 Alimentazione elettrica e condizionamento

Tutti i data center sono dotati di:

- sistemi di **alimentazione elettrica** ridondati a tutti i livelli 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.

Per le specificità dei singoli data center, si rimanda al paragrafo 5.1.1.

5.1.4 Prevenzione e protezione dagli allagamenti

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

Per le specificità dei singoli data center, si rimanda al paragrafo 5.1.1.

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. Per le specificità dei singoli data center, si rimanda al paragrafo 5.1.1.

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 alle norme vigenti.

I ruoli di fiducia e le relative responsabilità sono assegnate formalmente dalla Direzione 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.

Aruba PEC 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.
- 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 alle norme vigenti.
- 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 Aruba PEC 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);
- Responsabile della Sicurezza.

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 5.2.1 e in generale il personale di Aruba PEC utilizzano appropriati sistemi di identificazione e autenticazione prima dell'accesso ai sistemi informatici di Aruba PEC.

In particolare, per quanto riguarda l'accesso fisico alle sale dati e agli armadi che contengono i sistemi di CA, l'identificazione ed autenticazione avviene per mezzo di accesso controllato.

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 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 par. 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

Aruba PEC, 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. In particolare, in riferimento ai ruoli di fiducia, le caratteristiche e le competenze richieste sono descritte nel documento aziendale "job description".

Nel caso di nuove assunzioni, Aruba PEC, mediante strutture dedicate, 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, Aruba PEC si avvale, sia in ambito tecnico che amministrativo, tanto dei curricula inviati direttamente alla società tramite gli appositi canali (es. sito web) quanto della 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.). Le società di professionisti incaricate da Aruba PEC hanno inoltre l'obbligo di richiedere referenze possibilmente per ogni potenziale candidato prima di presentarlo ad Aruba PEC.

5.3.3 Requisiti di formazione

Il personale addetto ai servizi di CA viene adeguatamente formato, secondo le mansioni che svolge. Aruba PEC, mediante strutture dedicate, fornisce al personale una prima formazione al momento dell'assunzione, 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. Inoltre, con cadenza annuale viene svolta formazione a tutto il personale su tematiche di sicurezza delle informazioni.

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, Aruba PEC si riserva la facoltà di attivare il procedimento disciplinare previsto dal contratto collettivo, 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 Controlli sul personale non dipendente

Il personale non dipendente (es. consulenti) deve sottoscrivere un accordo di riservatezza (NDA) prima di iniziare a collaborare con Aruba PEC ed eventualmente accedere a dati confidenziali. Anche il personale non dipendente deve comunque conformarsi alle politiche di sicurezza aziendali.

5.3.8 Documentazione fornita al personale

Aruba PEC 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 e ora di occorrenza e, 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 par. 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 del CAD [2], la CA conserva 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.

I contratti stipulati con le Registration Authority (RA) sono conservati da Aruba PEC.

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

5.5.2 Periodo di conservazione degli archivi

Gli archivi sono conservati per almeno 20 anni, ai sensi del CAD [2].

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

Per questa casistica, Aruba PEC ha stipulato un contratto un'azienda leader nel campo dell'archiviazione e conservazione di materiale cartaceo e nei processi di dematerializzazione. Tale contratto prevede un servizio di gestione dell'archivio fisico che prevede le seguenti attività:

- ritiro dei moduli cartacei dall'archivio di Aruba e consegna presso il sito designato;
- movimentazioni in entrata e in uscita dall'archivio, utilizzando una procedura informatica realizzata appositamente per la gestione degli archivi cartacei,
- conservazione dei documenti presso il proprio Centro di Archiviazione dotato dei requisiti di sicurezza a norma sotto descritti,
- servizio di ricerca e consultazione del materiale cartaceo con SLA definiti,
- servizio di macerazione una volta scaduto il periodo di conservazione obbligatorio per legge,
- servizio di ritiro definitivo nel caso in cui Aruba PEC decida in seguito di avvalersi di altri fornitori o di gestire in proprio tale documentazione.

Il sito preposto per l'archiviazione è dotato degli impianti necessari, delle autorizzazioni necessarie e delle relative certificazioni per la conservazione del materiale cartaceo. Il fornitore infatti risponde ai prerequisiti progettuali richiesti dalle Sovrintendenze Archivistiche in materia di custodia e gestione degli archivi storici e degli enti pubblici (D.Lgs. 29/10/99 n° 490 – G.U. 27/12/99 n°302). Inoltre, alla medesima società è stato affidato il compito di dematerializzare i moduli attraverso una scansione degli stessi, una indicizzazione dei campi concordati tramite OCR ed il riversamento periodico delle immagini e degli indici su server messi a disposizione da Aruba PEC.

5.5.3.2 Archivi digitali

Nel caso di modulistica o documentazione digitale sono previsti due diversi approcci:

- nel caso in cui la documentazione viene gestita manualmente, quali ad es. moduli di richiesta certificato firmati digitalmente o richieste di revoca, gli operatori, una volta visionata le verificata la documentazione, procedono al caricamento della stessa sul sistema di conservazione a norma messo a disposizione da Aruba PEC;
- nel caso in cui la documentazione sia il risultato di processi applicativi, questa viene normalmente depositata su sistemi che sono sotto controllo della CA e, dopo l'apposizione di una marca temporale, vengono copiati su appositi sistemi ad accesso ristretto, garantendone il mantenimento per il tempo richiesto dalla normativa.

5.5.4 Procedure di backup degli archivi

Come dettagliato nel §5.5.3.1, gli archivi cartacei depositati e conservati presso un fornitore sterno sono scannerizzati ed una copia viene depositata su sistemi della CA.

Per quanto riguarda gli archivi digitali, come descritto nel §5.5.3.2, il backup è garantito o dal sistema di conservazione, che effettua per sua natura la doppia copia, o da un sistema di replica che effettua una seconda copia in un'area ad accesso limitato e controllato.

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

Le registrazioni di cui al par. 5.5.1 vengono tutte digitalizzate e quindi memorizzate in un sistema di gestione documentale e mantenute sui sistemi e con le modalità descritte al par. 5.5.3.

I documenti digitali e le copie scansionate dei documenti cartacei sono tutte mantenute nei data center di del gruppo Aruba.

5.5.7 Procedura di recupero e verifica delle informazioni archiviate

Per un rapido recupero delle informazioni archiviate è utile sapere secondo quale modalità è stato rilasciato lo specifico certificato al quale si riferiscono le informazioni ricercate; per fare questo vi sono varie modalità, fra cui la consultazione dei database della CA o dei siti web / portali che interfacciano i Richiedenti e le RA. È comunque possibile attivare più canali di ricerca in modo parallelo nel caso in cui la modalità di rilascio non sia nota a priori. In generale, vi sono due modalità di ricerca:

1) nel caso di documentazione cartacea, il contratto con il fornitore esterno include il servizio di ricerca e consultazione secondo SLA garantiti e conformi ai requisiti normativi e di business;
2) nel caso di documentazione digitale, è possibile effettuare le ricerche sul sistema di conserva-zione, attraverso i metadati principali, oppure nell'area di archiviazione della documentazione non ancora messa in conservazione a norma.

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), Aruba PEC 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, Aruba PEC 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 per la Gestione della Sicurezza delle Informazioni (SGSI) di Aruba PEC, conforme alla norma ISO/IEC 27001, prevede anche procedure di gestione degli incidenti e delle compromissioni.

La gestione di un incidente di sicurezza delle informazioni è gestita tramite una procedura in più fasi, ciascuna delle quali ha uno scopo ben preciso, coordinate da un comitato interno (Comitato per la Sicurezza e la Gestione delle Crisi, in seguito "Comitato") composto da figure di varia responsabilità e da membri della Direzione. Le fasi in cui si articola il processo sono descritte di seguito:

- Rilevazione: fase in cui qualsiasi persona (dipendente, collaboratore o comunque parte interessata) che rilevi un possibile incidente lo comunica al Comitato. Il Comitato si assicura che la segnalazione sia il più dettagliata possibile e che chi ha riscontrato il problema non compia alcuna azione in autonomia.
- Identificazione e analisi: il Comitato prende in carico la segnalazione e valuta se effettivamente sia un incidente di sicurezza. In caso positivo valuta la gravità e procede con le fasi successive. In caso negativo si limita alla chiusura dell'incidente.
- Contenimento: in questa fase si provvede per quanto possibile a contenere gli effetti dannosi provocati dall'incidente al fine di evitare che questi si propaghino ad altri ambiti dell'organizzazione.
- Raccolta evidenze: fase in cui si provvede a cercare e raccogliere le evidenze al fine di allegarle alla documentazione dell'incidente in caso di possibili conseguenze legali o per necessità di procedere con indagini più approfondite. Tutte le evidenze vengono raccolte seguendo delle linee guida il cui scopo è di garantire una raccolta corretta e attendibile.
- Rimozione e Ripristino: fase in cui si provvede a rimuovere la causa del danno e a riattivare, mediante le procedure di ripristino, i sistemi coinvolti dall'incidente, permettendo ai sistemi ed agli utenti di tornare ad operare.
- Chiusura Incidente e Notifica: terminata la fase di ripristino l'incidente si ritiene chiuso. In questa fase si notifica la chiusura ai vari responsabili coinvolti.

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

Aruba PEC implementa 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. Aruba PEC inoltre implementa 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 Aruba PEC 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 al par. 6.1.4.

5.7.4 Continuità operativa a fronte di un disastro

La continuità operativa a fronte di un disastro è garantita dal sito di DR collocato a distanza maggiore di 25 km rispetto ai datacenter primario e secondario.

5.8 Cessazione della CA o delle RA

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

Prima della effettiva cessazione:

- 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;
- si pianificherà la distruzione delle chiavi private di certificazione nonché del materiale crittografico annesso che ne consente il ripristino.

Alla data di cessazione:

- saranno rese disponibili le informazioni riguardanti lo stato dei certificati emessi e gestiti dalla CA cessante tramite l'emissione di un'ultima CRL statica conforme agli standard vigenti;
- 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 (cfr. il par. 6.2), 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 (cfr. il par. 1.4), 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 (cfr. il par. 1.4), 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 (cfr. il par. 1.4), il dispositivo viene generalmente fornito al titolare dalla CA o dalla RA già personalizzato (ossia contenente già la chiave privata ed il corrispondente certificato); in alcuni processi di rilascio le chiavi possono invece essere generate direttamente dal titolare tramite gli strumenti e le procedure messe a disposizione dalla CA. 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, eccetto nei casi in cui i certificati relativi alle chiavi sono consegnati in stato sospeso (fornendo al titolare gli strumenti e le procedure necessarie alla loro attivazione).

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) 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 sicuro

In questo caso le chiavi sono generate dal titolare stesso, con procedure approvate dalla CA, oppure sono generate dalla CA e fornite al titolare attraverso canali sicuri.

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 Aruba PEC 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 normalmente una lunghezza di 2048 bit.

Certificati qualificati per chiavi di lunghezza inferiore a 2048 bit possono essere erogati, a discrezione della CA, solo in casi circoscritti, motivati, e per un periodo di tempo limitato.

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 per firma elettronica o sigillo elettronico oppure per l'autenticazione di siti web. Nel certificato del titolare, l'estensione KeyUsage è valorizzata secondo il tipo di certificato come segue:

Tipo di certificato	KeyUsage
Firma elettronica, Sigillo elettronico (QSealC)	nonRepudiation
Sigillo elettronico per "Firma SPID"	digitalSignature + keyEncipherment
Autenticazione di sito web (QWAC)	digitalSignature + keyEncipherment

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 (vedere il 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, Aruba PEC 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 par. 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 par. 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 delle norme vigenti, 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.

I certificati per siti web (QWAC) hanno una durata massima di 2 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 al paragrafo 9.6.3.

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 Aruba PEC, incluso il servizio di CA, svolto da Aruba PEC o per conto di Aruba PEC, avviene nel rispetto del Sistema di Gestione Qualità (SGQ) aziendale, conforme alla norma UNI EN ISO 9001:2015.

6.6.2 Sistema di gestione della sicurezza

Aruba PEC ha definito e posto in opera un SGSI (Sistema di Gestione della Sicurezza delle Informazioni) conforme alla norma ISO/IEC 27001 che copre tutte le aree aziendali, incluse quelle coinvolte nello sviluppo ed erogazione del servizio di CA.

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.

Aruba PEC commissiona almeno trimestralmente un Vulnerability Assessment (VA) per verificare l'eventuale presenza di vulnerabilità, avvalendosi di specialisti indipendenti.

6.8 Riferimento temporale

Il riferimento temporale usato da Aruba PEC, 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).

Salvo diversa richiesta degli interessati, i certificati elettronici sono inoltre emessi secondo l'applicazione delle raccomandazioni emanate dall'Agenzia e volte a garantire maggiormente l'interoperabilità e la fruizione dei servizi in rete nel contesto italiano (Determinazione AgID n.121/2019, e successive modificazioni ed integrazioni). Quanto di seguito indicato presuppone il pieno soddisfacimento di tali raccomandazioni.

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 (cfr. il paragrafo 1.4 per ulteriori informazioni) ed eventuali qualificatori delle stesse.

L'estensione **CRLDistributionPoints** contiene l'indirizzo della **CRL** (per ulteriori informazioni si rimanda ai paragrafi 0 e 7.2).

L'estensione **AuthorityInformationAccess** contiene:

- l'indirizzo del servizio OCSP (per ulteriori informazioni si rimanda ai paragrafi 0 e 7.3);
- l'indirizzo (URL) dal quale si può scaricare il certificato della CA emittente.

Nel caso dei certificati per siti web (QWAC) è presente anche l'estensione **SubjectAlternativeNames** contenente uno o più **FQDN** (Fully Qualified Domain Names) sotto il controllo del titolare. Tra questi è incluso il FQDN contenuto nell'attributo commonName (CN) del campo Subject.

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 (vedere il paragrafo 1.4)
- **QcType** (0.4.0.1862.1.6)
- **QcPDS** (OID 0.4.0.1862.1.5)
- **etsi-psd2-qcStatement** (OID 0.4.0.19495.x così come previsti dallo standard ETSI 119 495) – solo nel caso di certificati per sigillo elettronico o per sito web da utilizzare nell'ambito di servizi di pagamento conformi alla direttiva comunitaria PSD2.

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).

Nei certificati di sigillo da utilizzarsi per le finalità di cui alla Determinazione AgID n.157/2020, è sempre presente anche l'estensione **ExtendedKeyUsage** (EKU) contenente l'elemento **id-kp-clientAuth**.

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.

Nei certificati per l'autenticazione di siti web (QWAC) viene inserito, nella estensione CertificatePolicies, anche l'OID standard indicativo della classe (EV) del certificato.

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 voci (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 Aruba PEC 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 Aruba PEC 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 interno sui 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.

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

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.

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 Aruba PEC.

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 (CAB) 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' Organismo di Valutazione (CAB).

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 sono pubblicate sul sito web della CA www.pec.it.

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.

9.1.5 Politica per il rimborso

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

9.2 Responsabilità finanziaria

9.2.1 Copertura assicurativa

Aruba PEC ha stipulato un'apposita assicurazione, con una società assicuratrice di primaria importanza, a copertura dei rischi derivanti dall'erogazione del servizio di certificazione e altri servizi fiduciari. In particolare, l'assicurazione prevede un massimale unico per sinistro e per periodo di assicurazione di EUR 15.000.000 (quindici milioni di Euro).

9.2.2 Altri asset

Nessuna stipula.

9.2.3 Garanzia o copertura assicurativa per gli utenti finali

Si rimanda al par. 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 9.3.2);
- 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 (si rimanda al par. 5.7).

Tutte le informazioni confidenziali sono trattate dalla CA nel rispetto delle norme applicabili, in particolare del D.lgs. 196/03 [4] e del Regolamento (UE) 2016/679 [5].

9.4 Trattamento e protezione dei dati personali

Aruba PEC 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 [4] nonché dal Regolamento (UE) 2016/679 [5].

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

9.4.1 Programma sulla privacy

Per quanto riguarda la privacy, la CA rispetta le norme vigenti, in particolare il D.lgs. 196/03 [4] ed il Regolamento (UE) 2016/679 [5]. La protezione dei dati personali rientra nel Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di Aruba PEC, certificato ISO/IEC 27001.

9.4.2 Dati che sono considerati personali

Si rimanda alla definizione di dati personali di cui alle norme vigenti, in particolare il Regolamento (UE) 2016/679 [5].

9.4.3 Dati che non sono considerati personali

Non sono considerati dati personali quelli che non rientrano nella definizione di cui al par. 9.4.2

9.4.4 Ruoli e Responsabilità nel trattamento di dati personali

Aruba PEC riveste il ruolo di "titolare del trattamento" dei dati personali ai sensi del D.lgs. 196/03 [4] e del Regolamento (UE) 2016/679 [5].

9.4.5 Informativa e consenso al trattamento dei dati personali

L'informativa sul trattamento dei dati personali, ai sensi del Regolamento (UE) 2016/679 [5], è pubblicata sul sito web della CA.
La richiesta del certificato comporta il trattamento dei dati personali dell'Interessato da parte della CA, in coerenza con l'informativa stessa rilasciata a quest'ultimo preliminarmente alla stipula del Contratto.

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 Regolamento (UE) 2016/679 [5], 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 Aruba PEC S.p.A. 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.

La CA si impegna altresì a rispettare tutti gli obblighi previsti dall'art. 32 del CAD ed in particolare:

- adotta tutte le misure organizzative e tecniche idonee ad evitare danno a terzi;
- a fronte di richieste di rilascio di certificati qualificati:
    - provvede con certezza alla identificazione della persona che fa richiesta della certificazione;
    - rilascia e rende pubblico il certificato elettronico nei modi o nei casi stabiliti dalle regole tecniche di cui all'articolo 71, nel rispetto del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni;
    - specifica, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della documentazione presentata dal richiedente che attesta la sussistenza degli stessi;
    - si attiene alle regole tecniche di cui all'articolo 71;
    - informa i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
    - procede alla tempestiva pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri del titolare medesimo, di perdita del possesso o della compromissione del dispositivo di firma o degli strumenti di autenticazione informatica per

l'utilizzo del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni, secondo quanto previsto dalle regole tecniche di cui all'articolo 71 del CAD;

- garantisce un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo nonché garantire il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;
- assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
- mantiene la registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno per venti anni anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- non copia, né conserva, le chiavi private di firma del soggetto cui il prestatore di servizi di firma elettronica qualificata ha fornito il servizio di certificazione;
- predispone su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio ed il prestatore di servizi di firma elettronica qualificata;
- utilizza sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato;
- garantisce il corretto funzionamento e la continuità del sistema e comunica immediatamente a AgID e agli utenti eventuali malfunzionamenti che determinano disservizio, sospensione o interruzione del servizio stesso.

- è responsabile dell'identificazione del soggetto che richiede il certificato qualificato di firma anche se tale attività è delegata a terzi.
- tratta i dati personali secondo quanto previsto dall'informativa di cui all'articolo 13 del Regolamento (UE) 2016/679. I dati non possono essere raccolti o elaborati per finalità diverse senza l'espresso consenso della persona cui si riferiscono.

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;
- 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 Aruba PEC 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 Aruba PEC presenti qualsiasi difformità rispetto alle attese.

Il titolare del certificato deve inoltre rispettare gli obblighi previsti dall'art. 32 del CAD ovvero:

- assicurare la custodia del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- utilizzare personalmente il dispositivo di firma.

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: 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 §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 Aruba PEC, 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 (in particolare [2] e [3]), il "Terzo Interessato" è la persona fisica o giuridica che acconsente all'inserimento di una qualifica 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

Gli obblighi e le responsabilità di Aruba PEC sono esclusivamente quelli definiti dal presente documento e dal Contratto di fornitura del Servizio. In particolare, Aruba PEC risponde dei danni causati a qualsiasi persona fisica o giuridica in seguito al mancato adempimento degli obblighi contrattuali e di quelli previsti dalla normativa vigente, nei casi ed entro i limiti previsti dall'art. 13 del Regolamento.
Fermo quanto precede in nessun altro caso, per nessun titolo e/o ragione, Aruba PEC potrà essere ritenuta responsabile nei confronti del Cliente, ovvero verso altri soggetti, direttamente o indirettamente, connessi o collegati al Cliente, per danni, diretti o indiretti, perdite di dati, violazione di diritti di terzi, ritardi, malfunzionamenti, interruzioni, totali o parziali, che si dovessero verificare a fronte dell'erogazione del Servizio, ove connessi, direttamente o indirettamente, o derivanti da:

a) cause di forza maggiore, caso fortuito, eventi catastrofici (a titolo esemplificativo ma non esaustivo: incendi, esplosioni, scioperi, sommosse, ecc.); e/o
b) manomissioni o interventi sul Servizio o sulle apparecchiature effettuati dal Cliente e/o da parte di terzi non autorizzati da Aruba PEC.

Aruba PEC non sarà considerata in nessun caso responsabile per l'uso fatto del Servizio in relazione a situazioni critiche che comportino, a titolo esemplificativo, rischi specifici per l'incolumità delle persone, danni ambientali, rischi specifici in relazione a servizi di trasporto di massa, alla gestione di impianti nucleari e chimici e di dispositivi medici; in tali casi, Aruba PEC si rende disponibile a valutare e negoziare con il Cliente uno specifico accordo "mission critical" con i rispettivi "SLA".
Aruba PEC non presta alcuna garanzia sulla validità ed efficacia, anche probatoria, del Servizio o di qualsiasi dato, informazione, messaggio, atto o documento ad esso associato o comunque immesso, comunicato, trasmesso, conservato o in ogni modo trattato mediante il Servizio medesimo:

a) quando il Cliente intende utilizzarli o farli valere in Stati ovvero ordinamenti diversi da quello Italiano, fatta eccezione, per quanto riguarda gli Stati facenti parte dell'Unione Europea, per i Certificati emessi in base al presente documento;
b) per la loro segretezza e/o integrità (nel senso che eventuali violazioni di queste ultime sono, di norma, rilevabili dal Titolare o dal destinatario attraverso l'apposita procedura di verifica).

Aruba PEC non assume, in nessun caso, alcuna responsabilità per le informazioni, i dati, i contenuti immessi o trasmessi e, comunque, trattati dal Cliente mediante il Servizio ed in genere per l'uso fatto dal medesimo del predetto Servizio e si riserva di adottare qualsiasi iniziativa ed azione, a tutela dei propri diritti ed interessi, ivi compresa la comunicazione ai soggetti coinvolti dei dati utili a consentire l'identificazione del Cliente.

9.9 Indennizzi

9.9.1 Indennizzi ai contraenti

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

Nel caso in cui i certificati rilasciati da Aruba PEC 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 - Aruba PEC 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 complessivo di EUR 1.250.000 (un milione e duecentocinquantamila Euro) incluse le spese di reclamo.

In caso di danno derivante dalle attività oggetto del Contratto, il Contraente dovrà, a pena di decadenza:

- farne denuncia ad Aruba PEC entro 24 ore dal suo verificarsi, ovvero da quando ne abbia avuta conoscenza (facendo seguire conferma per lettera raccomandata A.R. oppure Posta Elettronica Certificata entro le 24 ore successive);
- entro sei mesi dall'inoltro della denuncia di cui al punto precedente, quantificare l'eventuale danno subìto e formulare la relativa richiesta di risarcimento.

9.9.2 Indennizzi ad Aruba PEC

Fermo quanto previsto dalle Condizioni Generali di Fornitura, i Contraenti sono obbligati al risarcimento dei danni eventualmente sofferti da Aruba PEC 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 Aruba PEC; 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 1.5.1.

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 Foro competente

Per tutte le eventuali controversie giudiziarie nelle quali risulti attrice o convenuta Aruba PEC S.p.A e relative all'utilizzo del servizio di certificazione, alle modalità operative e all'applicazione delle disposizioni del presente Manuale sarà competente esclusivamente il Foro di Arezzo.

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.

[6] Direttiva (UE) 2015/2366 del Parlamento Europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno… ecc., Gazzetta Ufficiale dell'Unione Europea L337 del 23.12.2015.

[7] Regolamento Delegato (UE) 2018/389 della Commissione del 27 novembre 2017 che integra la Direttiva (UE) 2015/2366 del Parlamento Europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri.

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 Salvaguardia

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

Aruba PEC non sarà responsabile della mancata esecuzione delle obbligazioni qui assunte qualora tale mancata esecuzione sia dovuta a cause non imputabili ad Aruba PEC, 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.

9.17.2 Raccomandazioni

Gli applicativi di firma permettono di sottoscrivere digitalmente ogni tipo di file. Il Titolare deve tenere ben presente il fatto che alcuni formati consentono di inserire del codice eseguibile (macro o comandi) all'interno del documento senza che ciò vada ad modificarne la struttura binaria e tali da attivare funzionalità che possano alterare gli atti, i dati o i fatti rappresentati all'interno del documento stesso (Art. 4, comma 3 del DPCM 22 febbraio 2013).
Tali file, seppur sottoscritti con firma digitale, non producono gli effetti di cui all'articolo 21, comma 2 del CAD.

È unicamente responsabilità del Titolare firmatario accertarsi, attraverso le funzionalità tipiche di ciascun prodotto, che tale condizione sia soddisfatta.

Di seguito si forniscono alcune raccomandazioni a titolo esemplificativo e non esaustivo:

- Non apporre firme digitali a documenti che contengono “campi” il cui valore viene attualizzato automaticamente dall’applicazione con cui si visualizza il documento prima della firma (ad es. i campi Page e Date dell’applicazione Microsoft Word™).
- Non apporre firme digitali a documenti che contengono codice eseguibile (ad es. le “macro” della suite Microsoft Office™). Ove possibile, disabilitare la funzionalità prima di aprire il documento da firmare (ad es. in Adobe Reader™ accedere alla finestra delle Preferenze per disabilitare i “Javascript di Acrobat”).
- Prima di firmare un documento, trasformare i “campi” in valori statici (ad es. in Microsoft Word™ selezionare l’intero documento e poi premere la specifica combinazione di tasti, in genere CTRL+MAIUSC+F9).
- Verificare sempre l’esistenza di codice eseguibile incorporato nel documento da firmare (ad es. in Microsoft Word™ tramite il pannello di gestione delle “Macro”).

Le modalità operative possono divergere in base all’applicazione e alla versione del prodotto.
In caso di dubbi sull’affidabilità del documento è preferibile, prima di apporvi una o più firme digitali, convertire il documento a un diverso formato (ad es. PDF). Il processo di conversione consente infatti di eliminare dal documento elementi che possono potenzialmente rendere nulla la sottoscrizione stessa.

Lista allegati al presente CPS

ALLEGATO 1: DOCUMENTI DI RICONOSCIMENTO CONSENTITI

Appendice A – Chiavi di certificazione

Di seguito si elencano le chiavi di CA attualmente in uso da Aruba PEC 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 = ArubaPEC EU Qualified Certificates CA G2 OU = Qualified Trust Service Provider 2.5.4.97 = VATIT-01879020517 O = ArubaPEC S.p.A. L = Ponte San Pietro C = IT
Subject Key Identifier	13 d6 fa 13 94 9f a5 e1 c1 20 62 a8 fb c2 ee 37 4d 9f ed 25
Inizio validità	23/09/2017
Fine validità	18/09/2037

Subject DN	CN = ArubaPEC EU Qualified Certificates CA G1 OU = Qualified Trust Service Provider 2.5.4.97 = VATIT-01879020517 O = ArubaPEC S.p.A. L = Arezzo C = IT
Subject Key Identifier	c6 6f 3b 85 7b d1 26 b1 78 9a 42 a4 25 69 0c f6 ff 7a a0 67
Inizio validità	26/04/2017
Fine validità	21/04/2037

Subject DN	CN = ArubaPEC S.p.A. NG CA 3 OU = Certification AuthorityC O = ArubaPEC S.p.A. C = IT
Subject Key Identifier	f0 c0 45 b1 b6 35 b4 ea 5f 29 fa 83 03 4a dc 2f f5 b3 7d e8
Inizio validità	22/10/2010
Fine validità	23/10/2030

Subject DN	CN = ArubaPEC per Arma dei Carabinieri CA 1 OU = ArubaPEC per Certification Authority Carabinieri 1 O = ArubaPEC S.p.A. C = IT
Subject Key Identifier	1d ea a2 b9 4c b8 93 25 7f ec 3f 08 27 de 70 f2 8d 7f 83 20
Inizio validità	27/02/2009
Fine validità	28/02/2029

Subject DN	CN = ArubaPEC per Regione Basilicata CA 1 OU = ArubaPEC per CA Regione Basilicata di Firma Qualificata O = ArubaPEC S.p.A. C = IT
Subject Key Identifier	c5 db f0 51 6a a0 41 3f d1 ab 3c dd 09 54 18 72 05 ca b4 93
Inizio validità	21/03/2013
Fine validità	22/03/2033

Subject DN	CN = ArubaPEC per CA di firma qualificata OU = ArubaPEC per mod. ATe firma qualificata O = ArubaPEC S.p.A. C = IT
Subject Key Identifier	eb 09 88 fb eb 3b c5 07 ba cc b8 00 11 a0 a3 f7 f8 8b a5 64
Inizio validità	15/06/2016
Fine validità	16/06/2036

Subject DN	CN=CA di Firma Qualificata per Modello ATe OU=ArubaPEC per IPZS 2.5.4.97=VATIT-01879020517 O=ArubaPEC S.p.A. L=Ponte San Pietro C=IT
Subject Key Identifier	80 29 64 4e da aa da ac c5 61 24 27 a5 b3 90 75 aa 66 80 81
Inizio validità	28/03/2018
Fine validità	23/03/2038

Alla data di revisione del presente CPS, i certificati per siti web (QWAC) sono firmati con la chiave di certificazione “ArubaPEC EU Qualified Certificates CA G2”.

Appendice B – Modalità operative per la generazione e la verifica delle firme

In riferimento all'art. 14 del DPCM 22 febbraio 2013, Aruba PEC ha fornisce alla propria clientela applicazioni che permettono la verifica delle firme digitali apposte su documenti informatici sotto forma di "buste crittografiche" in standard PKCS#7 / CAdES, PAdES e XAdES. Tali applicazioni consentono di verificare:

1. l'integrità del documento firmato e i dati del firmatario;
2. l'autenticità e l'affidabilità del certificato del firmatario;
3. l'eventuale stato di sospensione o revoca del certificato del firmatario.

Pertanto il processo di validazione di una firma richiede:

- il certificato del firmatario;
- il certificato della chiave di certificazione emittente per verificare l'autenticità, integrità e affidabilità del certificato del firmatario;
- l'accesso alla CRL, ovvero al servizio OCSP, del certificatore emittente per verificare che il certificato del firmatario non sia stato sospeso o revocato.

Di seguito si fornisce la sintesi operativa del Titolare per l'utilizzo del sistema di verifica:

1. Avviare l'applicazione di firma e verifica.
2. Selezionare la funzione di verifica della firma.
3. Selezionare il file da verificare.
4. Il software necessita di avere una connessione ad internet in quanto tenterà l'accesso a CRL e/o OCSP.
5. Il software mostra a video il risultato della verifica. Il contenuto del file firmato potrà essere letto con programmi adeguati al formato del file stesso (esempio: i file in formato PDF saranno letti con Acrobat Reader).

Le stesse applicazioni qualificate per la verifica delle firme consentono di:

1. Apporre una firma digitale producendo come risultato una busta crittografica, nei formati standard PKCS#7 / CAdES, PAdES e XAdES.
2. Apporre firme multiple.

La generazione della firma avviene tramite una chiave privata la cui corrispondente chiave pubblica è stata certificata secondo le pratiche di cui al presente CPS. La sopra citata chiave privata è custodita o meno all'interno dei dispositivi sicuri di firma (cfr. il par. 1.4) forniti o qualificati da Aruba PEC. Alla firma digitale è sempre allegato il certificato qualificato del firmatario corrispondente alla chiave pubblica da utilizzare per la verifica.

Di seguito si fornisce la sintesi operativa del Titolare per la generazione della firma:

1. Avviare l'applicazione di firma.

2. Selezionare la funzione di firma dal menù principale o dal menù contestuale.
3. Selezionare il file da firmare.
4. Digitare il/i codice/i personale/i per l'accesso al dispositivo sicuro di firma (locale o remoto) o altro contenitore di chiave e certificato (cfr. il par. 1.4).

Appendice C – Procedura di registrazione e attivazione del servizio di firma remota con identificazione non contestuale

Sommario

Definizioni

Cliente	Persona giuridica, pubblica o privata, avente un rapporto contrattuale con la CA per la fornitura dei servizi oggetto del presente documento ed ulteriormente definita nella contrattualistica dedicata.

1. Introduzione

Questa Appendice descrive le condizioni e le regole secondo le quali il Certificatore Aruba PEC rilascia certificati qualificati per chiavi di sottoscrizione remota, in conformità con la vigente normativa in materia di firma digitale, nei casi in cui sono ottemperati gli obblighi di identificazione dell'utente richiedente in una fase successiva e comunque non contestuale all'emissione e al primo utilizzo del certificato stesso.

2. Campo di applicazione, scopo e raccomandazioni ai lettori

La presente appendice si applica in quei contesti in cui il processo di generazione del certificato, identificazione del richiedente ed apposizione della firma, segua un flusso particolare o comunque non esplicitamente dettagliato all'interno del CPS. Scopo dell'Appendice è quindi descrivere secondo quali modalità e con quali garanzie di sicurezza Aruba PEC possa emettere i certificati in questi specifici contesti di utilizzo.
Quanto segue integra, ove necessario, le modalità con cui Aruba PEC emette il certificato di firma remota nel suddetto contesto operativo, le misure di sicurezza adottate, gli obblighi, le garanzie e le responsabilità, già indicate nel presente Manuale Operativo (CPS) e/o nelle sue Appendici. Per tutto quanto non espressamente indicato nel CPS, resta valido quanto descritto nel presente documento, al quale si rimanda anche per i riferimenti normativi e tecnici eventualmente non riportati nel CPS stesso.

3. Modalità di emissione e utilizzo dei certificati

In questo paragrafo vengono descritte le procedure usate per la registrazione, l'identificazione e l'attivazione del servizio di firma agli utenti che non sono stati precedentemente o contestualmente identificati né dalla CA né dal Cliente. In un contesto tipico, ma non esclusivo, l'utente richiedente è un *prospect* attestato sul sito/portale web o altro sistema informatico del Certificatore o Cliente, di seguito semplicemente Sistema, che eroga il servizio di firma; l'utente in questione intende, per esempio,

sottoscrivere un contratto per l'acquisto di uno o più servizi o prodotti offerti, per il quale è necessaria la firma remota degli stessi.
Lo scenario prevede che un utente richieda un servizio per la firma digitale remota secondo un processo sintetizzato nelle seguenti fasi (si omettono i passaggi non essenziali ai fini del presente documento).

1) **Registrazione dei dati** – l'utente è attestato sull'area preposta del Sistema e deve inserire o confermare i propri dati anagrafici, tra i quali quelli indispensabili alla CA per la sua successiva identificazione e per l'emissione del certificato qualificato, gli attributi di contatto come il proprio indirizzo di posta elettronica e il proprio n. di telefono cellulare, oltre a quei dati eventualmente necessari al Cliente per i propri scopi (si veda il par. 4.1.2.1 "Informazioni che il Richiedente deve fornire" del presente CPS per maggiori dettagli).

2) **Generazione del certificato** – l'utente procede con la richiesta del certificato di firma remota (nel corso del processo, l'utente riceve o specifica eventuali codici necessari per l'autenticazione in fase di firma, in base alla specifica procedura attivata). Una volta che la CA riceve i dati anagrafici del richiedente procede all'emissione del certificato qualificato, che sarà revocato qualora non si concluda con esito positivo il processo di verifica dell'identità del titolare da parte della CA o dei soggetti da essa delegati. Tale certificato qualificato avrà specifiche limitazioni d'uso e d'utilizzo relativamente allo scenario in questione.

   La CA si riserva la facoltà di richiedere al Cliente specifiche, misure e strumenti nell'implementazione della soluzione, se quelle adottate fossero ritenute non adeguate o non sufficienti allo scenario di utilizzo del certificato qualificato, compreso raccogliere e trasmettere attraverso i canali concordati peculiari evidenze / attestazioni relativamente ai dati e alle attività di registrazione, autenticate dal soggetto stesso o altra persona fisica autorizzata in qualità di incaricato applicativo o responsabile di processo del Cliente.

3) **Firma delle condizioni contrattuali** – il titolare firma digitalmente la documentazione prevista (moduli, documenti e contratti sia del Cliente sia della CA) inserendo i codici personali statici e/o dinamici (OTP) di autenticazione previsti dal processo; il certificato digitale di firma, dopo l'avvenuta sottoscrizione dei documenti, viene sospeso dalla CA, altresì su indicazione del Cliente, in attesa della conclusione del processo di identificazione.

4) **Identificazione del titolare** (Attivazione/Revoca del Certificato) – conseguentemente, la CA o i soggetti delegati (es. il Cliente a valle della sua contrattualizzazione in qualità di CDRL) procedono con l'identificazione certa del titolare. Aruba PEC considera valide le identificazioni svolte utilizzando esclusivamente una delle modalità di identificazione già consentite alla CA ai sensi del par. 3.2.3 del presente CPS e comunque concordate con Aruba PEC nel momento di definizione delle attività di CDRL.

   Si configurano due scenari alternativi:
   - nel caso in cui il processo di verifica dell'identità del titolare sia completato positivamente, così risultando confermata l'assegnazione del certificato del titolare, la CA provvede alla riattivazione del certificato e questi è reso disponibile per il normale utilizzo attraverso i servizi previsti;
   - se invece il processo di verifica dell'identità del titolare non si è concluso o è terminato negativamente (es. individuando difformità rilevanti nei dati identificativi forniti e/o riportati nel certificato), la CA procederà alla revoca del certificato.

La CA si riserva la facoltà di richiedere al Cliente, quando anche CDRL, peculiari evidenze / attestazioni relativamente all'esito di tali attività di validazione dell'identità del titolare, concordando anche contrattualmente misure e specifiche decorrenze in relazione alle peculiarità del contesto.
Ciò nonostante, la CA rimane responsabile di garantire la revoca del certificato qualora sia decorso il termine massimo previsto dal presente CPS sul periodo di sospensione.

4. Certificate policy

I certificati emessi secondo le regole del presente allegato sono identificati con i seguenti Object Identifier (OID):

- 1.3.6.1.4.1.29741.1.7.11 = "Certificati qualificati eIDAS emessi con procedure ad hoc per progetti specifici"

OID aggiuntivi possono essere presenti nel certificato in rapporto all'uso previsto del certificato, a specifici standard e regolamentazioni e comunque secondo le indicazioni del presente CPS (par. 1.4).

5. Limiti d'uso e limiti d'utilizzo

I certificati sono emessi nell'ambito di un ben preciso contesto applicativo e d'utilizzo, prevedono pertanto l'inserimento di opportune limitazioni d'uso della firma digitale. Come previsto dalle regole tecniche, tale limitazione sarà codificata all'interno del certificato in forma human readable.
Una volta attivato il servizio di firma digitale remota, secondo le procedure descritte nei paragrafi precedenti, il titolare potrà disporre del proprio certificato esclusivamente tramite i servizi applicativi esposti dal Cliente (o dal Certificatore). Pertanto, l'uso del certificato sarà limitato sia attraverso le limitazioni d'uso riportate nel certificato stesso, come anzidetto, sia da misure tecniche che lo rendono fruibile esclusivamente attraverso i servizi (tipicamente on-line) previsti / offerti in relazione allo specifico scenario in questione.

Appendice D – Procedura di attivazione e utilizzo del servizio di firma remota One Shot

Sommario

Definizioni

Certificato One-Shot	Il certificato digitale qualificato disciplinato nella presente Appendice avente durata limitata nel tempo per un periodo non superiore a 30 (trenta) giorni a decorrere dal momento della sua emissione
Cliente	Persona giuridica, pubblica o privata, avente un rapporto contrattuale con la CA per la fornitura dei servizi oggetto del presente documento ed ulteriormente definita nella contrattualistica dedicata.

1. Introduzione

In questa appendice vengono descritte le regole, le modalità e le procedure operative adottate dal Certificatore per l'emissione di certificati "One Shot", ossia una particolare tipologia di certificato qualificato che, in presenza di determinati vincoli di dominio o ambiti di utilizzo, è caratterizzato dalla semplicità di fruizione e dalla breve durata.

2. Campo di applicazione, scopo e raccomandazioni ai lettori

Aruba PEC, oltre ai certificati aventi le caratteristiche descritte nella sezione generale di questo CPS, ha altresì la facoltà in specifici contesti, riconducibili a limitati utilizzi della firma digitale, di emettere un tipo particolare di certificato denominato One Shot. La caratteristica di detti certificati qualificati One Shot è quella di avere un periodo di validità più breve, solitamente non superiore a 30 (trenta) giorni dal momento della loro emissione, un utilizzo entro le 24 (ventiquattro) ore dal momento dell'emissione, ed un'esperienza utente semplificata.
Conclusasi la fase di registrazione iniziale, il rilascio del Certificato One Shot è previsto in un'unica modalità, ossia remotamente con chiavi generate su dispositivi HSM (QSCD). Questa procedura viene effettuata sotto la responsabilità di personale specializzato del Certificatore o da quest'ultimo debitamente autorizzato, negli spazi che ospitano l'HSM e i server collegati.
La presente appendice identifica i soggetti coinvolti nel procedimento di rilascio dei suddetti certificati qualificati di firma remota One Shot, gli obblighi e le responsabilità di detti soggetti e degli utenti, i presupposti e le modalità di rilascio dei certificati, e quelle di loro utilizzo.

Quanto segue integra ove necessario le modalità operative già indicate nel presente Manuale Operativo (CPS) e/o nelle sue Appendici. Per tutto quanto non espressamente qui indicato, resta valido quanto descritto nel presente documento, al quale si rimanda anche per i riferimenti normativi e tecnici eventualmente qui non riportati.

3. Modalità utilizzo dei certificati One Shot

La CA ha predisposto per il Certificato One Shot un sistema di gestione semplificato delle credenziali che richiede, per l'apposizione della firma remota, un singolo fattore di autenticazione informatica, ossia l'utilizzo di una One Time Password (OTP).
L'impostazione da parte dell'utente e l'inserimento del nome utente e password non sono ritenuti obbligatori ai fini dell'utilizzo del certificato One Shot in quanto, questo specifico tipo di certificato, può essere utilizzato solo attraverso i processi di firma preposti dal Certificatore o dal Cliente e solo contestualmente o in un arco temporale vicino al rilascio del certificato richiesto; l'utilizzo del certificato è comunque subordinato all'identificazione iniziale del soggetto richiedente conformemente con le funzioni di identificazione e autenticazione approvate dal Certificatore e indicate nel presente CPS.
In base alle procedure per l'emissione e il rilascio dei certificati digitali previsti nello specifico contesto operativo, la CA si avvale della possibilità di autorizzare i propri Clienti, con un atto di delega, ad adempiere a tutte o a una parte delle attività di registrazione e attivazione, ivi compresa l'identificazione certa dei soggetti richiedenti e la raccolta del consenso dell'utente; in tal caso il Cliente si configura come Centro di Registrazione Locale (CDRL) del Certificatore accreditato Aruba PEC.

4. Generazione e gestione dell'OTP

Come accennato sopra, l'unico fattore di autenticazione necessario per utilizzare questo certificato è una One-Time Password (OTP).
L'OTP è generata randomicamente dal sistema del Certificatore al momento dell'attivazione da parte del Titolare della procedura di firma remota.
La OTP viene trasmessa al Titolare o generata dallo stesso tramite uno strumento hardware o software, prescelto al momento della registrazione o stabilito dalle parti contraenti, Aruba PEC e il suo Cliente, rispetto al contesto di utilizzo. In ogni caso, il token OTP è associato al Titolare attraverso procedure sicure che dipendono dal tipo di dispositivo utilizzato; tipicamente la OTP è ricevuta sul numero di cellulare dichiarato e verificato in fase di identificazione/registrazione.
Con l'inserimento della OTP, il titolare avvia la procedura di firma remota provvedendo a trasmettere il dato per la creazione della firma di sua esclusiva conoscenza.

5. Verifiche preliminari e obblighi contrattuali

Considerando la necessità di assicurare l'utilizzo del certificato al legittimo titolare, Aruba PEC, prima di implementare o autorizzare il processo che ne consenta l'erogazione, verifica che la soluzione adottata dal Cliente sia sostenibile, adeguata ai propri standard e compliant con il presente CPS.
Pertanto, il Cliente è contrattualmente obbligato ad implementare tutti gli accorgimenti organizzativi e le misure di sicurezza che Aruba PEC riterrà nel caso necessarie al fine di considerare sufficientemente sicura la soluzione che si intende realizzare. Questi obblighi particolari, disposti per l'utilizzo di certificati One Shot, verranno formalizzati nei contratti tra le parti.

6. Uso della chiave privata e del certificato da parte del titolare

Il titolare è pertanto tenuto a proteggere la riservatezza del proprio dispositivo sul quale genererà o riceverà l'OTP per poi sbloccare l'utilizzo della propria chiave privata, custodendolo in un luogo sicuro e con le adeguate misure di sicurezza in modo tale da evitare di far accedere terzi.
Come per tutti i certificati qualificati, anche per i certificati One Shot il suo utilizzo è strettamente personale e non può mai, per nessuna ragione, essere ceduto o concesso in uso a terzi.

7. Certificate policy

I certificati emessi secondo le regole del presente allegato sono identificati con il seguente Object Identifier (OID): 1.3.6.1.4.1.29741.1.7.10
OID aggiuntivi possono essere presenti nel certificato in rapporto all'uso previsto del certificato, a specifici standard e regolamentazioni e comunque secondo le indicazioni del presente CPS (par. 1.4).

8. Limiti d'uso e limiti d'utilizzo

I certificati sono emessi nell'ambito di un ben preciso contesto applicativo e d'utilizzo, prevedono pertanto l'inserimento di opportune limitazioni d'uso della firma digitale. Come previsto dalle regole tecniche, tale limitazione sarà codificata all'interno del certificato in forma human readable.
Conseguentemente, il titolare potrà disporre del proprio certificato esclusivamente tramite specifici servizi applicativi e sottoscrivere documenti informatici nell'ambito di processi autorizzati.