Certificatore Aruba PEC S.p.A.

Servizio di Certificazione Digitale

Manuale operativo

Revisione 1.0

Approvato da ***:*** ***Libero Marconi***
Direttore servizi di certificazione

Marconi/Libero/MRCLBR64E08L117O/10026976
Firmato digitalmente da Marconi/Libero/MRCLBR64E08L117O/10026976
ND: cn=Marconi/Libero/MRCLBR64E08L117O/10026976, 2.5.4.13=C=Marconi/N=Libero/D=08-05-1964/I=Direttore, email=lmarconi@trustitalia.it, o=Trust Italia S.p.A., ou=Servizi di Certificazione FD, l=Terni, c=IT
Data: 2007.10.08 15:21:16 +02'00'

il 8 / 10 /2007

Storia delle modifiche apportate.

Prima revisione del documento; nessuna modifica apportata .

Indice

Cap. 1 Introduzione

1.1 Scopo del documento e principali raccomandazioni ai lettori.

Questa sezione illustra lo scopo del manuale operativo e fornisce alcune raccomandazioni per il corretto utilizzo del servizio di certificazione. Si prega di leggere l'intero testo del Manuale in quanto le raccomandazioni contenute nella presente sezione sono incomplete e molti altri importanti punti sono trattati negli altri capitoli. Per una più agevole e scorrevole lettura del Manuale Operativo si raccomanda la consultazione dell'elenco di acronimi e abbreviazioni posti alla fine della presente sezione. Il presente manuale operativo ha lo scopo di illustrare e definire le modalità operative adottate dalla Aruba PEC S.p.A. nella attività di certificazione ai sensi del Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445, "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", pubblicato sul Supplemento Ordinario alla Gazzetta Ufficiale n. 42 del 20 febbraio 2001. del Decreto Legislativo 7 marzo 2005, n. 82: "Codice dell'amministrazione digitale", pubblicato nella Gazzetta Ufficiale. n. 112 del 16 maggio 2005.. e successive modifiche ed integrazioni e del Decreto del Presidente del Consiglio dei Ministri (DPCM) 13/01/2004, "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ", pubblicato sulla Gazzetta Ufficiale 27 aprile 2004, n. 98. In particolare, il presente documento illustra le modalità di richiesta, registrazione, validazione, emissione, utilizzo, sospensione, revoca, scadenza e rinnovo del certificato, nonché le responsabilità e gli obblighi del certificatore, dei titolari del certificato e di tutti coloro che accedono al servizio di certificazione pubblica per la verifica delle firme. In ottemperanza all'obbligo di informazione (DPCM 13 Gennaio 2004, art. 38 e successive modifiche ed integrazioni) è richiesto dalla legge; Aruba PEC S.p.A. come struttura di certificazione digitale, pubblica il presente manuale operativo in modo da permettere ad ogni singolo utente di valutare il grado di affidabilità del servizio offerto.
Nel presente Manuale Operativo, si parte dal presupposto che il lettore abbia una adeguata conoscenza della materia relativa alla firma digitale ed alla struttura PKI. In caso contrario, prima di richiedere un certificato, si consiglia un adeguato training nell'uso delle tecniche a chiave pubblica. Le informazioni riguardanti formazione e training sono rese disponibili da Aruba PEC S.p.A., all'indirizzo: https://ca.arubapec.it. Ulteriore assistenza è offerta dagli addetti al servizio clienti di Aruba PEC S.p.A. (customer_service@ca.arubapec.it). Aruba PEC S.p.A., allo scopo di consentire un corretto utilizzo del servizio di certificazione, oltre a raccomandare all'utente una attenta lettura del presente documento, invita tutti coloro i quali dovranno fare affidamento su di un certificato e/o sulle informazioni in esso contenute, di controllare preventivamente (nelle apposite liste di certificati revocati o sospesi, disponibili per via telematica agli utenti – vedi definizioni di CRL, CSP) che il certificato sia valido e non revocato o sospeso, che la firma digitale sia stata creata durante il periodo operativo del certificato stesso dalla chiave privata corrispondente alla chiave pubblica riportata nel certificato, e che il messaggio associato alla firma digitale non sia stato modificato. Il titolare del certificato si impegna a proteggere ed a tenere segreta la propria chiave privata (vedi definizioni) nonché a dare avviso al Certificatore dell'eventuale smarrimento, sottrazione o compromissione (vedi definizioni) della stessa. Per ulteriori informazioni, vedi il sito web di Aruba PEC S.p.A. http://www.arubapec.it oppure contattare il sevizio clienti all'indirizzo: customer_service@ca.arubapec.it.

1.2 Riferimenti agli standard

PKCS#1. Public Key Cryptography Standards. Standard realizzati per assicurare l'interoperabilità delle tecniche crittografiche. Le componenti di questo standard sono numerate. Maggiori dettagli sugli standard PKCS implementati sono disponibili presso il sito http://www.rsa.com.
LDAP. Lightweight Directory Access Protocol. Protocollo per utilizzato per accedere online a servizi di directory (in particolare servizi directory X.500) che possono contenere informazioni riguardo ad utenti e ad i loro certificati digitali.
X.500. Insieme di standards ITU-T relativi a servizi di directory elettroniche.
X.509. Standards ITU-T T relativi a certificati digitali. X.509 v3 si riferisce a certificati contenenti o in grado di contenere estensioni.
Secure Sockets Layer (SSL). Protocollo originariamente sviluppato da Netscape, poi divenuto standard universale per l'autenticazione dei siti Web e per cifrare le comunicazioni tra i client (browsers) e i Web server.
IPSec. Insieme di standard aperti per assicurare comunicazioni private sicure nelle reti IP al livello network, che forniscono la crittografia a livello network.
SHA-1. Secure Hash Algorithm (SHA), algoritmo specificato nel Secure Hash Standard (SHS, FIPS 180), sviluppato dal NIST [NIS93a]. SHA-1 [NIS94c] è una revisione del algoritmo SHA pubblicata nel 1994.

1.3 Riferimenti normativi

- Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445, “Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa”, pubblicato sul Supplemento Ordinario alla Gazzetta Ufficiale n. 42 del 20 febbraio 2001.
- Decreto del Presidente del Consiglio dei Ministri **(DPCM)** 13/01/2004, "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ", pubblicato sulla Gazzetta Ufficiale 27 aprile 2004, n. 98.
- Direttiva del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche (Gazzetta Ufficiale delle Comunità europee L. 13 del 13 dicembre 1999).
- Decreto Legislativo **(DLGS 196)** 30 giugno 2003, n. 196, “Codice in materia di protezione dei dati personali”, pubblicato nel Supplemento Ordinario n.123 della Gazzetta Ufficiale n. 174, 29 luglio 2003.
- Decreto 2 luglio 2004, “Competenza in materia di certificatori di firma elettronica” pubblicato nella Gazzetta Ufficiale n.199, 25 agosto 2004.
- Decreto Legislativo **(CAD)** 7 marzo 2005, n. 82: "Codice dell’amministrazione digitale", pubblicato nella Gazzetta Ufficiale. n. 112 del 16 maggio 2005.
- Deliberazione 17 febbraio 2005 **(DELIB 4/05)**, “Regole per il riconoscimento e la verifica del documento informatico” (Deliberazione n. 4/2005), Pubblicato nella Gazzetta Ufficiale n. 51 del 3 marzo 2005.
- Legge 11 agosto 1991, “Istituzione del Sistema Nazionale di Taratura”, Pubblicato nella Gazzetta Ufficiale 6 maggio 2002, n. 104.
- Decreto legislativo 4 aprile 2006, n. 159 “Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell’amministrazione digitale”, Pubblicato in Gazzetta Ufficiale 29 aprile 2006, n.99.
- Decreto del Presidente della Repubblica 2 marzo 2004, n. 117, “Regolamento concernente la diffusione della Carta Nazionale dei Servizi, a norma dell'articolo 27, comma 8, lettera b), della legge 16 gennaio 2003, n. 3.” (G.U. n. 105 del 6 maggio 2004).
- Decreto del Ministero dell’Interno, del Ministro per l’innovazione e le tecnologie e del Ministro dell’economia e delle finanze 9 dicembre 2004, recante “Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale dei Servizi” pubblicato nella Gazzetta Ufficiale n.296, 18 dicembre 2004.
- “Linee guida per l’emissione e l’utilizzo della Carta Nazionale dei Servizi”, Ufficio standard e metodologie d’identificazione, CNIPA, Versione 3.0, 15 maggio 2006.

1.4 Definizioni ed acronimi

CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
CA	certification authority – autorità di certificazione
CDRL	Centro Di Registrazione Locale
CSL	certificate suspension list – lista dei certificati sospesi
CSR	certificate signing request
CRL	certificate revocation list – lista dei certificati revocati
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol con SSL
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
LRA	local registration authority – autorità di registrazione locale
LRAA	local registration authority administrator – amministratore LRA
NTP	Protocollo di accesso a servizi di data e ora certa
OdR	Operatore di Registrazione
POP	Point of Presence
PIN	personal identification number
PKCS	Public Key Cryptography Standards
PKI	public key infrastructure – infrastruttura a chiave pubblica
RDN	Relative Distinguished Name
RPA	Relying Party Agreement
RSA	sistema crittografico
SET	Secure Electronic Transaction
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
URL	uniform resource locator
OCSP	Protocollo per il controllo on-line dello stato dei certificati digitali
OdR	Operatore di registrazione
OID	Object identifier
ISO	International Standard Organization
TSA	Time Stamping Authority (sistema di marcatura temportale)
SP	Security Procedures – procedure di sicurezza Aruba PEC S.p.a
WWW	Web World Wide Web
X.509	specifica ITU-T in materia di certificazione e relativo framework di autenticazione

Cap. 2 Dati identificativi - Pubblicazione Manuale Operativo

2.1 Dati identificativi del certificatore (art. 38/3/a)

Denominazione Sociale : **Aruba PEC S.p.A.**
Indirizzo della sede legale : **Via Sergio Ramelli, 8 – 52100 - Arezzo**
Legale Rappresentante : **Dott. Giorgio Cecconi**
N° REA : **145843**
N° iscrizione al Registro delle imprese : **01879020517**
N° Partita IVA : **01879020517**
N° Telefono (centralino) : **+39 0744 5459227**
N° FAX : **+39 0575 515790**
e-mail PEC : **direzione.ca@arubapec.it**
ISO OID (private enterprise number) : **1.3.6.1.4.1.29741**
Web server principale : **http://www.arubapec.it**
Web server firma digitale : **https://ca.arubapec.it**

2.2 Versione del manuale operativo (art. 38/3/b)

Il presente Manuale Operativo è di proprietà di Aruba PEC S.p.A., tutti i diritti sono ad essa riservati. Questo documento è la versione 1.0 del Manuale Operativo del Servizio di Certificazione Digitale individuato da codice interno 1810LM0007, erogato da Aruba PEC S.p.A..

2.3 Pubblicazione del manuale

Ai sensi dell'art. 38, comma 2, del Decreto del Presidente del Consiglio dei Ministri (DPCM) 13/01/2004 questo documento è pubblicato sul web server principale e sul web server firma digitale con collegamento alla URL evidenziato e reperibile sulle pagine principali dei web server citati.

2.4 Responsabile del manuale operativo (art. 38/3/c)

Il responsabile del presente manuale operativo è :

Libero Marconi
Direttore servizi di certificazione
Aruba PEC S.p.A.

Tel. +39 0744 5459227
Fax. +39 0575 515790
E-mail: CPS-requests@ca.arubapec.it

Cap. 3 Disposizioni generali

3.1 Obblighi del titolare e del certificatore di quanti accedono per la verifica delle firme (art. 38/3/d)

1. Il titolare del certificato di firma è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri ed a custodire e utilizzare il dispositivo di firma con la diligenza del buon padre di famiglia.
2. Il certificatore è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri, ivi incluso il titolare del certificato.
3. Il certificatore che rilascia, ai sensi dell'articolo 29 del CAD, certificati qualificati deve inoltre:
    a. provvedere con certezza alla identificazione della persona che fa richiesta della certificazione;
    b. rilasciare e rendere pubblico il certificato elettronico nei modi o nei casi stabiliti dalle regole tecniche di cui all'articolo 71 del CAD, nel rispetto del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni;
    c. specificare, 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;
    d. attenersi alle regole tecniche di cui all'articolo 71 del CAD;
    e. informare 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;
    f. non rendersi depositario di dati per la creazione della firma del titolare;
    g. procedere 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, di provvedimento dell'autorita', di acquisizione della conoscenza di cause limitative della capacita' del titolare, di sospetti abusi o falsificazioni, secondo quanto previsto dalle regole tecniche di cui all'articolo 71 del CAD;
    h. garantire 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;
    i. assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
    j. tenere 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;
    k. non copiare, nè conservare, le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione;
    l. predisporre 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 certificatore;
    m. utilizzare sistemi affidabili per la gestione del registro dei certificati con modalita' tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticita' 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 requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato.

4. Il certificatore è responsabile dell'identificazione del soggetto che richiede il certificato qualificato di firma anche se tale attività è delegata a terzi.
5. Il certificatore raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono.

3.1.1 Obblighi di coloro che accedono alla verifica delle firme.

Il registro dei certificati di Aruba PEC S.p.A. è una raccolta di database disponibile al pubblico per l'archiviazione e il reperimento di certificati e altre informazioni a essi relative. I contenuti del registro dei certificati di Aruba PEC S.p.A. includono: certificati, liste dei certificati revocati o sospesi, e altre informazioni fornite occasionalmente da Aruba PEC S.p.A. Tutti coloro che intendono utilizzare documenti sottoscritti con firma digitale dovranno preventivamente consultare, in modo scrupoloso, il registro dei certificati di Aruba PEC S.p.A..
In particolare, coloro che intendono utilizzare documenti sottoscritti con firma digitale dovranno:

1. verificare le informazioni contenute nel certificato relative alla chiave pubblica della coppia di chiavi utilizzata per la firma ;
2. verificare la data di scadenza del certificato;
3. verificare lo stato del certificato (se è valido, se è stato revocato o sospeso);
4. verificare che la firma digitale sia stata apposta nel periodo di validità del certificato;
5. verificare che il messaggio associato non sia stato modificato e/o alterato.

3.2 Obblighi connessi al trattamento dei dati personali

3.2.1 Definizione di dato personale

Ai sensi dell'art. 1 comma 2 lett. B) del DLGS 196 per dato personale si intende "qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione, identificati o identificabili, anche mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
Dati personali saranno anche quelli relativi all'utente ovvero ad eventuali terzi e contenuti nei campi informativi presenti sui moduli e negli archivi – elettronici e/o cartacei – di registrazione, di richiesta di sospensione, di riabilitazione, di revoca, di cambio anagrafica e nei certificati di cui al presente manuale operativo.
Alla luce del dato normativo, quindi, sono da considerarsi dati personali anche i codici identificativi forniti dal Certificatore, i puntatori ed i PIN.

3.2.2 Tutela e diritti degli interessati

In materia di trattamento dei dati personali ARUBA PEC S.p.A. garantisce la tutela degli interessati in ottemperanza al DLGS 196. In particolare:

1. agli interessati sono fornite le necessarie informazioni ai sensi dell'art. 13 DLGS 196
2. nella suddetta informativa gli utenti saranno informati sui diritti di accesso ai dati personali ed altri diritti. (art. 7 DLGS 196)

Agli interessati verrà chiesto il consenso scritto al trattamento dei propri dati personali da parte di ARUBA PEC S.p.A..

3.2.3 Modalità del trattamento

I dati personali sono trattati con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti. Specifiche misure di sicurezza, come descritte nel presente manuale operativo, sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.
I dati saranno gestiti elettronicamente, secondo le leggi in vigore e archiviati nei server ubicati presso la sede operativa di Aruba PEC S.p.A., in Piazzale Bosco 3/A, 05100 Terni, Italia. I dati in formato cartaceo saranno conservati negli archivi cartacei di ARUBA PEC S.p.A., a tali dati avranno diritto di accesso solo gli incaricati a ciò espressamente autorizzati.

3.2.4 Finalità del trattamento

Erogazione del servizio:
richieste di certificati ed emissione degli stessi. I dati raccolti saranno utilizzati per l'iscrizione del richiedente, nonché per l'emissione, la sospensione, la revoca e la gestione dei certificati. Aruba PEC S.p.A., inoltre, utilizzerà le informazioni esclusivamente per lo svolgimento del servizio di certificazione e di ogni altra attività connessa e derivante da tale servizio quale, a mero titolo esemplificativo, la gestione della fatturazione. Eventuali controlli sulla qualità dei servizi e di sicurezza del sistema senza procedere, in alcun modo, alla sua profilazione. Scopi di natura commerciale, ciò ARUBA PEC S.p.A. potrà utilizzare le coordinate di posta elettronica fornite al momento della sottoscrizione del contratto per inviare comunicazioni relative a prodotti e/o servizi analoghi a quelli acquistati salva in ogni caso la possibilità dell'interessato di opporsi a tale trattamento.

Altre forme di utilizzo dei dati:
ARUBA PEC S.p.A., per motivi d'ordine pubblico, nel rispetto delle disposizioni di legge per la sicurezza e difesa dello Stato, per la prevenzione, accertamento e/o repressione dei reati, i dati forniti potranno essere usati con altre finalità rispetto alla fornitura dei servizi ed essere comunicati a soggetti pubblici, quali forze dell'ordine, Autorità pubbliche e autorità Giudiziaria, per lo svolgimento delle attività di loro competenza.

3.2.5 Sicurezza dei dati

Come previsto dalle norme vigenti in materia, Aruba PEC S.p.A adotta idonee e preventive misure di sicurezza al fine di ridurre al minimo:

i rischi di distruzione o perdita, anche accidentale, dei dati, di danneggiamento risorse hardware su cui sono registrati ed i locali ove vengono custoditi;
l'accesso non autorizzato ai dati stessi;
le modalità di trattamento non consentite dalla legge o dai regolamenti aziendali.

Le misure di sicurezza adottate assicurano:

1. l'integrità dei dati, da intendersi come salvaguardia dell'esattezza dei dati, difesa da manomissioni o modifiche da parte di soggetti non autorizzati;
2. la disponibilità dei dati da intendersi come la certezza che l'accesso sia sempre possibile quando necessario; indica quindi la garanzia di fruibilità dei dati e dei servizi, evitando la perdita o la riduzione dei dati e dei servizi anche accidentale utilizzando un sistema di backup e di disaster recovery;
3. la riservatezza dei dati da intendersi come garanzia che le informazioni siano accessibili solo da persone autorizzate e come protezione delle trasmissioni e controllo degli accessi stessi.

3.3 Limitazioni di Responsabilità ed eventuali limitazioni agli indennizzi (art. 38/3/e)

La sezione illustra le limitazioni di responsabilità assunte dal Certificatore nell'esercizio della propria attività.

3.3.1 Conoscenza del manuale operativo

Il richiedente il certificato, il Titolare del certificato e coloro i quali intendono accedere alla verifica delle firme sono tenuti a consultare preventivamente ed a conoscere il presente Manuale Operativo, le modalità in esso contenute per le operazioni di certificazione e di verifica delle firme. E' espressamente esclusa ogni responsabilità del Certificatore che sia derivante dalla non conoscenza o dal non corretto utilizzo delle procedure descritte nel presente manuale.

3.3.2 Forza Maggiore

La responsabilità del Certificatore sarà esclusa nel caso di eventi che esulino dalla propria volontà o da cause a lui non imputabili. Il Certificatore quindi non sarà responsabile per i danni di qualsiasi natura, da chiunque subiti e causati da caso fortuito o forza maggiore, impossibilità della prestazione, ordine o divieto dell'autorità quali, a titolo esemplificativo e non esaustivo, mancato funzionamento di reti o apparati tecnici al di fuori del controllo del Certificatore, interruzione nella fornitura di energia elettrica, allagamenti, incendi, azioni di guerra, epidemie, colpi di stato, terremoti e altri disastri.

3.3.3 Declinazioni e Limitazioni del Certificatore

Il Certificatore una volta terminata la fase di registrazione, non ha alcun ulteriore obbligo di verifica della validità dei dati e delle informazioni contenute nella richiesta di registrazione ed eventualmente nel certificato; non assume alcun ulteriore obbligo, garanzia o responsabilità rispetto a quanto previsto nel presente Manuale Operativo, ovvero dalle vigenti disposizione di legge, e non sarà responsabile per i danni di qualsiasi natura, da chiunque subiti, qualora tali danni derivino dalla violazione di quanto previsto e contenuto nel presente Manuale Operativo, ovvero dalle vigenti disposizione di legge.

3.3.4 Manleva

Il richiedente e/o il Titolare del certificato manlevano e tengono indenne il Certificatore ed i suoi aventi causa da qualsiasi responsabilità, spesa, pregiudizio o danno, diretto o indiretto, derivante da pretese o azioni giudiziali da parte di terzi di cui esso Certificatore sia chiamato a rispondere nei confronti dei terzi per fatto imputabile al richiedente e/o al Titolare del certificato, ivi espressamente incluse, a titolo esemplificativo e non esaustivo, le responsabilità e i danni derivanti dalla eventuale erroneità o non attualità delle informazioni o dei dati rilasciati al Certificatore; dal non corretto utilizzo delle procedure descritte nel presente Manuale

Operativo; dall'erroneo utilizzo di più codici identificativi attribuiti al medesimo soggetto per ciascuno dei ruoli per cui esso stesso può firmare; dall'utilizzo di pseudonimi, ecc..

3.3.5 Esclusione di risarcibilità di danni indiretti

Salvo i casi di dolo o colpa grave il Certificatore non sarà responsabile di alcun danno indiretto o di qualsiasi perdita di profitto e/o perdita dei dati o altri danni indiretti e conseguenti derivanti o collegati all'utilizzo, consegna, licenze, prestazioni o mancate prestazioni di certificati, firme digitali o qualsiasi altra transazione digitale o servizio offerto o contemplato dal presente Manuale Operativo.

3.3.6 Limitazioni di responsabilità

La responsabilità complessiva del Certificatore nei confronti di tutte le parti (inclusi il Titolare, il richiedente, il destinatario o l'utente utilizzatore) non supererà gli importi di seguito, con riferimento alla totalità di tutte le firme digitali e transazioni relative a tale certificato:

Limite di indennizzo : € 1.000.000,00 per sinistro e in aggregato annuo

3.3.7 Attività pericolose

Il servizio di certificazione offerto da Aruba PEC S.p.A. non è studiato, inteso o autorizzato per l'uso o la vendita come dispositivi di controllo in circostanze pericolose, o l'impiego in situazioni che richiedano un ambiente a prova di errore, come la gestione di impianti nucleari, sistemi di navigazione o comunicazione aerea, sistemi di controllo del traffico aereo o sistemi di comunicazione, sistemi di controllo d'armi, in cui un eventuale guasto comporterebbe direttamente decesso, danni alla persona, o gravi danni ambientali.

3.4 Tariffe del servizio(art. 38/3/f)

Le tariffe del servizio sono pubblicate sul sito web del servizio di certificazione https://ca.arubapec.it

Cap. 4 Operatività

Questa sezione descrive le modalità con le quali opera il Certificatore ed in particolare le funzioni del personale addetto al servizio di certificazione, le modalità di richiesta del certificato, di identificazione del richiedente e le modalità di comunicazione con il richiedente il certificato ovvero con il Titolare del certificato.

4.1 Funzioni del personale addetto al Servizio di Certificazione per Firma Digitale

Tutto il personale di Aruba PEC S.p.A. è stato assunto nel rispetto di politiche rigorose volte ad accertarne, tra l'altro, l'alto grado di professionalità nonché i requisiti morali e di onorabilità. Il personale addetto al Servizio di Certificazione per Firma Digitale nel rispetto dell'art. 33 del DPCM prevede, per ogni settore operante nella attività, le seguenti figure responsabili:

a) responsabile della sicurezza;

b) responsabile della generazione e custodia delle chiavi;

c) responsabile della personalizzazione dei dispositivi di firma;

d) responsabile della generazione dei certificati;

e) responsabile della gestione del registro dei certificati;

f) responsabile della registrazione degli utenti;

g) responsabile della sicurezza dei dati;

h) responsabile della crittografia o di altro sistema utilizzato;

i) responsabile dei servizi tecnici;

l) responsabile delle verifiche e delle ispezioni (auditing);

m) responsabile del sistema di riferimento temporale.

Alcune figure professionali possono svolgere più funzioni tra loro compatibili.

Le funzioni sopra elencate possono avvalersi, per lo svolgimento delle funzioni di loro competenza, di addetti ed operatori.

Gli operatori di Registrazione possono eventualmente operare presso sedi remote, rispetto al processing center presso Aruba PEC sede di Terni, e scambiare informazioni con il sito principale mediante canali sicuri ed identificazione certa dell'operatore stesso

4.2 Centri Di Registrazione Locale (CDRL)

Per consentire una diffusione sul territorio delle pratiche operative, le funzioni di registrazione possone essere svolte anche da terze parti. Tali terze parti possono operare successivamente alla stipula di un contratto con Aruba PEC in cui la terza parte indica il proprio personale, che sarà definito Operatore di Registrazione (O.d.R.), che dovrà operare nel contesto delle pratiche operative di registrazione. L'autorizzazione e successivamente la qualificazione degli O.d.R. come abili alle operazioni di registrazione, avviene mediante corso di formazione e superamento di un verifica scritta. A seguito della firma da parte dei rispettivi legali rappresentati del certificatore e del CDRL e previa qualificazione degli OdR, il certificatore rende disponibili agli OdR stessi, gli strumenti telematici sicuri per consentire lo svolgimento delle attività di registrazione e di sospensione e di revoca dei certificati. I privilegi di accesso agli strumenti telematici sicuri e le operazioni degli OdR sono sotto il costante controllo del certificatore.

4.3 Modalità di identificazione e registrazione degli utenti (art. 38/3/g)

L'identificazione e registrazione degli utenti avviene attraverso una procedura che si articola in diverse fasi alcune delle quali attraverso canali sicuri (HTTPS) altre attraverso la necessaria presenza fisica del richiedente il certificato dinanzi ad un responsabile di registrazione ovvero ad un operatore equivalente. I moduli per effettuare la richiesta di certificato si trovano presso gli uffici del Certificatore ovvero possono essere direttamente stampati dal richiedente attraverso il sito internet del Certificatore. Le fasi possono essere suddivise nel seguente modo:

1. invio della richiesta mediante un modulo disponibile presso gli uffici del Certificatore ovvero attraverso la compilazione di un modulo disponibile attraverso il server web firma digitale;
2. verifica delle informazioni contenute nel modulo di richiesta e registrazione;
3. presenza personale del soggetto richiedente il certificato dinanzi ad un addetto alla registrazione con contestuale presentazione di documento di riconoscimento legalmente valido, copia cartacea della richiesta del certificato preventivamente compilata in ogni sua parte e debitamente sottoscritta ed eventuale ulteriore documentazione necessaria al rilascio del certificato;
4. autenticazione e validazione (identificazione) da parte del personale addetto con conseguente accettazione o rifiuto della richiesta.

In particolare, le attività di identificazione e validazione dei richiedenti il certificato possono essere effettuate sia direttamente da dipendenti del Certificatore - presenti nelle proprie sedi dislocate sul territorio - sia da Notai o Pubblici Ufficiali ai quali il Certificatore ha conferito specifici incarichi, sia da altri soggetti debitamente incaricati ed autorizzati dal Certificatore quali i CDRL.
In ogni caso la responsabilità delle operazioni di registrazione, identificazione e validazione è di Aruba PEC S.p.A..
Per poter sottoscrivere la richiesta è necessario aver compiuto il diciottesimo anno di età.

4.3.1 Modalità di Richiesta del certificato e Registrazione del richiedente.

Le comunicazione tra il Certificatore ed il richiedente il certificato ovvero tra il Certificatore ed il Titolare del certificato avvengono attraverso una sessione sicura, protetta da un certificato SSL a 128 bit.
La richiesta del certificato può avvenire o presso gli uffici del certificatore dislocati sul territorio ovvero ricorrendo ai CDRL. Il richiedente deve obbligatoriamente fornire al personale preposto al ricevimento della richiesta le sottoelencate informazioni:

- nome e cognome, (*)
- data di nascita,
- comune, provincia e stato estero di nascita,
- codice fiscale, (*)

- indirizzo di residenza, eventualmente all'estero,
- indirizzo di posta elettronica, (*)
- tipo e numero del documento d'identità o del documento di riconoscimento equipollente esibito,
- eventuali abilitazioni professionali . (*)
- eventuali poteri di rappresentanza, (*)
- eventuale pseudonimo da inserire nel certificato in luogo del nome di battesimo e cognome del titolare ai sensi dell'art. 33 del CAD e della lettera e), comma 3 dell'art.4 della DELIB 4/05. (*)

(*) Tutti i dati contrassegnati con l'asterisco sono inseriti nel certificato, tranne nel caso di utilizzo dello pseudonimo (in tal caso solo lo pseudonimo ed il paese di residenza sono inseriti nel certificato).

Durante tale procedura il sistema provvede ad assegnare automaticamente un codice identificativo univoco nell'ambito del proprio archivio di utenti; a tal proposito il codice identificativo sarà diverso nel caso che un medesimo richiedente possieda più certificati per diversi ruoli.
Tutte le informazioni inviate in tale modalità vengono raccolte dal Certificatore ed archiviate nel database di registrazione in automatico, ed al termine della procedura di richiesta, il richiedente riceve un messaggio e-mail inviato automaticamente che conferma la presa visione della richiesta da parte di Aruba PEC., contenente informazioni generali..
Ricevuta la richiesta, un operatore provvede, attraverso una postazione amministrativa sicura, all'avvio delle procedure di verifica delle informazioni contenute nel modulo di registrazione.

4.3.2 Presenza fisica del richiedente dinanzi ad un incaricato del Certificatore

Il richiedente dovrà, successivamente alla compilazione del modulo di registrazione, comparire personalmente dinanzi ad un incaricato del certificatore per fornire :

1. Documento di identità (almeno un documento in corso di validità tra i seguenti: carta di identità, passaporto, patente auto, tessere di riconoscimento del personale di Amministrazioni Statali, libretto di pensione INPS con foto e firme autenticate).
2. Copia cartacea della richiesta - sulla base del modulo di registrazione - completata in ogni sua parte e sottoscritta dal richiedente.
3. Firmando il modulo di registrazione, il richiedente:
    a. fornisce tutti i dati personali necessari per la registrazione;
    b. si assume esplicitamente gli obblighi di cui all'art. 32, comma 1 del CAD;
    c. si assume esplicitamente gli obblighi di cui all'art. 7, comma 3 del DPCM;
    d. dichiara di aver preso visione del Manuale Operativo e di averlo compreso ed accettato;
    e. acconsente al trattamento dei propri dati personali nel rispetto del DLGS 196 e dell'informativa fornita.
4. Nel modulo di registrazione, inoltre, il richiedente può fornire la propria autorizzazione alla pubblicazione del certificato.
5. Solo nel caso di rilascio di certificato destinato ad essere utilizzato in funzione di un ruolo ovvero in funzione di titoli relativi all'esercizio della professione (avvocato, ingegnere, medico, ecc.), ovvero di una carica rivestita presso organizzazioni terze, la Documentazione necessaria che comprovi la sussistenza dei requisiti di abilitazione alla professione ovvero la sussistenza dei poteri di rappresentanza, delle cariche o dei titoli che si dichiarano nel certificato.

La copia cartacea del Modulo di registrazione costituirà elemento indispensabile per completare il processo di richiesta ed il processo di autenticazione e validazione.
Le informazioni contenute nei certificati, qualora venga espressamente richiesto dal richiedente e sia consentito dal Certificatore, possono essere sostituite nel certificato da uno pseudonimo.
Il Certificatore indica esplicitamente nel certificato la presenza di uno pseudonimo in luogo dei dati anagrafici è conserva le informazioni relative alla reale identità del Titolare per almeno 20 anni dopo la scadenza del certificato.

La Aruba PEC S.p.A. si fa inoltre carico della conservazione delle copie cartacee delle richieste per un periodo non inferiore a 20 anni.

4.3.3 Identificazione del richiedente

La verifica dell'identità del richiedente viene definita da Aruba PEC S.p.A. autenticazione e validazione; essa consiste nella seguente procedura e richiede la presenza fisica del richiedente presso l'operatore di registrazione e per ciascuna richiesta di certificato sono verificate le seguenti informazioni:

1. Verifica della corretta compilazione e sottoscrizione autografa della richiesta cartacea del certificato.
2. Verifica dell'esistenza dell'indirizzo e-mail per il quale si richiede il certificato, effettuata attraverso un apposito software.
3. Nome, Cognome, data di nascita e codice fiscale forniti in fase di registrazione;

questi dati sono confrontati con quelli contenuti in un documento di identità valido (carta d'identità o patente di guida o passaporto da esibirsi unitamente al tesserino del codice fiscale) presentato personalmente dal richiedente. In questa fase un operatore di registrazione che provvede alle procedure di autenticazione e validazione riceve dalle mani del richiedente i documenti sopra indicati e verifica che la persona che ha di fronte sia effettivamente il richiedente. La presenza fisica del richiedente presso l'operatore di registrazione deve quindi considerarsi necessaria ed indispensabile ai fini del rilascio del certificato richiesto. Se il richiedente ha compilato il campo "TITOLO" della richiesta al fine di descrivere i propri poteri di rappresentanza o abilitazioni professionali, dovrà produrre idonea documentazione atta a documentare e dimostrare quanto dichiarato nella richiesta. Tale documentazione sarà allegata dal Certificatore in formato cartaceo alla pratica di richiesta e conservata con la medesima cura della richiesta stessa. Al termine di tutte le suddette verifiche, l'incaricato del Certificatore approva o rigetta la richiesta. Nel caso di rigetto della richiesta il Certificatore ne informa tempestivamente il richiedente indicando i motivi che hanno provocato il rigetto stesso. Il richiedente che si vede rigettata la richiesta può formulare una nuova richiesta. Il rigetto della richiesta esonera il Certificatore da qualsiasi responsabilità, pregiudizio e/o danno, diretto e/o indiretto che possa derivare da tale rifiuto. Nel caso di accettazione della richiesta, il Certificato viene emesso ed inserito nel dispositivo di firma contenente la chiave privata relativa alla chiave pubblica riportata nel certificato medesimo. Il Certificatore è responsabile in ogni caso nei confronti di terzi circa la identificazione del Titolare. La eventuale erroneità o la falsità dei documenti prodotti per la identificazione del Titolare, non limita la responsabilità del Certificatore nei confronti di terzi.

4.4 Dispositivo di firma

4.4.1 Fornitura del dispositivo di firma

Tutti i certificati emessi dal Certificatore devono essere inseriti in un dispositivo di firma contenente la chiave privata relativa alla chiave pubblica riportata nel certificato medesimo. Prima di avviare le procedure di richiesta, il richiedente dovrà munirsi del dispositivo di firma richiedendolo a Aruba PEC S.p.A. ovvero acquisendolo da un terzo fornitore a patto che il dispositivo sia conforme alle specifiche di utilizzo di Aruba PEC S.p.A. e dalla stessa approvato nonché conforme alle caratteristiche ed ai requisiti di sicurezza di cui all'art. 35 del CAD ed all'art. 9 comma 1, 2 e 3 del DPCM.

4.4.2 Impiego del dispositivo di firma

La Aruba PEC S.p.A. garantisce il corretto funzionamento del dispositivo di firma a condizione che venga utilizzato con software preventivamente approvato dalla propria Direzione dei servizi di certificazione.

4.4.3 Personalizzazione del dispositivo di firma

Il dialogo per l'acquisizione dei dati identificativi dal dispositivo di firma e l'associazione al Titolare e relativa restituzione verso il dispositivo di firma, avviene tramite canale sicuro ed è automatizzata attraverso procedure di dialogo tra il software che utilizza il dispositivo di firma e processi software in esecuzione sui server di Aruba PEC S.p.A..

4.5 Modalità di generazione delle chiavi (art. 38/3/h)

Questa sezione descrive le modalità di generazione delle coppie di chiavi crittografiche.

Coppie di chiavi generate nell'attività di certificazione

La generazione delle chiavi di certificazione costituisce il primo passo nel procedimento di creazione di una CA (Certification Authority), per l'esercizio della attività di CA e può essere effettuata soltanto dal responsabile del servizio che utilizzerà le chiavi Le chiavi di certificazione sono destinate alla generazione ed alla verifica delle firme apposte ai certificati ed alle loro liste di revoca/sospensione (CRL/CSL), mentre le chiavi di sottoscrizione sono destinate alla generazione e verifica delle firme apposte o associate ai documenti. Il termine 'coppia di chiavi' si riferisce a due chiavi strettamente legate tra di loro: la chiave pubblica e la privata. La chiave privata viene conservata all'interno dell'area protetta un dispositivo hardware sicuro. La chiave pubblica è visibile nel certificato pubblico della CA ed è strettamente legata alla informazioni che identificano univocamente la CA per il Servizio di Certificazione per Firma Digitale. Le chiavi generate dal Certificatore sono conformi all'algoritmo RSA sono generate (art. 6, comma 3), conservate (art. 7) ed utilizzate (art. 9, comma 1) all'interno di uno stesso dispositivo elettronico avente le caratteristiche di sicurezza di cui all'art. 9, comma 3 del DPCM..

Nell'attività di certificazione, vengono generate tre diverse tipologie di chiavi:

1. chiavi di certificazione generate dal Certificatore per uso proprio e destinate a firmare i certificati relativi a chiavi di sottoscrizione e marcatura temporale emessi dal Certificatore nonché le relative liste di revoca e sospensione;
2. chiavi di sottoscrizione , generate dai sottoscrittori, destinate alla generazione e verifica delle firme apposte o associate ai documenti;
3. chiavi di marcatura temporale destinate alla generazione e verifica delle marche temporali.

4.5.1 Modalità di generazione delle chiavi di certificazione

Questa avviene nel rispetto dell'art. 13 del DPCM. Una delle funzioni più importanti svolte sotto il controllo del responsabile della generazione e custodia chiavi in presenza del responsabile del servizio tecnico o sotto la sua supervisione, è finalizzata alla generazione ed alla configurazione delle coppie di chiavi di certificazione. Le chiavi di certificazione vengono generate durante un apposito processo (c.d. "Cerimonia di generazione delle chiavi") costituito da un insieme di procedure formali ed altamente sicure, tramite le quali viene creata ed emessa una CA ; il tutto con l'ausilio di un particolare e sofisticato software ('CA Key Management Tool'). Tale software viene utilizzato esclusivamente per la generazione delle coppie di chiavi e certificati relativi alla CA. Le procedure eseguite durante la " Cerimonia di generazione delle chiavi" con l'ausilio del software sopra citato, assicurano l'unicità e la robustezza delle coppie di chiavi che vengono generate, nonché la segretezza della chiave privata. Ogni "Cerimonia di generazione delle chiavi" si svolge in locali adeguatamente protetti e controllati, locali nei quali, a causa di una rigorosa politica di sicurezza interna, non è consentito l'accesso e la permanenza di una sola persona. I locali ove si svolge la "Cerimonia di generazione delle chiavi" sono inoltre dotati di sofisticati impianti di allarme, telecamere, microfoni, rilevatori di movimento (che si attivano soltanto quando nessuna persona vi è presente), al fine di controllare ogni movimento all'interno degli stessi. Per ciascuna chiave di certificazione generata durante una

"Cerimonia di generazione delle chiavi", il Certificatore genera un certificato sottoscritto con la chiave privata della coppia cui il certificato si riferisce. Queste chiavi, ai sensi dell'art. 6, comma 1 del DPCM, sono generate sotto il controllo del responsabile della generazione e custodia chiavi in presenza del responsabile del servizio tecnico o sotto la sua supervisione. Tramite il software chiamato 'CA Key Management Tool' si generano le chiavi direttamente all'interno del dispositivo di firma. Le chiavi private pertanto risiedono su di un dispositivo hardware di firma (HSM). Per generare coppie di chiavi su HSM, viene utilizzata una specifica workstation, equipaggiata del software 'CA Key Management Tool', installata all'interno degli appositi locali ove si svolge la "Cerimonia di generazione delle chiavi" e isolata da qualsiasi rete dati.

4.5.2 Modalità di generazione delle chiavi di sottoscrizione degli utenti

Le chiavi di sottoscrizione degli utenti sono generate dagli utenti stessi o dal Certificatore, rif. art. 6, comma 2, del DPCM. Detta generazione avviene all'interno di un dispositivo di firma hardware (smart-card), obbligatoriamente attivato da software approvati da Aruba PEC S.p.A che sono in grado di garantire livelli di sicurezza analoghi a quelli previsti per la generazione delle chiavi di certificazione e marcatura temporale. La chiave privata del titolare rimane all'interno del dispositivo di firma hardware la cui attivazione per scopo di firma è ulteriormente controllata da un apposito PIN (Numero Identificativo Personale).

4.5.3 Modalità di generazione delle chiavi di marcatura temporale

Questa avviene nel rispetto dell'art. 46 del DPCM. La generazione delle chiavi viene sotto il controllo del responsabile del servizio di marcatura temporale in presenza del responsabile del servizio tecnico o sotto la sua supervisione. La coppia di chiavi utilizzata per la validazione temporale viene associata in maniera univoca ad un sistema di validazione temporale. Le chiavi di marcatura temporale vengono sostituite ogni mese. La sottoscrizione dei certificati relativi a chiavi di marcatura temporale avviene con chiavi di certificazione diverse da quelle utilizzate per le chiavi di sottoscrizione.

4.6 Modalità di emissione dei certificati (art. 38/3/i/l)

Questa sezione descrive le modalità di emissione, generazione, invio e pubblicazione dei certificati.

4.6.1 Richiesta del certificato

La certificazione della coppia di chiavi da parte del Titolare viene ottenuta dopo una appropriata richiesta definita nel paragrafo 4.3.1 del presente manuale operativo. Il software e il dispositivo di firma utilizzati nel processo di richiesta devono essere approvati da Aruba PEC. Per la generazione della coppia di chiavi, il Titolare deve procedere come riportato al paragrafo 4.5.2 del presente manuale operativo. L'invio della chiave pubblica e la prova di possesso della chiave privata deve avvenire secondo la specifica PKCS#10.

4.6.2 Generazione del certificato

La generazione del certificato avviene, nel rispetto dell'art. 14 del DPCM, secondo la seguente procedura:
si accerta l'autenticità della richiesta, provvedendo alla identificazione del richiedente, alla verifica dell'autenticità della richiesta;

1. si richiede la prova del possesso della chiave privata e verifica il corretto funzionamento della coppia di chiavi;

2. si provvede a pubblicare e inserire gli stessi nel proprio registro dei certificati, con attestazione del momento della pubblicazione mediante un riferimento temporale che verrà conservata fino alla scadenza della validità delle chiavi;
3. si invia al titolare il certificato emesso unitamente al relativo riferimento temporale;
4. si provvede a fornire al titolare di ciascun certificato emesso un codice riservato da utilizzare, in caso di emergenza, per l'autenticazione della eventuale richiesta di revoca del certificato;
5. si provvede a registrare la generazione di ciascun certificato nel giornale di controllo.

Il profilo del certificato è conforme alla DELIB 4/05 e contiene le informazioni previste nell'art. 15 del DPCM e nell'art. 28 del CAD e successive correzioni ed integrazioni. Attributi ed estensioni facoltativi possono variare in rapporto alle specifiche policy utilizzate, previamente concordate con il cliente. Il periodo di validità può variare tra 2 a 3 anni.

Qualora esistano delle condizioni che impediscano la generazione del certificato, l'operatore provvede a rigettare la richiesta del Titolare richiedente e a segnalargli l'evento. Tale evento di rigetto di richiesta viene registrato nel giornale di controllo.

4.6.3 Invio e Pubblicazione del certificato

Al buon fine della procedura di generazione il certificato viene inviato al Titolare insieme al riferimento temporale attraverso un meccanismo che prevede un invio tramite e-mail, all'indirizzo fornito in fase di richiesta e verificato in fase di identificazione, di un codice di identificazione per il prelievo e la URL dalla quale prelevare il certificato tramite sessione sicura. Attraverso la sessione sicura SSL stabilita tramite il browser (es. internet explorer) del Titolare verso il sito del certificatore Aruba PEC, il certificato viene inserito automaticamente nella smart card previo inserimento del PIN della smart card stessa a cura del Titolare. Il PIN/PUK della smart card ed il codice di emergenza riservato per autenticare il Titolare per una eventuale richiesta di revoca e/o sospensione, sono consegnati in una busta retinata fornita separatamente dalla smart card. L'indirizzo internet del registro dove sono pubblicati i certificati, previa richiesta del Titolare, è indicato nella home page del web server di firma digitale https://ca.arubapec.it

Gli eventi di pubblicazione e di riferimento temporale sono registrati nel giornale di controllo.

4.7 Modalità di sospensione e revoca dei certificati (art. 38/3/m)

Questa sezione descrive le modalità di sospensione e revoca dei certificati.

4.7.1 Circostanze che impongono la sospensione o la revoca del certificato.

La sospensione o revoca del certificato avviene, nel rispetto degli artt. da 18 a 24 del DPCM, secondo le modalità e le procedure descritte nei paragrafi successivi.

Il Certificatore provvederà alla revoca ovvero alla sospensione del certificato digitale qualora si verifichi una delle seguenti circostanze:

1. Richiesta esplicita formulata dal Titolare (redatta per iscritto)
2. Richiesta da parte del "terzo interessato" (che deve essere inoltrata per iscritto ai sensi di quanto previsto all'art. 32 DPCM).
3. Richiesta nei casi di urgenza formulata telefonicamente dal Titolare o "terzo interessato", identificati mediante il codice riservato per l'autenticazione rilasciatogli al momento della emissione del certificato.
4. Il riscontro che il certificato non è stato rilasciato secondo le modalità previste dal presente Manuale Operativo ovvero in maniera non conforme alle modalità previste dalla normativa vigente.

5. Il riscontro di una avvenuta violazione degli obblighi incombenti sul richiedente e/o sul Titolare del certificato.
6. Compromissione della segretezza o rottura della chiave privata.
7. Smarrimento della chiave privata.
8. Abusi e falsificazioni.
9. Richiesta provenie nte dall'Autorità giudiziaria .

Il certificatore provvede ad inserire in stato di sospensione il certificato nel caso in cui non possa accertare in tempo utile l'autenticità della richiesta.

I certificati relativi a chiavi di certificazione possono essere revocati o sospesi solo in uno dei seguenti casi:

1. compromissione della chiave privata;
2. guasto del dispositivo di firma;
3. cessazione dell'attività.

4.7.2 Richiesta di sospensione o revoca da parte del Titolare.

La revoca/sospensione del certificato può essere effettuata dal Titolare dello stesso secondo tre diverse modalità:

la revoca/sospensione del certificato può essere richiesta dal Titolare dello stesso attraverso l'invio per iscritto di una esplicita richiesta formale inviata al Certificatore, che deve contenere :

1. tutte le indicazioni relative agli elementi di identificazione del Titolare e del certificato,
2. le ragioni per le quali si richiede la revoca/sospensione
3. essere firmata dal Titolare del certificato.

la revoca/sospensione del certificato può essere effettuata direttamente dal Titolare dello stesso attraverso il servizio disponibile presso il sito di Aruba PEC S.p.A. alla pagina del web server Firma Digitale esplicitamente dedicata alla revoca/sospensione evidenziata sulla pagina principale, utilizzando il codice riservato di emergenza consegnato insieme al PIN/PUK della smart card, in una busta retinata fornita separatamente dalla smart card a seguito della generazione del certificato. La revoca/sospensione del certificato può essere effettuata direttamente dal Titolare dello stesso attraverso il servizio telefonico disponibile al n. +39.0744.5459210, comunicando il codice riservato di emergenza consegnato insieme al PIN/PUK della smart card, in una busta retinata fornita separatamente dalla smart card a seguito della generazione del certificato. A detta richiesta dovrà comunque seguire comunicazione scritta con le ragioni per le quali si richiede la revoca/sospensione, firmata dal titolare del certificato. In particolare, la sospensione è uno strumento posto principalmente a tutela del Titolare del certificato allorquando non vi sia la possibilità di accertare in tempo utile l'autenticità di una richiesta di revoca e ragioni di urgenza impongano la cautelativa inefficacia del certificato. La sospensione del certificato determina la immediata cessazione della validità del certificato stesso.
Sia la revoca che la sospensione di un certificato sono pubblicate nelle liste CRL e tramite OCSP appositamente pubblicate e consultabili via internet.

4.7.3 Sospensione o revoca su iniziativa del Certificatore.

Avviene nel rispetto degli artt. 18 e 22 del DPCM.
La revoca/sospensione del certificato può essere eseguita su insindacabile iniziativa del Certificatore indipendentemente dalla volontà del Titolare qualora se ne ravvisi la necessità o si verifichi una delle seguenti circostanze:

1. sopravvenuta modifica dei dati personali riportati sul certificato o di altri dati riportati sul certificato;

2. conoscenza della avvenuta compromissione o rottura della chiave privata;
3. inadempimento agli obblighi incombenti sul Titolare del certificato e previsti dalla normativa vigente e/o dal presente Manuale Operativo;
4. uso improprio da parte del Titolare del certificato;
5. eventuale compromissione della chiave di certificazione o marcatura temporale relativa al certificato;
6. eventuale richiesta proveniente dall'Autorità Giudiziaria.

Il Certificatore provvederà a notificare al Titolare le ragioni della revoca, nonché la data e l'ora a partire dalla quale il certificato non è più valido.

4.7.4 Richiesta di sospensione o revoca da parte del terzo interessato

Avviene nel rispetto degli artt. 20 e 24 del DPCM.
La Richiesta di sospensione o revoca da parte del "terzo interessato" deve essere firmata e pervenire per iscritto alla Aruba PEC S.p.A.. La richiesta di revoca e/o sospensione può anche essere inoltrata via e-mail purché debitamente sottoscritta con il certificato digitale del "terzo interessato". Nei casi di particolare urgenza il "terzo interessato" potrà richiedere la revoca/sospensione del certificato attraverso il servizio telefonico disponibile al n. +39.0744.5459227, comunicando il codice riservato di emergenza consegnato insieme al PIN/PUK della smart card, in una busta retinata fornita separatamente dalla smart card a seguito della generazione del certificato. A detta richiesta dovrà comunque seguire comunicazione scritta a mezzo posta raccomandata o posta elettronica certificata all'indirizzo direzione.ca@arubapec.it con ragioni per le quali si richiede la revoca/sospensione. A mero titolo esemplificativo, i casi più frequenti in cui un "terzo interessato" può richiedere la sospensione o la revoca di un certificato sono qualora il terzo sia una organizzazione (ente, società, associazione, ecc) che abbia acquistato una serie di certificati e li abbia destinati a suoi dipendenti e/o fornitori e/o clienti e/o a persone, in qualunque modo, ad essa afferenti e:

1. siano modificati o terminati i rapporti tra la organizzazione ed il Titolare del certificato per qualsiasi motivo;
2. si siano verificati casi di dolo e/o infedeltà del dipendente per il quale la organizzazione ha richiesto il certificato;
3. si sia verificato il decadere del titolo o della carica o del ruolo inerente i poteri di rappresentanza o la qualifica professionale in virtù del quale il certificato è stato rilasciato.

Il Certificatore provvederà a comunicare al Titolare del certificato l'avvenuta richiesta di revoca e/o sospensione effettuata dal "terzo interessato". La Aruba PEC S.p.A. può rigettare la richiesta nel caso la giudichi non autentica, inesatta o incompleta e provvederà alla notifica del rigetto al "terzo interessato" richiedente.

4.7.5 Completamento della sospensione o revoca del certificato.

La revoca/sospensione del certificato può essere eseguita dagli operatori alle procedure di autenticazione/validazione attraverso il software preposto alla gestione di tutte le operazioni relative al ciclo di vita del certificato. Il certificato revocato/sospeso sarà inserito nella CRL e ne sarà data comunicazione al Titolare. Il momento di pubblicazione del certificato nella CRLsarà asseverato da un riferimento temporale e annotato nel giornale di controllo. La CRL viene pubblicata in maniera periodica ogni 60 minuti, in ogni caso eventi straordinari possono richiedere una pubblicazione più celere ed in questa circostanza la Aruba PEC S.p.A. può provvedere ad una pubblicazione immediata entro i tempi puramente tecnici degli elaboratori. Resta inteso che la consultazione della CRL è uno specifico dovere a cura degli utenti utilizzatori e di tutti coloro che intendono verificare la validità e l'operatività delle firme digitali connesse ai certificati.

4.8 Modalità di sostituzione delle chiavi (art. 38/3/n)

Questa sezione descrive le modalità di sostituzione delle chiavi di certificazione.

4.8.1 Sostituzione chiavi di sottoscrizione dei Titolari

Ai sensi dell'art. 15 comma 4 del DPCM, la Aruba PEC S.p.A. determina da un minimo di anni 2 (due) ad un massimo di anni 3 (tre) la durata dei certificati per firma digitale per chiavi RSA da 1024 bit, pertanto il periodo di validità delle chiavi dei Titolari di certificati per firma digitale coincide con la durata del certificato stesso. Con anticipo di 30 gg rispetto alla scadenza del certificato, la Aruba PEC S.p.A. comunica via e-mail all'indirizzo fornito dal Titolare e verificato in fase di identificazione, l'approssimarsi della scadenza. Per la sostituzione il Titolare dovrà procedere secondo le istruzioni che saranno fornite nella citata e-mail di avviso scadenza e che prevedono :

- smart card e lettore configurato e funzionante con relativo software di firma
- accesso ad internet disponibile
- un browser funzionante

i passi principali sono (sono escluse le pratiche amministrative di pagamento della sostituzione delle chiavi. Per i costi e le modalità si rimanda al sito web https://ca.arubapec.it) :

- ricezione a cura del Titolare tramite prelievo web alla URL indicata nella e-mail di avviso scadenza di un documento elettronico, firmato digitalmente, di richiesta di rinnovo inviato da Aruba PEC S.p.A.
- sottoscrizione a cura del Titolare della richiesta di rinnovo ricevuta mediante propria smart card prima della scadenza del proprio certificato che non deve essere in stato di revoca e/o sospensione
- invio a cura del Titolare della richiesta sottoscritta dal medesimo tramite invio web alla URL indicata nella e-mail di avviso scadenza
- previa verifica della validità della firma del Titolare, se positiva Aruba PEC S.p.A. genera dei codici di sostituzione chiavi di tipo "usa e getta" che debbono essere utilizzati entro 5 giorni dalla ricezione. Tali codici di sostituzione vengono inviati via e-mail al Titolare
- il Titolare ricevuta la e-mail contenente i codici di sostituzione deve utilizzare la URL indicata nella stessa e-mail per procedere in autonomia alle operazioni di generazione di una nuova coppia di chiavi, mediante l'uso guidato dalla procedura disponibile alla URL inviata e il PIN della propria smart card, utilizzando nella sottomissione della chiave pubblica i codici di sosituzione
- l'invio del certificato segue quanto descritto in 4.6.3.

4.8.2 Sostituzione delle chiavi di certificazione

Avviene nel rispetto dell'art. 25 del DPCM sotto il controllo del responsabile della generazione e custodia chiavi in presenza del responsabile del servizio tecnico o sotto la sua supervisione, è finalizzata alla sostituzione ed alla configurazione delle coppie di chiavi di certificazione. Il processo è analogo a quanto indicato in 4.5.1 ed avviene con almeno 3 mesi di anticipo rispetto alla scadenza del certificato relativo alla coppia di chiavi di certificazione da sostituire.

4.8.3 Sostituzione delle chiavi di marcatura temporale

Avviene nel rispetto dell'art. 46 del DPCM. Viene eseguita mensilmente sotto il controllo del responsabile del servizio di marcatura temporale in presenza del responsabile del servizio tecnico o sotto la sua supervisione. La procedura è analoga a quanto indicato in 4.5.3.

4.9 Modalità di gestione e di accesso del registro dei certificati (art. 38/3/o/p)

Questa sezione descrive le modalità di gestione del registro dei certificati, la sua funzione e pubblicazione.

4.9.1 Funzione e Pubblicazione del Registro dei certificati e delle CRL

Il Repository di Aruba PEC S.p.A. è una raccolta di dati (database) disponibile al pubblico mediante Internet attraverso un server LDAP utilizzato per l'archiviazione e il reperimento di certificati ed altre informazioni in essi contenute e ad essi relative. Aruba PEC S.p.A. provvederà alla tempestiva pubblicazione di tutti i certificati emessi, delle informazioni in essi contenute e la loro eventuale sospensione o revoca.

Nel Repository sono contenuti :

1. CRL
2. i certificati pubblici per le chiavi dei Titolari ove richiesto.
3. i certificati pubblici per le chiavi del Certificatore Aruba PEC S.p.A.
4. i certificati per le chiavi di firma del CNIPA
5. i certificati per interoperabilità con altri Certificatori iscritti nell'elenco pubblico dei certificatori CNIPA

TUTTI COLORO CHE INTENDONO FARE AFFIDAMENTO SU UNA FIRMA DIGITALE CONTENUTA IN UN CERTIFICATO E/O SULLE INFORMAZIONI IN ESSO CONTENUTE DEVONO CONSULTARE PREVENTIVAMENTE IL REPOSITORY DI ARUBA PEC AL FINE DI VERIFICARE (NELLE APPOSITE LISTE DI CERTIFICATI REVOCATI O SOSPESI, DISPONIBILI PER VIA TELEMATICA AGLI UTENTI – CRL E OCSP) SE IL CERTIFICATO SIA VALIDO E NON REVOCATO O SOSPESO E SE LA FIRMA DIGITALE SIA STATA CREATA DURANTE IL PERIODO OPERATIVO DEL CERTIFICATO STESSO DALLA CHIAVE PRIVATA CORRISPONDENTE ALLA CHIAVE PUBBLICA RIPORTATA NEL CERTIFICATO.

4.9.2 Realizzazione, sicurezza , copia e accesso del registro dei certificati

La copia di riferimento del registro dei certificati è mantenuta nel database di registrazione funzionante tramite un apposito DBMS, localizzato nella parte protetta a livello logico della rete interna di Aruba PEC S.p.A. ed in locali adeguatamente protetti. Tale copia è aggiornata in tempo reale ad ogni emissione di un certificato e l'effettuazione di operazioni che modificano il contenuto del registro sono possibili esclusivamente al personale espressamente autorizzato. La copia di riferimento è sincronizzata in automatico con eventi di sincronizzazione sottoposti aregistrazione in un apposito registro operativo, con una copia operativa. L'evento di aggiornamento della copia operativa avviene quotidianamente mediante l'impostazione di un file generato automaticamente per mezzo di una interrogazione del database di registrazione. Tale copia operativa è accessibile tramite internet in modo anonimo ed in sola lettura tramite il protocollo LDAP. Il prototipo di una richiesta LDAP è :

- ldap://directory.arubapec.trustitalia.it:389/NULL??sub?(mail=utente@dominio.tld).

4.9.3 Replica del registro operativo dei certificati

Il registro operativo viene duplicato su un elaboratore presente nel sito di disaster recovery di Aruba PEC presso una rete esterna al centro elaborazione della sede principale della CA di Aruba PEC., in modo da garantire la accessibilità del servizio anche nei casi di indisponibilità prolungate del centro elaborazione citato. Il metodo di accesso ed il percorso rimangono gli stessi, indicati nel web server firma digitale e nel presente manuale.

4.10 Modalità di protezione della riservatezza (art. 38/3/q)

4.10.1 Archivi contenenti dati personali.

Tutta la documentazione cartacea ed in formato elettronico raccolta durante le fasi di elaborazione delle richieste di certificato è conservata negli elaboratori utilizzati dagli addetti alle procedure di autenticazione e validazione in locali altamente sicuri.

4.10.2 Misure di tutela della riservatezza.

Aruba PEC è titolare dei dati personali raccolti in fase di identificazione e registrazione degli utenti che richiedono i certificati e si obbliga quindi a trattare tali dati con la massima riservatezza e nel rispetto di quanto previsto dal DLGS 196. Nel caso in cui l'attività di identificazione e registrazione degli utenti avvenga presso una struttura delegata CDRL quest'ultima è qualificata come "titolare di trattamento autonomo correlato".

4.10.3 Informativa ai sensi del D.Lgs. 196/03

Vale quanto indicato nel par. 3.2

4.11 Modalità per l'apposizione e la definizione del riferimento temporale (art.38/3/r)

4.11.1 Riferimento temporale

Il riferimento temporale è un'informazione contenente la data e l'ora associata ad uno o più documenti informatici. Il riferimento temporale è generato con un sistema che garantisce stabilmente uno scarto non superiore ad un minuto secondo rispetto alla scala UTC. Il riferimento temporale usato da Aruba PEC è ottenuto da un dispositivo di alta precisione e certificato per tale scopo che rileva il segnale radio fornito dallo IEN e lo inoltra ad un NTP server interno. Un riferimento temporale di backup è poi ottenuto dal segnale proveniente dal server NTP accessibile via internet dello IEN.

4.11.2 Marcatura temporale

Il servizio di marcatura temporale offerto da Aruba PEC S.p.A. è fruibile esclusivamente tramite software approvato e fornito dalla stessa Aruba PEC S.p.A. La richiesta viene accettata dal web server tsa.arubapec.it, tramite l'indirizzo https://tsa.arubapec.it/request.php (che deve essere configurato in Signo alla voce Strumenti->Opzioni->Marcatura Temporale->Server URL) con le credenziali fornite da Aruba PEC S.p.A. al momento dell'attivazione dell'account TSA (che devono essere inserite nel sofware Signo alle voci Strumenti->Opzioni->Marcatura Temporale->Login e Password). Le marche temporali prodotte dal servizio TimeStampingAuthority sono conformi alle strutture dati descritte del documento RFC3161.

4.11.3 Sicurezza logica e fisica del sistema di marcatura temporale

L'elaboratore che offre il servizio di marcatura temporale è dotato di hardware crittografico per la firma delle marche temporali che possiede i medesimi requisiti di protezione di quanto installato nell'elaboratore per la generazione dei certificati di firma digitale, ed è protetto da livelli di protezione logica estremamente elevati

essendo collocato nel centro elaborazione dati di Aruba PEC S.p.A. (backend). La medesima collocazione fisica nel "backend" garantisce l'elaboratore dalla possibilità di compromissioni fisiche grazie agli accorgimenti tecnici atti ad impedire accessi non autorizzati da persone e danneggiamenti da eventi accidentali. Il sistema per il servizio di marcatura temporale può essere attivato solo da operatori autorizzati tramite l'utilizzo di smar tcard. Una volta attivato, il sistema non necessita di ulteriori procedure interattive di login, tranne che per arrestarlo e riattivarlo a scopo di manutenzione. Un eventuale arresto del sistema può essere eseguito solamente dagli operatori autorizzati. Il sistema TSA dispone di uno specifico componente dedicato al monitoraggio delle seguenti condizioni:

- tentativi di manomissione della sicurezza del sistema;
- perdita del segnale di sincronismo con la fonte esterna di tempo;
- disponibilità del supporto di archiviazione non riscrivibile.

4.12 Modalità operative per l'utilizzo del sistema di verifica delle firme (art. 38/3/s)

In riferimento all'art. 10 del DPCM, Aruba PEC ha qualificato delle applicazioni che fornisce alla propria clientela e che permettono la verifica delle firme digitali apposte su documenti informatici sotto forma di "buste crittografiche" in standard PKCS#7. 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 ed affidabilità del certificato del firmatario;
- l'accesso alla CRL, ovvero al OCSP, del certificatore emittente per verificare che il certificato del firmatario non sia stato sospeso o revocato.

Sintesi operativa dell'utente :

1. avviare l'applicazione di firma e verifica;
2. selezionare la funzione di apertura busta (PKCS#7) dal menu principale;
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 e il contenuto della busta (PKCS#7) che potrà essere letto con programmi adeguati al formato del file firmato (esempio: i file in formato PDF saranno letti con Acrobat Reader).

I prodotti di verifica delle firme forniti da Aruba PEC sono conformi a quanto indicato all'art. 40, comma 2 del DPCM ed ai requisiti di cui all'art. 14 della DELIB. 4/05.

4.13 Modalità operative per la generazione della firma digitale (art.38/3/t)

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

apporre una firma digitale producendo come risultato una busta crittografica, nel formato standard PKCS#7;
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 manuale operativo. La sopra citata chiave privata è custodita all'interno dei dispositivi sicuri di firma 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, nel rispetto dell'Art. 36 del DPCM.

Sintesi operativa dell'utente :

6. avviare l'applicazione di firma;
7. selezionare la funzione di firma dal menu principale o dal menù contestuale;
8. selezionare il file da firmare;
9. digitare il PIN per l'accesso al dispositivo sicuro di firma;

Prima di apporre la firma, un'apposita funzione consente di visualizzare il contenuto dell'oggetto da firmare e richiede contestualmente conferma della volontà di apporre la firma.

L'utente deve tenere ben presente il fatto che, affinché il documento firmato abbia "l'efficacia prevista dall'articolo 2702 del codice civile" (Art. 21, comma 2 del CAD), il documento da firmare "non deve contenere macroistruzioni e codice eseguibile tali da attivare funzionalità che possano alterare gli atti, i dati o i fatti rappresentati" (Art. 3, comma 3 del DPCM). È unicamente responsabilità dell'utente firmatario accertarsi che tale condizione sia soddisfatta. Come esempio di attenzione citiamo i file con estensione HTM o HTML. Questi file sono documenti scritti in HTML che è il linguaggio di marcatura per creare pagine web. Questi file, visualizzabili tramite qualsiasi Web Browser, possono contenere sia del codice interpretato (JavaScript, VBScript) che codice eseguibile (Applet Java, ActiveX ecc...) i quali ne forniscono una forte connotazione dinamica. E' pertanto decisamente sconsigliato fare affidamento al contenuto mostrato tramite il Browser senza analizzarne attentamente l'effettivo contenuto.

Si ricorda inoltre che l'apposizione ad un documento informatico di una firma digitale basata su un certificato revocato, sospeso o scaduto non è valida (Art. 21, comma 3 del CAD).

4.14 Disponibilità del servizio.

Gli orari di disponibilità del servizio sono :

Registrazione, emissione di certificati, revoca/sospensione tramite Operatore :

Operatori di Registrazione: dalle 09:00 alle 18:00
tutti i giorni lavorativi

Accesso all'archivio dei certificati (incluso stato certificati):

server http, LDAP, OCSP : dalle 00:00 alle 24:00
tutti i giorni della settimana festivi inclusi

Revoca e sospensione tramite web :

server http : dalle 00:00 alle 24:00
tutti i giorni della settimana festivi inclusi

Cap. 5 Termini e condizioni generali

Il presente capitolo presenta i termini e le condizioni generali del presente Manuale Operativo che non sono stati trattati nelle altre sezioni.

5.1.1 Obblighi degli Utenti

L'utente che utilizza un certificato del quale non è il Titolare, ha i seguenti obblighi:

- conoscere l'ambito di utilizzo del certificato, le limitazioni di responsabilità e i limiti di indennizzo del Certificatore, riportati nel Manuale Operativo del Certificatore stesso;
- verificare la validità del certificato prima di usare la chiave pubblica in esso contenuta;
- verificare con particolare attenzione il periodo di validità e che il certificato non risulti sospeso o revocato controllando la CRL ovvero utilizzando OCSP;
- adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

5.1.2 Nullità o inapplicabilità di clausole

Se una qualsivoglia disposizioni del presente Manuale Operativo, o relativa applicazione, risulti per qualsiasi motivo o in qualunque misura nulla o inapplicabile, il resto del presente Manuale Operativo (così come l'applicazione della disposizione invalida o inapplicabile ad altre persone o in altre circostanze) rimarrà valido e la disposizione nulla o inapplicabile sarà interpretata nel modo più vicino possibile agli intenti delle parti.

5.1.3 Interpretazione

Salvo disposizioni diverse, questo Manuale Operativo dovrà essere interpretato in conformità alla correttezza, buona fede ed a quanto ragionevole anche in virtù degli usi commerciali internazionali.

5.1.4 Nessuna rinuncia

La mancata applicazione da parte di qualsivoglia persona di una delle disposizioni di cui al presente Manuale Operativo non sarà ritenuta rinuncia a future applicazioni di suddetta disposizione o di qualsiasi altra disposizione.

5.1.5 Comunicazioni

Qualora una persona desideri o sia tenuta ad effettuare delle comunicazioni, domande o richieste in relazione al presente Manuale Operativo, tali comunicazioni dovranno avvenire attraverso messaggi a firma digitale conformi al Manuale Operativo, o per iscritto. Le comunicazioni elettroniche saranno effettive allorché al mittente venga recapitata una ricevuta di ritorno valida, con firma digitale. Tale ricevuta dovrà essere recapitata entro cinque (5) giorni, altrimenti si dovrà provvedere all'invio di una notifica scritta. Le comunicazioni scritte dovranno essere consegnate da un servizio di posta che confermi la consegna per iscritto oppure tramite assicurata convenzionale, raccomandata a/r, indirizzate al seguente indirizzo:
Aruba PEC S.p.A.: 3/A Piazzale Bosco , 05100 Terni Italia

5.1.6 Intestazioni e Appendici del presente Manuale Operativo

Le intestazioni, sottotitoli e altri titoli del presente Manuale Operativo sono utilizzati solo per comodità e riferimento, e non saranno utilizzati nell'interpretazione o applicazione di qualsiasi disposizione ivi contenuta. Le appendici, comprese le definizioni del presente Manuale Operativo, sono parte integrante e vincolante del presente Manuale Operativo a tutti gli effetti.

5.1.7 Modifiche del Manuale Operativo

Modifiche Generali

Aruba PEC S.p.A. si riserva il diritto di aggiornare periodicamente il presente Manuale Operativo (in modo estensibile al futuro e non retroattivo). Aruba PEC S.p.A. ha facoltà di inserire le modifiche nel repository di Aruba PEC S.p.A., sotto forma di versione aggiornata del Manuale Operativo o nella sezione del repository di Aruba PEC S.p.A. intitolata "Aggiornamenti delle procedure e comunicazioni". Tutte le modifiche al Manuale Operativo saranno eseguite in conformità DPCM e successive variazioni.

Aggiornamenti delle procedure e comunicazioni

Le rettifiche apportate al presente Manuale Operativo inserite nel repository di Aruba PEC S.p.A. nella sezione Aggiornamenti di Procedure e Avvisi (vedi indirizzo Internet https://ca.arubapec.it/repository/updates) andranno a modificare il Manuale Operativo. Le modifiche sostituiranno qualsiasi disposizione in conflitto con la versione di riferimento del Manuale Operativo.

5.1.8 Violazioni e altri danni materiali

I richiedenti il certificato (e, previa accettazione, i titolari) rappresentano e garantiscono che la loro presentazione (alla CA) e l'utilizzo di un dominio e del distinguished name (e di tutte le altre informazioni relative alla richiesta del certificato) non interferisca né danneggi i diritti di una qualsiasi terza parte di qualunque giurisdizione in merito a marchi, marchi di identificazione di servizio, nomi commerciali, nomi societari, o ogni altro diritto di proprietà intellettuale, e che non tenteranno di utilizzare il dominio e il distinguished name 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 richie denti si obbligano (e, previa accettazione, i sottoscrittori) a manlevare e indennizzare la CA contro qualunque perdita o
danno derivanti da una tale interferenza o infrazione. Generalmente, non è possibile limitare la distribuzione dei contenuti su Internet o su talune altre reti sulla base dell'ubicazione dell'utente/osservatore. Di conseguenza, richiedenti e sottoscrittori dovranno attenersi alle leggi di ciascuna giurisdizione nella quale i contenuti possono essere consultati o usati.

5.1.9 Norme Applicabili

Le operazioni di certificazione contenute nel presente Manuale Operativo sono assoggettate alle leggi dell'ordinamento italiano. L'applicabilità, l'esecuzione, l'interpretazione e la validità del presente Manuale Operativo sono regolate dalla leggi italiane, indipendentemente dal contratto o altre scelte di disposizioni di legge e senza la necessità di stabilire un punto di contatto commerciale in Italia. Questa scelta è volta a garantire a tutti gli utenti un'uniformità di procedure e interpretazioni, indipendentemente dal luogo in cui essi risiedono o utilizzano i loro certificati.

5.1.10 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 .