Manuale Operativo

Servizio di Certificazione Digitale

Revisione 2.5

Approvato da: **Andrea Sassetti**
Direttore dei Servizi di Certificazione
il **01/04/2014**

Firmato digitalmente da
Andrea Sassetti

- Questa pagina è lasciata intenzionalmente bianca -

Indice

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, Decreto legislativo 7 marzo 2005, n. 82 pubblicato in G.U. del 16 maggio 2005, n. 112 - S.O. n. 93 "Codice dell'amministrazione digitale" e successive modifiche ed integrazioni e del Decreto del Presidente del Consiglio dei Ministri (DPCM) 30 Marzo 2009, " Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.", pubblicato sulla Gazzetta Ufficiale 6 Giugno 2009, n. 129.
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 22 febbraio 2013, art. 40 e successive modifiche ed integrazioni) 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.
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:

1. Che il certificato sia valido e non revocato o sospeso attraverso l'utilizzo delle apposite liste di certificati revocati o sospesi, disponibili per via telematica agli utenti (vedi definizioni di CRL e CSL).
2. Che la firma digitale sia stata creata durante il periodo operativo del certificato stesso dalla chiave privata corrispondente alla chiave pubblica riportata nel certificato.
3. 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.pec.it oppure contattare il sevizio clienti all'indirizzo: assistenza@ca.arubapec.it.

1.2 Riferimenti agli standard

PKCS. 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. SHA-1 è una revisione del algoritmo SHA pubblicata nel 1994.
Lo standard di riferimento è costituito dalla norma ISO/IEC 10118-3:2004.
SHA-256. Secure Hash Algorithm (SHA), algoritmo specificato nel Secure Hash Standard (SHS, FIPS 180), sviluppato dal NIST.
Lo standard di riferimento è costituito dalla norma ISO/IEC 10118-3:2004.

1.3 Riferimenti normativi

[1] Decreto del Presidente della Repubblica (DPR) 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.

[2] Decreto del Presidente del Consiglio dei Ministri (DPCM) 22 febbraio 2013 , "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71.", pubblicato sulla Gazzetta Ufficiale del 21 maggio 2013 n. 117.

[3] 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).

[4] 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.

[5] Decreto 2 luglio 2004, “Competenza in materia di certificatori di firma elettronica” pubblicato nella Gazzetta Ufficiale n.199, 25 agosto 2004.

[6] Decreto Legislativo (CAD) 7 marzo 2005, n. 82: "Codice dell’amministrazione digitale", pubblicato nella Gazzetta Ufficiale. n. 112 del 16 maggio 2005.

[7] Deliberazione n. 45 del 21 maggio 2009 “Regole per il riconoscimento e la verifica del documento informatico” (Deliberazione n. 45/2009).

[8] Legge 11 agosto 1991, “Istituzione del Sistema Nazionale di Taratura”, Pubblicato nella Gazzetta Ufficiale 6 maggio 2002, n. 104.

[9] 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.

[10] Decreto del Presidente del Consiglio dei Ministri (DPCM) 12/10/2007, “Differimento del termine che autorizza l’autodichiarazione circa la rispondenza ai requisiti di sicurezza di cui all’articolo 13, comma 4, del decreto del Presidente del Consiglio dei Ministri”, pubblicato sulla Gazzetta Ufficiale 30 Ottobre 2003, n. 13.

[11] 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).

[12] 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.

[13] “Linee guida per l’emissione e l’utilizzo della Carta Nazionale dei Servizi”, Ufficio Standard e tecnologie d’identificazione, CNIPA, Versione 3.0, 15 maggio 2006

1.4 Definizioni ed acronimi

CA	Certification authority – Autorità di certificazione
CAD	Codice dell'Amministrazione Digitale
CDRL	Centro Di Registrazione Locale
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione
CRL	Certificate revocation list – lista dei certificati revocati
CSL	Certificate suspension list – lista dei certificati sospesi
CSR	Certificate signing request
DigitPA	Nuova denominazione del Centro Nazionale per l'Informatica nella Pubblica Amministrazione
DPCM	Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 [2]
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GMT	Greenwich Mean Time
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol con SSL
IR	Incaricato alla Registrazione
ISO	International Standard Organization
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
OCSP	Protocollo per il controllo on-line dello stato dei certificati digitali
OdR	Operatore di Registrazione
OID	Object Identifier
OTP	One Time Password
Parametri Grafometrici	Un insieme di parametri (velocità, pressione, ritmo, accelerazione, movimenti aerei) che vengono "catturati" nel momento in cui si appone una firma con una particolare penna e che rendono l'autenticazione del Titolare assolutamente certa.
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
Tablet	Dispositivo su cui viene apposta la firma utilizzata per autenticare il Titolare
TLS	Transport Layer Security
TSA	Time Stamping Authority (sistema di marcatura temportale)
SP	Security Procedures – procedure di sicurezza Aruba PEC S.p.a
WebCam	Telecamera digitale destinata a trasmettere immagini in streaming via Internet ed in grado di catturare immagini fotografiche. Generalmente utilizzata, collegata ad un pc, per videoconferenze o chat video.
WWW	World Wide Web
X.509	Specifica ITU-T in materia di certificazione e relativo framework di autenticazione

2 Dati identificativi - Pubblicazione Manuale Operativo

2.1 Dati identificativi del certificatore (art. 40/3/a)

Denominazione Sociale : **Aruba Posta Elettronica Certificata S.p.A.**
Indirizzo della sede legale : **Via Sergio Ramelli, 8 – 52100 - Arezzo**
Legale Rappresentante : **Simone Braccagni**
N° REA : **145843**
N° iscrizione al Registro delle imprese : **01879020517**
N° Partita IVA : **01879020517**
N° Telefono (centralino) : **+39 0575 0500**
N° FAX : **+39 0575 862022**
e-mail PEC : **direzione.ca@arubapec.it**
ISO OID (private enterprise number) : **1.3.6.1.4.1.29741**
Web server principale : http://www.pec.it
Web server firma digitale : https://ca.arubapec.it

2.2 Versione del manuale operativo (art. 40/3/b)

Questo documento è la versione 2.5 del Manuale Operativo del Servizio di Certificazione Digitale individuato da codice interno 100113AS01, erogato da Aruba PEC S.p.A.

2.3 Pubblicazione del manuale

Ai sensi dell'art. 40, comma 2, del Decreto del Presidente del Consiglio dei Ministri (DPCM) 22 febbraio 2013 questo documento è pubblicato sulle pagine principali del web server di firma digitale indicato all'interno del paragrafo 2.1.

2.4 Responsabile del manuale operativo (art. 40/3/c)

Il responsabile del presente manuale operativo è :

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

Tel. +39 0575 1939715
Fax. +39 0575 862022
E-mail: CPS-requests@ca.arubapec.it

3 Disposizioni generali

3.1 Obblighi del titolare, del certificatore e di quanti accedono per la verifica delle firme (art. 40/3/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'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;
    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. Garantire che il Titolare mantenga il controllo esclusivo di almeno uno dei dati per la creazione della firma;
    l. Non copiare, le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione;
    m. 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;

n. utilizzare 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'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. sono indicati nel paragrafo 4.8.
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 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 sono 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.

3.2.2 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 Via Sergio Ramelli, 8 – 52100 Arezzo. 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.

3.2.3 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:
  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.

3.2.4 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;
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. 40/3/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. 40/3/f)

Per le tariffe del servizio si rimanda al form di richiesta informazioni presente sul sito web http://www.pec.it.

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. 38 del DPCM, prevede, le seguenti figure responsabili:

a) responsabile della sicurezza;

b) responsabile del servizio di certificazione e validazione temporale;

c) responsabile della conduzione tecnica dei sistemi;

d) responsabile dei servizi tecnici e logistici;

e) responsabile delle verifiche e delle ispezioni (auditing).

Non è possibile attribuire ad un medesimo soggetto più funzioni tra quelle citate.

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

4.2 Modalità di Identificazione e Registrazione (art. 40/3/g)

Per consentire una diffusione sul territorio delle pratiche operative, le funzioni di registrazione, identificazione e autenticazione possono essere svolte attraverso varie modalità:

Modalità 1
L'identità del soggetto Titolare viene accertata dal Certificatore.

Modalità 2
L'identità del soggetto Titolare viene accertata da un soggetto incaricato dall'Ente Certificatore denominato Centro di Registrazione Locale (CDRL).

Modalità 3
L'identità del soggetto Titolare viene accertata da un soggetto incaricato dall'Ente Certificatore denominato Incaricato alla Registrazione (IR).

Modalità 4
L'identità del soggetto Titolare viene accertata dal Pubblico Ufficiale.

Modalità 5
L'identità del soggetto Titolare viene accertata:

- dal Certificatore
- da un soggetto, incaricato dall'Ente Certificatore, denominato Centro di Registrazione Locale (CDRL)
- da un soggetto incaricato dall'Ente Certificatore denominato Incaricato alla Registrazione (IR)

per mezzo di un sistema di videoconferenza.

4.2.1 Modalità di identificazione e registrazione degli utenti secondo la Modalità 1

In tale modalità l'identificazione e la registrazione sono effettuate direttamente dall'Ente Certificatore ed è prevista la presenza fisica del soggetto Titolare dinnanzi ad un dipendente della CA addetto alla registrazione.

L'incaricato della CA effettua l'identificazione del Titolare attraverso il riscontro con uno dei seguenti documenti valido e non scaduto, secondo quanto previsto dall'art 35, Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445:

- Carta d'Identità
- Passaporto
- Patente di guida
- Patente nautica
- Libretto di pensione
- Patentino di abilitazione alla conduzione di impianti termici
- Porto d'armi

Sono anche ammesse altre tessere di riconoscimento, purché munite di fotografia e di timbro, rilasciate da un'Amministrazione dello Stato.

Al momento dell'identificazione l'incaricato della CA effettua anche la registrazione richiedendo al Titolare la seguente documentazione:

a. Copia cartacea della richiesta - sulla base del Modulo di Registrazione e Richiesta del Certificato[1] - completata in ogni sua parte ad eccezione delle firme. Nel caso di sottoscrizione

[1] Tali 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.

del Modulo di Registrazione e Richiesta del Certificato tramite procedura di Firma Elettronica, il Modulo di Registrazione sarà generato in formato elettronico secondo la procedura descritta in § 4.2.6

b. 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.
c. Eventuale ulteriore documentazione necessaria al rilascio del certificato.

Il Modulo di Registrazione e Richiesta del Certificato precompilato viene sottoscritto con firma autografa dal soggetto Titolare dinnanzi all'incaricato della CA.
Nel caso di sottoscrizione del Modulo di Registrazione e Richiesta del Certificato tramite procedura di Firma Elettronica, verrà seguita la procedura descritta in § 4.2.6.
Si rende noto in tal senso che il soggetto Titolare, firmando il Modulo di Registrazione e Richiesta del Certificato:

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. 8, comma 5 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.
f. Può fornire la propria autorizzazione alla pubblicazione del certificato.

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.

Durante il processo di identificazione e registrazione da parte dell'Ente Certificatore, l'incaricato della CA, utilizzando canali di comunicazione sicuri, invia tutte le informazioni indicate in § 4.2.7 ai sistemi della CA.
Tali informazioni verranno quindi utilizzate dall'Ente Certificatore per il rilascio del Certificato Qualificato e archiviate nel database di registrazione automatico.

In caso di chiavi di sottoscrizione generate su dispositivo HSM (**OID 1.3.6.1.4.1.29741.1.1.11.1**) l'incaricato della CA procede con la consegna nelle mani del titolare di una credenziale di autenticazione forte (ad esempio OTP). Questa credenziale verrà utilizzata dall'utente per la personalizzazione del dispositivo di firma e per il controllo esclusivo delle proprie chiavi di sottoscrizione.

Le modalità di rilascio del certificato, personalizzazione elettrica del dispositivo e consegna del kit seguono quanto riportato in § 4.3, § 4.4 e § 4.5.

4.2.2 Modalità di identificazione e registrazione degli utenti secondo la Modalità 2

In tale modalità l'identificazione e la registrazione sono effettuate da una terza parte denominata Centro di Registrazione Locale (CDRL) ed è prevista la presenza fisica del soggetto Titolare dinnanzi ad un incaricato del CDRL definito Operatore di Registrazione (OdR).

Tali terze parti (CDRL) 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 (OdR), che dovrà operare nel contesto delle pratiche operative di registrazione.
L'autorizzazione e successivamente la qualificazione degli OdR come abili alle operazioni di identificazione, registrazione e rilascio, avviene mediante corso di formazione 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 identificazione, registrazione e rilascio dei certificati. I privilegi di accesso agli strumenti telematici sicuri e le operazioni degli OdR sono sotto il costante controllo del certificatore.

L'OdR effettua l'identificazione del Titolare attraverso le stesse modalità riportate in § 4.2.1.

Al momento dell'identificazione l'OdR effettua anche la registrazione richiedendo al Titolare la seguente documentazione:

a. Copia cartacea della richiesta - sulla base del Modulo di Registrazione e Richiesta del Certificato - completata in ogni sua parte ad eccezione delle firme. Nel caso di sottoscrizione del Modulo di Registrazione e Richiesta del Certificato tramite procedura di Firma Elettronica, il Modulo di Registrazione sarà generato in formato elettronico secondo la procedura descritta in § 4.2.6
b. 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.
c. Eventuale ulteriore documentazione necessaria al rilascio del certificato.

Il Modulo di Registrazione e Richiesta del Certificato precompilato viene sottoscritto con firma autografa dal soggetto Titolare dinnanzi all'OdR.
Nel caso di sottoscrizione del Modulo di Registrazione e Richiesta del Certificato tramite procedura di Firma Elettronica, verrà seguita la procedura descritta in § 4.2.6.

Si rende noto in tal senso che il soggetto Titolare, firmando il Modulo di Registrazione e Richiesta del Certificato:

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. 8, comma 5 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.
f. Può fornire la propria autorizzazione alla pubblicazione del certificato.

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.

Un volta terminato il processo di identificazione e registrazione da parte del CDRL, l'OdR, utilizzando canali di comunicazione sicuri, invia tutte le informazioni indicate in § 4.2.7 ai sistemi della CA e procede con la personalizzazione elettrica del dispositivo di firma che verrà quindi consegnato in modo sicuro nelle mani del Titolare.
Le informazioni scambiate durante le operazioni appena descritte sono utilizzate dall'Ente Certificatore per il rilascio del Certificato Qualificato e archiviate nel database di registrazione automatico.

In caso di chiavi di sottoscrizione generate su dispositivo HSM (**OID 1.3.6.1.4.1.29741.1.1.11.1**) l'OdR ha la facoltà di:

1. procedere con la registrazione dei dati grafometrici che serviranno come strumento di autenticazione/autorizzazione per permettere l'utilizzo delle chiavi di sottoscrizione;

e/o

2. procedere con la consegna nelle mani del titolare di una credenziale di autenticazione forte (ad esempio OTP) Questa credenziale verrà utilizzata dall'utente per la personalizzazione del dispositivo di firma e per il controllo esclusivo delle proprie chiavi di sottoscrizione.

Nel caso in cui venga effettuata la registrazione dei parametri grafometrici del titolare, viene richiesta l'apposizione da quattro a sei firme su di un tablet attraverso l'utilizzo di una particolare penna messa a disposizione dal CDRL. Grazie infatti ad uno specifico software dedicato a tali riconoscimenti, il sistema è in grado di trasporre in *specimen* una serie di informazioni relative al modo di firmare del Titolare. Queste informazioni saranno utilizzate successivamente per permettere al Titolare l'utilizzo delle chiavi di

sottoscrizione. Le modalità di rilascio del certificato, personalizzazione elettrica del dispositivo e consegna del kit seguono quanto riportato in § 4.3, § 4.4 e § 4.5.

Nel caso in cui il CDRL proceda con la sola registrazione dei dati grafometrici del titolare, la personalizzazione elettrica del dispositivo ed il rilascio del certificato qualificato, avvengono in un'unica sessione e contestualmente alla procedura di identificazione e registrazione.

4.2.3 Modalità di identificazione e registrazione degli utenti secondo la Modalità 3

In tale modalità l'identificazione e la registrazione sono effettuate da un soggetto terzo denominato Incaricato alla Registrazione (IR) ed è prevista la presenza fisica del soggetto Titolare dinnanzi all'incaricato.

Tali soggetti (IR) possono operare successivamente alla stipula di un contratto con Aruba PEC in cui la società terza indica il proprio personale, che sarà individuato come Incaricato di Registrazione (IR) e che dovrà operare nel contesto delle pratiche operative di registrazione.

L'IR effettua l'identificazione del Titolare attraverso le stesse modalità riportate in § 4.2.1.

Al momento dell'identificazione l'IR effettua anche la registrazione richiedendo al Titolare la seguente documentazione:

a. Copia cartacea della richiesta - sulla base del Modulo di Registrazione e Richiesta del Certificato - completata in ogni sua parte ad eccezione delle firme. Nel caso di sottoscrizione del Modulo di Registrazione e Richiesta del Certificato tramite procedura di Firma Elettronica, il Modulo di Registrazione sarà generato in formato elettronico secondo la procedura descritta in § 4.2.6.
b. 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.
c. Eventuale ulteriore documentazione necessaria al rilascio del certificato.

Il Modulo di Registrazione e Richiesta del Certificato precompilato viene sottoscritto con firma autografa dal soggetto Titolare dinnanzi all'IR.
Nel caso di sottoscrizione del Modulo di Registrazione e Richiesta del Certificato tramite procedura di Firma Elettronica, verrà seguita la procedura descritta in § 4.2.6.

Si rende noto in tal senso che il soggetto Titolare, firmando il Modulo di Registrazione e Richiesta del Certificato:

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. 8, comma 5 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.
f. Può fornire la propria autorizzazione alla pubblicazione del certificato.

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.

In caso di chiavi di sottoscrizione generate su dispositivo HSM (**OID 1.3.6.1.4.1.29741.1.1.11.1**) l'IR ha la facoltà di:

1. procedere con la registrazione dei dati grafometrici che serviranno come strumento di autenticazione/autorizzazione per permettere l'utilizzo delle chiavi di sottoscrizione;

e/o

2. procedere con la consegna nelle mani del titolare di una credenziale di autenticazione forte (ad esempio OTP) Questa credenziale verrà utilizzata dall'utente per la personalizzazione del dispositivo di firma e per il controllo esclusivo delle proprie chiavi di sottoscrizione.

Nel caso in cui venga effettuata la registrazione dei parametri grafometrici del titolare, viene richiesta l'apposizione da quattro a sei firme su di un tablet attraverso l'utilizzo di una particolare penna messa a disposizione dal CDRL. Grazie infatti ad uno specifico software dedicato a tali riconoscimenti, il sistema è in grado di trasporre in *specimen* una serie di informazioni relative al modo di firmare del Titolare. Queste informazioni saranno utilizzate successivamente per permettere al Titolare l'utilizzo delle chiavi di sottoscrizione.

Le modalità di rilascio del certificato, personalizzazione elettrica del dispositivo e consegna del kit seguono quanto riportato in § 4.3, § 4.4 e § 4.5.

Nel caso in cui l'IR proceda con la sola registrazione dei dati grafometrici del titolare, la personalizzazione elettrica del dispositivo ed il rilascio del certificato qualificato, avvengono in un'unica sessione e contestualmente alla procedura di identificazione e registrazione.
La procedura di personalizzazione elettrica del dispositivo e di rilascio del certificato qualificato sono attivate dal Titolare.

4.2.4 Modalità di identificazione e registrazione degli utenti secondo la Modalità 4

In questa modalità l'identificazione è effettuata 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 successive modifiche ed integrazioni.

L'Utente che intende effettuare l'identificazione attraverso tale modalità dovrà recarsi presso il Pubblico Ufficiale munito di un documento di identità valido e non scaduto oltre che dell'ulteriore documentazione necessaria al rilascio del certificato indicata dal Certificatore.

La registrazione del Titolare è invece effettuata automaticamente attraverso l'inserimento dei dati identificativi all'interno di apposite pagine di registrazione che il Certificatore rende disponibili presso il proprio Server web.

Le comunicazioni tra il Titolare e le pagine di registrazione del Certificatore avvengono tramite canale sicuro.

Le modalità di rilascio del certificato, personalizzazione elettrica del dispositivo e consegna del kit seguono quanto riportato in § 4.3, § 4.4 e § 4.5.

4.2.5 Modalità di identificazione e registrazione degli utenti secondo la Modalità 5

In tale modalità l'identificazione e la registrazione, fatte dai soggetti indicati al par. 4.2, viene effettuata mediante l'ausilio di un sistema di videoconferenza e prevede che il Titolare sia dotato di una webcam correttamente collegata ad un PC con sistema audio funzionante.
L'Operatore seguirà delle particolari procedure – che per ragioni di sicurezza sono riservate – volte a garantire l'autenticità della richiesta del corso della sessione in videoconferenza.
L'Operatore che effettua l'identificazione si accerta dell'identità del Titolare tramite la verifica di un documento di riconoscimento in corso di validità (tra quelli previsti nel § 4.2.1), purché munito di fotografia

recente e riconoscibile del Titolare, firma autografa del Titolare e di timbro, rilasciato da un'Amministrazione dello Stato.
L'Operatore che effettua l'identificazione si può riservare di escludere l'ammissibilità del documento presentato dal Titolare 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 dell'art 32 comma 3, lettera a) del CAD.

Al momento dell'identificazione il Titolare dovrà 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

Durante la sessione di videoconferenza e successivamente alla sua identificazione viene fornito al Titolare un codice di riservato di emergenza da utilizzare per l'autenticazione delle eventuali comunicazioni tra Certificatore e Titolare (cfr. art. 21 DPCM).
La sessione di videoconferenza è interamente registrata (audio+video).
Per garantire la tutela e la gestione dei propri dati personali in piena aderenza al DLGS 196, ad ogni richiedente verrà preventivamente fornita l'informativa sulla privacy chiedendo il consenso alla videoregistrazione ed al trattamento dei dati.
Solo dopo l'assenso del richiedente potrà essere avviata la registrazione della video conferenza che inizierà con la ripetizione della procedura di richiesta del consenso.

I dati di registrazione, costituiti dal file audio-video e metadati strutturati in formato elettronico, vengono conservati in maniera sicura per una durata ventennale, secondo quanto indicato nell'art. 32, comma 3, lettera j) del CAD.

4.2.6 Sottoscrizione del Modulo di Registrazione e Richiesta del Certificato con procedura di Firma Elettronica

Il modulo di registrazione può essere predisposto e compilato in forma cartacea oppure elettronica. Nel primo caso, come riportato in § 4.2.1, § 4.2.2, § 4.2.3, § 4.2.4, dev'essere sottoscritto dal richiedente con firma autografa, mentre nel secondo caso deve essere sottoscritto dal richiedente con firma elettronica. A tal fine, il certificatore accetta i seguenti tipi di firma elettronica:

1. firma digitale (con certificato non necessariamente emesso da ArubaPEC)
2. firma elettronica apposta mediante il certificato di autenticazione presente su CNS/CRS (Carta Nazionale o Regionale dei Servizi)
3. firma elettronica basata su un dato riservato conosciuto solo dal richiedente, oltre che dal certificatore. Ad esempio, tale dato riservato potrebbe essere una password dinamica (OTP) che il certificatore invia al telefono cellulare dell' Utente (mediante SMS o con altre modalità), previa raccolta e memorizzazione del numero di cellulare dell'Utente richiedente in fase di identificazione e registrazione.

Il terzo tipo di firma è accettato solo nel caso di identificazione de visu dell'Utente da parte dell'Operatore e di firma elettronica del Modulo di Registrazione in presenza dell'Operatore stesso, il quale appone al modulo la propria controfirma digitale. In questo caso, il modulo include anche la dichiarazione dell'Operatore che la firma elettronica dell'Utente è avvenuta in sua presenza.

Tale procedura sarà applicabile nelle Modalità 1, 2 e 3 previste dal Paragrafo 4.2

I Centri di Registrazione Locale (CDRL) sono soggette ad ispezioni da parte di ArubaPEC, nonché a "controlli a campione", al fine di verificare la corretta operatività nel rispetto dell'accordo di delega stipulato con ArubaPEC.

4.2.7 Informazioni che il Titolare deve fornire

L'utente che intende richiedere il rilascio del Certificato Qualificato svolgendo l'identificazione e la registrazione secondo le modalità descritte nei precedenti paragrafi, deve obbligatoriamente fornire le seguenti informazioni:

- Nome e Cognome (*)
- Data di nascita
- Comune, provincia e stato di nascita
- Codice fiscale o analogo codice identificativo[2] (*)
- Indirizzo di residenza, eventualmente all'estero
- Indirizzo di posta elettronica (*)
- Estremi del documento di riconoscimento presentato per l'identificazione, quali tipo, numero, ente emittente e data di rilascio dello stesso
- Numero di cellulare.
  Questo dato è obbligatorio solo in caso di Firma Digitale basata su HSM (**OID 1.3.6.1.4.1.29741.1.1.11.1**) o in caso di identità accertata da Pubblico Ufficiale
- 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.12 della Deliberazione CNIPA 21 maggio 2009. (*)

(*) Tutti i dati contrassegnati con l'asterisco sono inseriti nel certificato, tranne nel caso di utilizzo dello pseudonimo (in tal caso l'inserimento dei dati segue quanto previsto dalla lettera e), comma 3 dell'art.12 della DELIB 45/09 [7]).

4.2.7.1 Titolo e/o Abilitazioni professionali

Con riferimento alla lettera a), comma 3 dell'art. 28 del CAD [6] e successive correzioni ed integrazioni, nel caso in cui sia richiesta, dal titolare o dal terzo interessato, l'indicazione nel certificato di Abilitazioni Professionali (es. l'appartenenza ad un ordine professionale, l'iscrizione ad un albo o la qualifica di pubblico ufficiale), il richiedente, salvo diversa pattuizione tra il Certificatore e l'Ordine di appartenenza, deve produrre un certificato rilasciato dall'Ordine unitamente al consenso scritto da parte di quest'ultimo manifestato sull'apposito modulo fornito dal Certificatore o, in alternativa, un'autocertificazione ai sensi dell'art. 46 del D.P.R. n. 445/2000.
La documentazione da presentare non dovrà essere anteriore di oltre 10 (dieci) giorni alla data della richiesta di registrazione.

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

[2] Per i cittadini stranieri che non fossero in possesso del codice fiscale né di alcun altro codice identificativo nazionale, deve essere presentato il passaporto, il cui identificativo sarà inserito nel certificato nello spazio predisposto per il codice fiscale nel formato **CC**:PASSPORT**XXXXX** dove **CC** = Country Code ISO 3166 e **XXXXX** = Numero del Passaporto.

4.2.7.2 Limiti d'uso e limiti di valore

Con riferimento alla let. c comma 3 dell'art. 28 del CAD [6] è facoltà del Titolare richiedere al certificatore l'inserimento nel certificato di limiti di valore che indichino un limite di valore degli atti unilaterali e dei contratti per i quali il certificato stesso può essere usato. **I valori devono essere espressi come numeri interi positivi, senza indicazione di cifre decimali.**
Per quanto riguarda invece i limiti d'uso (let. b comma 3 dell'art. 28 del CAD [6]), Aruba Pec, ai sensi dell'articolo 12, comma 6, lettera c) della Deliberazione CNIPA 21 maggio 2009, n. 45 [7], 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. La presente dichiarazione costituisce evidenza dell'adozione di tale procedura per i documenti firmati.**
- **The certificate may be used only for automatic procedure signature purposes.**
- **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).**

Ferma restando la responsabilità del Certificatore di cui al CAD (art.30 comma 1 lettera a), è responsabilità dell'**Utente** verificare il rispetto dei limiti d'uso inseriti nel certificato.

La richiesta di inserire altre specifiche limitazioni d'uso sarà valutata dal Certificatore per gli aspetti legali, tecnici e di interoperabilità e valorizzata di conseguenza.
Si rende noto in ogni caso che eventuali altre limitazioni d'uso specificate dagli utenti non potranno eccedere i 200 caratteri (spazi inclusi).

4.2.7.3 Ruolo ed Organizzazione

Con riferimento alla let. a comma 3 dell'art. 28 del CAD [6] il Titolare può ottenere, direttamente, o con il consenso dell'eventuale Terzo Interessato, l'inserimento nel certificato di sottoscrizione di informazioni relative a Funzioni, Titoli e/o Abilitazioni Professionali e Poteri di Rappresentanza.
In questo caso, il Titolare, oltre alla documentazione e alle informazioni identificative necessarie (cfr. § 4.2.7), dovrà produrre anche quella idonea a dimostrare l'effettiva sussistenza dello specifico Ruolo anche attestandolo, ove espressamente consentito dal presente Manuale Operativo, mediante Autocertificazione, ai sensi dell'art. 46 del D.P.R. 445/2000.
Come indicato nella Deliberazione CNIPA 21 maggio 2009, n. 45 [7], nel caso in cui la richiesta di inserimento del ruolo nel certificato sia stata effettuata mediante la sola autocertificazione da parte del Titolare, il certificato non riporterà informazioni inerenti l'organizzazione a cui potrebbe eventualmente essere legato il ruolo stesso.
Il Certificatore, in tali ipotesi, non assume alcuna responsabilità, salvo i casi di dolo o colpa grave, in merito all'inserimento nel certificato delle informazioni autocertificate dal Titolare.
La ragione sociale o la denominazione e il codice identificativo dell'Organizzazione saranno invece riportate nel certificato se essa ha richiesto o autorizzato il rilascio del certificato al Titolare, anche senza l'esplicita indicazione di un ruolo.
In tale ipotesi il Certificatore effettua un controllo sulla regolarità formale della documentazione presentata dal Titolare.
Per poter ottemperare alle previsioni dell'Art 12 comma 3 della Deliberazione CNIPA 21 maggio 2009, n. 45 [7], la richiesta di certificati con l'indicazione dell'Organizzazione e/o del Ruolo può provenire solo da organizzazioni in possesso di Codice Fiscale.

Tutte le informazioni specificate in § 4.2.7, § 4.2.7.1, § 4.2.7.2, § 4.2.7.3, sono soggette a verifiche e controlli da parte del Certificatore il quale si riserva il diritto, qualora la documentazione presentata sia affetta da irregolarità, di rigettare 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.

4.3 Dispositivo di firma

4.3.1 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 agli articoli 11,12 e 13 del DPCM.
Aruba PEC S.p.A. rende disponibile anche la possibilità di utilizzare chiavi di sottoscrizione generate su dispositivi HSM (**OID 1.3.6.1.4.1.29741.1.1.11.1** o **OID 1.3.6.1.4.1.29741.1.1.11.2**).

4.3.2 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 dai propri Servizi di Certificazione.

4.3.3 Personalizzazione del dispositivo di firma

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

4.3.4 Distribuzione del dispositivo sicuro di firma

La consegna del dispositivo sicuro di firma avviene al termine del processo personalizzazione elettrica dello stesso e prevede diverse modalità:

- Nel caso di grandi lotti di dispositivi di firma personalizzati elettricamente dal Certificatore, attraverso meccanismi automatizzati di produzione massiva, i dispositivi vengono consegnati al Titolare in stato di sospensione e riattivati personalmente dal Titolare stesso attraverso un meccanismo interattivo caratterizzato da altissimi livelli di sicurezza.

- Nel caso di dispositivi di firma personalizzati elettricamente in modalità live dal CDRL o dal Certificatore questi vengono consegnati da un incaricato della CA o da un Operatore di Registrazione (OdR) personalmente al Titolare.

- Nel caso di chiavi di sottoscrizione generate su dispositivi HSM (**OID 1.3.6.1.4.1.29741.1.1.11.1**), al titolare viene associata una credenziale di autenticazione forte che verrà utilizzata per il controllo esclusivo delle proprie chiavi di sottoscrizione.
  Tra i meccanismi di autenticazione forte attualmente supportati rientrano:

  - Username, Password e codice OTP;
  - Tecniche di riconoscimento biometrico (ad. es grafometria) rafforzate dalla presenza fisica del titolare dinnanzi ad un incaricato della CA.

Le indicazioni riportate nel presente paragrafo non sono applicabili nel caso di chiavi di sottoscrizione generate autonomamente dal Titolare all'interno del proprio dispositivo di firma.

4.4 Modalità di generazione delle chiavi (art. 40/3/h)

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

Coppie di chiavi generate nell'attività di certificazione

La generazione della coppia di chiavi di certificazione costituisce il primo passo nel procedimento di creazione di una CA (Certification Authority) 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).
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, esse sono generate, conservate ed utilizzate all'interno di uno stesso dispositivo sicuro (HSM) avente caratteristiche di sicurezza paragonabili e/o conformi a quelle previste dal DPCM.

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

1. Chiavi di certificazione, generate dal Certificatore e destinate alla generazione e verifica delle firme apposte o associate ai certificati qualificati, alle informazioni sullo stato di validità del certificato ovvero alla sottoscrizione dei certificati relativi a chiavi di marcatura temporale;
2. Chiavi di sottoscrizione , 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.

4.4.1 Modalità di generazione delle chiavi del certificatore

La generazione e configurazione delle coppie di chiavi del certificatore avviene nel rispetto dell'art.16 del DPCM e, costituendo una delle funzioni più importanti, è svolta sotto il controllo del responsabile dei servizi tecnici e logistici. 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. 7, comma 1 del DPCM, sono generate sotto il controllo del responsabile del servizio.

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.

4.4.2 Modalità di generazione delle chiavi di sottoscrizione degli utenti

Le chiavi di sottoscrizione degli utenti sono generate dagli utenti stessi o dal Certificatore (anche attraverso i propri CDRL), rif. art. 7, comma 2, del DPCM. Detta generazione avviene all'interno di un dispositivo di firma hardware (smart-card, token o HSM), obbligatoriamente attivato da software approvati da Aruba PEC S.p.A che sono in grado di garantire livelli di sicurezza paragonabili 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 codice personale ovvero da accoppiata username/password e credenziale di autenticazione forte (ad esempio OTP) ovvero da procedure di autorizzazione/autenticazione basate su tecniche di riconoscimento biometrico (ad es. grafometria) rafforzate dalla presenza fisica del titolare dinnanzi ad un incaricato del Certificatore.
La generazione delle chiavi di sottoscrizione può avvenire secondo diverse modalità:

- Massiva (Bulk): Nella quale le chiavi vengono generate all'interno dei singoli dispositivi sicuri di firma che sono inizializzati da un meccanismo di personalizzazione elettrica automatizzato.
- Live: Nella quale le singole copie di chiavi vengono generate all'interno del dispositivo sicuro di firma in presenza del Titolare;

4.4.3 Modalità di generazione delle chiavi di marcatura temporale

Questa avviene nel rispetto dell'art. 49 del DPCM. La generazione delle chiavi viene attivata sotto il controllo del responsabile del servizio di certificazione e validazione temporale. 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 dopo non più di tre mesi di utilizzazione. La sottoscrizione dei certificati relativi a chiavi di marcatura temporale avviene con chiavi di certificazione appositamente generate.

4.5 Modalità di emissione dei certificati (art. 40/3/i)

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

4.5.1 Richiesta del certificato

Aruba PEC prevede che la certificazione della coppia di chiavi di sottoscrizione sia ottenuta dopo aver sottoposto un'appropriata richiesta effettuata secondo una delle modalità descritte in § 4.2 del presente manuale operativo. L'invio della chiave pubblica, e la prova di possesso della chiave privata, avviene secondo la specifica PKCS#10.

4.5.2 Generazione del certificato

La generazione del certificato avviene nel rispetto dell'art. 18 del DPCM, utilizzando un processo articolato in diverse fasi e basato su canali di comunicazione sicuri.
In particolare la procedura, che prevede l'identificazione certa del soggetto che attiva il processo di rilascio, può essere descritta dai seguenti passi:

1. Si accerta l'autenticità della richiesta, provvedendo nel contempo alla identificazione del richiedente;
2. Si richiede la prova del possesso della chiave privata e si verifica il corretto funzionamento della coppia di chiavi;

3. Si assegna al Titolare, attraverso una procedura automatica, un codice identificativo univoco[3] nell'ambito del proprio archivio di utenti, che verrà inserito all'interno dell'attributo *dnQualifier* (OID: 2.5.4.46) del certificato.
4. Si genera il certificato:
    a. Nel caso di chiavi di sottoscrizione generate dal Certificatore in modalità massiva (cfr §4.4.2) il certificato è rilasciato in stato di sospensione ed è necessario attivarlo successivamente attraverso codice OTP temporaneo inviato sul cellulare del Titolare;

    b. Nel caso di chiavi di sottoscrizione generate dal CDRL o dal Certificatore in modalità live (cfr §4.4.2) il certificato è rilasciato in presenza del Titolare e contestualmente alla generazione della coppia di chiavi;

    c. Nel caso di chiavi di sottoscrizione generate dal Titolare posso essere individuati due ulteriori casistiche:

        i. **OID 1.3.6.1.4.1.29741.1.1.11.1**: il certificato viene rilasciato contestualmente alla generazione della coppia di chiavi.
        ii. **OID 1.3.6.1.4.1.29741.1.1.11.2**: il certificato può essere rilasciato anche in un momento diverso rispetto alla generazione della coppia di chiavi.

5. Si provvede a pubblicare e inserire il certificato nel proprio registro dei certificati, con attestazione del momento dell'inserimento mediante un riferimento temporale certo che verrà conservato per il periodo indicato nell'articolo 32, comma 3 del CAD;
6. Si invia al dispositivo di firma il certificato appena emesso, affinché quest'ultimo possa essere registrato in modo protetto all'interno del dispositivo stesso.
   Il meccanismo di invio del certificato prevede la comunicazione su canale cifrato;
7. Si provvede, sempre utilizzando un canale cifrato, a modificare i codici personali di attivazione del dispositivo di firma (smart-card o token) impostando gli stessi a dei valori contenuti in buste chiuse e sigillate (o scratch-card).
   In caso di chiavi di sottoscrizione generate dal Titolare all'interno di HSM, vengono individuate due casistiche:

   OID 1.3.6.1.4.1.29741.1.1.11.2: L'operazione di modifica dei codici personali di attivazione non è applicabile in quanto tali dispositivi possiedono policy di accesso alle funzionalità crittografiche e alle relative chiavi, notevolmente differenziate che, nei casi più stringenti, possono prevedere anche meccanismi di autenticazione a doppio fattore.
   OID 1.3.6.1.4.1.29741.1.1.11.1: Alle chiavi di sottoscrizione del Titolare viene automaticamente associata una credenziale di autenticazione forte (ad esempio OTP o dato biometrico) già in possesso del Titolare ed utilizzata in fase di generazione della coppia di chiavi.
   L'accesso alla coppia di chiavi è inoltre assoggettato alla conoscenza di uno Username e di un Password precedentemente scelte dal Titolare stesso (nel caso dell'OTP) o alla presenza fisica del Titolare dinnanzi ad un incaricato della CA (nel caso del riconoscimento basato su tecniche biometriche).

8. Si provvede ad associare al titolare di ciascun certificato emesso un codice riservato da utilizzare, in caso di emergenza, per l'autenticazione della eventuale richiesta di sospensione del certificato;
9. Si provvede a registrare la generazione di ciascun certificato nel giornale di controllo;
10. Si rendono disponibili al Titolare i codici personali ed il codice di emergenza attraverso procedure sicure:
    a. Nel caso di chiavi generate dal Certificatore, i codici personali, unitamente al codice di emergenza, vengono resi disponibili al Titolare attraverso l'invio di una busta chiusa e sigillata (o scratch-card) contenente tali informazioni;

    b. Nel caso di chiavi generate dal CDRL, i codici personali, unitamente al codice di emergenza, vengono resi disponibili al Titolare attraverso la consegna di una busta chiusa e sigillata (o scratch-card) contenente tali informazioni;

[3] A tal proposito il codice identificativo sarà diverso nel caso che un medesimo richiedente possieda più certificati (ad esempio per diversi ruoli o per motivi di affidabilità del servizio).

c. Nel caso di chiavi di sottoscrizione generate dal Titolare all'interno di HSM, vengono individuate due casistiche:

   i. **OID 1.3.6.1.4.1.29741.1.1.11.1:** I codici personali di attivazione del dispositivo sicuro, unitamente al codice di emergenza, risultano già a disposizione del Titolare. Lo Username e la Password vengono impostati dal Titolare in fase di generazione della coppia di chiavi. La credenziale OTP ed il codice di emergenza sono già stati consegnati al Titolare al momento della sua identificazione.

      Nel caso di chiavi di sottoscrizione il cui utilizzo è assoggettato a meccanismi di autenticazione/autorizzazione di tipo biometrico (ad es. grafometria), il codice di emergenza è consegnato al Titolare al momento della sua identificazione.

   ii. **OID 1.3.6.1.4.1.29741.1.1.11.2:** I codici personali di attivazione del dispositivo sicuro di firma non vengono modificati (cfr step 7 del presente paragrafo). Il codice di emergenza viene altresì notificato al Titolare attraverso procedure sicure.

Qualora esistano delle condizioni che impediscano la generazione del certificato, il sistema o provvede a rigettare la richiesta e a segnalare l'evento all'operatore ovvero al Titolare richiedente.

4.5.3 Formato e contenuto del certificato

Il profilo del certificato di firma digitale emesso da Aruba PEC S.p.A. è conforme a quanto previsto dalla Deliberazione CNIPA [7] e contiene le informazioni previste nell'art. 19 del DPCM e nell'art. 28 del CAD e successive correzioni ed integrazioni. In questo modo ne è garantita la piena interoperabilità all'interno del contesto della normativa e dei certificatori italiani.
Attributi ed estensioni facoltativi possono variare in rapporto alle specifiche policy utilizzate, previamente concordate con il cliente.
Il certificato inoltre contiene l'indicazione di Certificato Qualificato.
Ciò è realizzato attraverso l'inserimento dell'apposita estensione: [Qualified Certificate Statements - esi4-qcStatement-1 (OID: 0.4.0.1862.1.1)] nel rispetto di quanto previsto dalla norma ETSI TS 101 862.

All'interno del certificato posso infine essere presenti i seguenti OID che qualificano ulteriormente il suo utilizzo e tipologia:

Certificati di Firma Digitale senza limitazioni d'uso	1.3.6.1.4.1.29741.1.1.1
Certificati di Firma Digitale su HSM ospitato presso il Certificatore	1.3.6.1.4.1.29741.1.1.11.1
Certificati di Firma Digitale su HSM ospitato presso Cliente	1.3.6.1.4.1.29741.1.1.11.2
Certificati di Firma Digitale con limitazioni d'uso[4].	1.3.6.1.4.1.29741.1.1.13
Certificati di Firma Digitale con procedura automatica	1.3.6.1.4.1.29741.1.1.15

[4] La particolare limitazione è inserita nell'attributo *explicitText* del campo *userNotice* dell'estensione certificatePolicies. Sul sito istituzionale del DigitPA sono inoltre pubblicati i testi e le codifiche delle limitazioni d'uso che i certificatori devono garantire agli utenti.

4.6 Modalità di inoltro delle richieste e della gestione di sospensione e revoca dei certificati (art. 40/3/l)

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

4.6.1 Circostanze che impongono la sospensione o la revoca del certificato

La sospensione o revoca del certificato avviene, nel rispetto delle disposizione 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) e sottoscritta da questi
2. Richiesta da parte del "terzo interessato" da inviare mezzo Fax o PEC unitamente alla fotocopia del documento di identità di colui che sta richiedendo la revoca o sospensione.
3. Richiesta scritta da parte del Titolare da inviare mezzo Fax o PEC.
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 della chiave privata.
7. Smarrimento del dispositivo sicuro di firma o della chiave privata.
8. Abusi e falsificazioni.
9. Richiesta proveniente 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.

4.6.2 Richiesta di sospensione o revoca da parte del Titolare

La revoca/sospensione del certificato può essere effettuata dal Titolare dello stesso secondo due 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. Firma del Titolare del certificato.

Alla richiesta di revoca deve essere allegata una fotocopia del documento di identità.

La sospensione del certificato può essere effettuata direttamente dal Titolare dello stesso attraverso il servizio disponibile presso la pagina https://lcm.arubapec.it/lcm/, esplicitamente dedicata alla sospensione dei certificati, tramite codice riservato di emergenza (codice utente) consegnato insieme al PIN/PUK della smart card, in una busta retinata (o scratch-card) fornita separatamente dalla smart card a seguito della generazione del certificato.

In alternativa la sospensione può avvenire contattando il seguente numero telefonico 05751939715 e fornendo come credenziali di autenticazione i propri dati unitamente al codice riservato di emergenza (codice utente) consegnato assieme al certificato che si intende sospendere.

In particolare si evidenzia che 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.

4.6.3 Sospensione o revoca su iniziativa del Certificatore

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 dell'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 privata certificazione attraverso la quale è stato firmato il certificato del Titolare.
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 la revoca sarà efficace.

4.6.4 Richiesta di sospensione o revoca da parte del terzo interessato

La revoca/sospensione del certificato può essere richiesta dal "terzo interessato" 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. Dati identificativi e firma di colui che sta richiedendo la revoca/sospensione del certificato.

Alla richiesta di revoca deve essere allegata una fotocopia del documento di identità di colui che sta richiedendo la revoca/sospensione del certificato.

A mero titolo esemplificativo, il "terzo interessato" può richiedere la sospensione o la revoca di un certificato 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.

4.6.5 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 CRL sarà 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.

Si rende noto che l'Ente Certificatore Aruba Pec S.p.A. fissa al giorno antecedente la scadenza del certificato la durata massima dello stato di sospensione dei certificati.
Aruba Pec, attraverso un meccanismo di notifica automatico e con un preavviso di 10 giorni rispetto al termine sopraindicato, comunica, al titolare dei certificati ed eventualmente al soggetto che ha richiesto la sospensione, l'approssimarsi della scadenza del periodo di sospensione.
Il giorno antecedente la scadenza del certificato, e in assenza di diverse indicazioni da parte del soggetto che ha richiesto la sospensione ovvero da parte del titolare, Aruba Pec procederà d'ufficio, anche a fini cautelativi, alla revoca dei certificati sospesi con decorrenza pari alla data di sospensione.

4.7 Modalità di sostituzione delle chiavi (art. 40/3/m)

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

4.7.1 Sostituzione chiavi di sottoscrizione dei Titolari

Ai sensi dell'art. 19 del DPCM, la Aruba PEC S.p.A. determina da un minimo di anni 3 (tre) ad un massimo di anni 6 (anni) 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 almeno 30 gg rispetto alla scadenza del certificato, la Aruba PEC S.p.A. comunica via e-mail all'indirizzo fornito dal Titolare in fase di identificazione, l'approssimarsi della scadenza. Per la sostituzione il Titolare dovrà prendere contatto con il CDRL di riferimento o con il Certificatore.

I passi principali sono:

- Compilazione del modulo di richiesta del certificato e successiva firma digitale dello stesso, a cura del titolare, tramite il certificato in scadenza che non deve essere sospeso o revocato.
- Invio del suddetto modulo ad Aruba Pec S.p.A. o al CDRL di riferimento.
- Verifica della correttezza dei dati contenuti nel modulo e della validità della firma digitale associata.
- Emissione nuova smart card e consegna separatamente alla busta PIN PUK (o scratch-card), all'indirizzo comunicato dall'utente oppure consegna del kit nella mani del titolare a cura di un Operatore di Registrazione.

Dal suddetto elenco sono escluse le pratiche amministrative di pagamento della sostituzione delle chiavi.
Per i costi e le modalità si rimanda al form di richiesta informazioni presente sul sito web http://www.pec.it.

4.7.2 Sostituzione delle chiavi di certificazione

La sostituzione delle chiavi di certificazione avviene sotto il controllo del responsabile della generazione e custodia chiavi in presenza del responsabile del servizio tecnico o sotto la sua supervisione. L'operazione è finalizzata alla sostituzione ed alla configurazione delle coppie di chiavi di certificazione. Il processo è analogo a quanto indicato in 4.4.1 ed avviene con almeno 3 mesi di anticipo rispetto alla scadenza del certificato relativo alla coppia di chiavi di certificazione da sostituire.

4.7.3 4.7.3 Sostituzione delle chiavi di marcatura temporale

La sostituzione delle chiavi di marcatura temporale viene eseguita dopo non più di tre mesi di utilizzazione ed è attivata sotto il controllo del responsabile del servizio di certificazione e validazione temporale. La procedura è analoga a quanto indicato in 4.4.3.

4.8 Modalità di gestione e di accesso del registro dei certificati (art. 40/3/n/o)

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

4.8.1 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 e HTTP 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 (HTTP).
2. I certificati pubblici per le chiavi dei Titolari ove richiesto (LDAP HTTP).
3. I certificati pubblici per le chiavi del Certificatore Aruba PEC S.p.A (HTTP).
4. I certificati per le chiavi di firma del DigitPA (ex CNIPA) (LDAP HTTP).

TUTTI COLORO CHE INTENDONO FARE AFFIDAMENTO SU UNA FIRMA DIGITALE E/O SULLE INFORMAZIONI CONTENUTE NEL CERTIFICATO ASSOCIATO AD ESSA DEVONO:

1. CONSULTARE PREVENTIVAMENTE IL REPOSITORY DELL'ENTE CERTIFICATORE AL FINE DI VERIFICARE (NELLE APPOSITE LISTE DEI CERTIFICATI REVOCATI O SOSPESI, DISPONIBILI PER VIA TELEMATICA AGLI UTENTI – CRL, CSL) SE IL CERTIFICATO SIA VALIDO E NON REVOCATO O SOSPESO.
2. VERIFICARE SE LA FIRMA DIGITALE SIA STATA CREATA DURANTE IL PERIODO DI VALIDITA' DEL CERTIFICATO STESSO DALLA CHIAVE PRIVATA CORRISPONDENTE ALLA CHIAVE PUBBLICA RIPORTATA NEL CERTIFICATO.

4.8.2 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.
Ai fini della consultazione la copia di riferimento è accessibile in modo anonimo ed in sola lettura attraverso dei Front End internet tramite protocollo HTTP e LDAP.

Il prototipo di una richiesta LDAP per un certificato utente è :

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

Il link per la consultazione HTTP è contenuto invece all'interno delle pagine del Web server firma digitale.

4.9 Modalità di protezione dei dati personali (art. 40/3/q)

4.9.1 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.

4.9.2 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".

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

Vale quanto indicato nel par. 3.2.

4.10 Modalità per l'apposizione e la definizione del riferimento temporale (art. 40/3/p)

4.10.1 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 che garantisce una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC (IEN), di cui al decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591.

4.10.2 Marcatura temporale

Il servizio di marcatura temporale offerto da Aruba PEC S.p.A. è fruibile attraverso protocollo HTTPS.
I formati e la codifica delle richieste accettate e delle marche temporali restituite dal servizio sono conformi alle strutture dati descritte nella RFC 3161.
La richiesta viene accettata dal web server servizi.arubapec.it, tramite l'indirizzo https://servizi.arubapec.it/tsa/ngrequest.php (che deve essere configurato all'interno del client prescelto per l'interfacciamento al servizio) con le credenziali fornite da Aruba PEC S.p.A. al momento dell'attivazione dell'account TSA (che devono essere inserite nel software prescelto per l'interfacciamento al servizio).
Il servizio di TSA ArubaPec accetta solo ed esclusivamente richieste di marcatura temporale contenenti impronte dell'evidenza informatica da sottoporre a validazione temporale calcolate secondo l'algoritmo hash SHA-1 (dedicated hash-function 3 definito nella norma ISO/IEC 10118-3:2004) e secondo l'algoritmo hash SHA-256 (dedicated hash-function 4 definito nella norma ISO/IEC 10118-3:2004).
Nel caso in cui il sistema TSA riceva una richiesta di marcatura temporale non conforme al requisito di cui sopra viene restituito un messaggio di errore.

4.10.3 Sicurezza logica e fisica del sistema di marcatura temporale

Gli elaboratori che offrono il servizio di marcatura temporale possiedono i medesimi requisiti di protezione previsti dagli elaboratori utilizzati per la generazione dei certificati di firma digitale, e sono protetti da livelli di protezione logica estremamente elevati. La medesima collocazione fisica del sistema di validazione temporale garantisce gli elaboratori dalla possibilità di compromissioni fisiche grazie agli accorgimenti tecnici atti ad impedire accessi non autorizzati da persone e danneggiamenti da eventi accidentali.

4.10.3.1 Sicurezza fisica

Il sistema di validazione temporale reso disponibile da Aruba Pec ai propri titolari si basa su dei server web di Front-end che gestiscono le transazioni con i client, l'autenticazione, l'accounting e l'archiviazione delle marche temporali ed dei server di Back-end che si occupano della creazione delle marche temporali e della gestione degli apparati di acquisizione e sincronizzazione del riferimento temporale.
I server del sistema di validazione temporale sono ospitati in sale tecniche ad accesso controllato attraverso badge e/o fattore biometrico.
Solo il personale autorizzato può accedere a tali sale. Questi ambienti, inoltre, sono protetti da allagamenti ed incendi mediante appositi presidi (sensori, spruzzatori, condiziona-mento, etc) e gli elaboratori sono alimentati con linea elettrica preferenziale, sorretta da gruppo di continuità.

4.10.3.2 Sicurezza logica

I server di Front-end e di Back-end del sistema di validazione temporale dialogano tra loro attraverso protocolli di comunicazioni sicuri e possono essere attivati solo da operatori autorizzati.
In particolare, i server di Back-end firmano le marche temporali mediante un dispositivo crittografico hardware (o "dispositivo di firma") di altissima qualità e sicurezza. L'algoritmo di sottoscrizione utilizzato è RSA con chiave di lunghezza 2048 bit ed usata esclusivamente a scopo di marcatura temporale. La coppia di chiavi RSA è generata all'interno del dispositivo di firma. La chiave privata della coppia è usata all'interno del dispositivo di firma. Il dispositivo di firma può essere attivato solo da un operatore appositamente autorizzato e dotato della necessaria parola-chiave.

4.11 Modalità operative per l'utilizzo del sistema di verifica delle firme (art. 40/3/r)

In riferimento all'art. 14 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 / 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 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 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).

I prodotti di verifica delle firme forniti da Aruba PEC sono conformi a quanto indicato all'art. 42, commi 2 e 6 del DPCM ed ai requisiti di cui all'art.27 della DELIB. 45/09 [7].

4.12 Modalità operative per la generazione della firma elettronica qualificata e della firma digitale (art.40/3/s)

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

1. Apporre una firma digitale producendo come risultato una busta crittografica, nel formato standard PKCS#7 / CAdES[5].
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 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.
Sintesi operativa dell'utente:

1. Avviare l'applicazione di firma;
2. Selezionare la funzione di firma dal menu principale o dal menù contestuale;
3. Selezionare il file da firmare;
4. Digitare il codice personale per l'accesso al dispositivo sicuro di firma;

L'applicativo di firma di Aruba PEC permette di sottoscrivere digitalmente ogni tipo di file e, tramite un apposita funzione, del menù, consente la visualizzazione delle seguenti tipologie di file:

DOC (corrispondente al prodotto Microsoft Word)
XLS (corrispondente al prodotto Microsoft Excel)
PDF (corrispondete al prodotto Adobe Acrobat o Adobe Reader)
TIF
JPEG
BMP
RTF
TXT
HTM/HTML

L'utente deve tenere ben presente il fatto che alcuni di questi 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 [2]).
Tali file, seppur sottoscritti con firma digitale, non producono gli effetti di cui all'articolo 21, comma 2 del CAD [6].
È unicamente responsabilità dell'utente firmatario accertarsi, attraverso le funzionalità tipiche di ciascun prodotto, che tale condizione sia soddisfatta.

[5] Alla data del presente Manuale, il formato in vigore per la creazione di buste crittografiche destinate a contenere documenti informatici sottoscritti digitalmente, risulta essere conforme allo standard Rfc 2315 (PKCS#7). Si rende noto per tanto che gli applicativi per la Firma Digitale forniti dall'Ente Certificatore Aruba Pec S.p.A. abilitano l'utilizzo del formato CAdES (ETSI TS 101 733) a far data dal 1 Settembre 2010.

Nell'Appendice A sono riportate delle linee guida che posso essere seguite per verificare che il documento non contenga macroistruzioni o codici eseguibili.

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 [6]).

4.13 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

Sospensione tramite web :

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

Sospensione via Telefono:

Operatore:	dalle 09:00 alle 18:00 tutti i giorni lavorativi

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, ai soli fini di verifica delle Firme Digitali, 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 PEC indirizzati alla seguente casella direzione.ca@arubapec.it oppure in forma 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.: Via Sergio Ramelli, 8 – 52100 Arezzo

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.
Le modifiche sostituiranno qualsiasi disposizione in conflitto con la versione di riferimento del Manuale Operativo.

5.1.8 Violazioni e altri danni materiali

I titolari e 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, nomi societari, o 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.

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.

Appendice A Codici eseguibili e Macroistruzioni

In questa appendice vengono riportate le linee guida per verificare la presenza di macroistruzioni e codici eseguibili all'interno dei formati di cui al paragrafo 4.12 e, nell'eventualità, per disabilitarne l'esecuzione da parte degli applicativi comunemente utilizzati per la loro visualizzazione.
In particolare verranno presi in considerazione i seguenti software:

MS Word 2003	Normalmente associato dal sistema operativo Windows alla gestione dei file con estensione **.doc**
MS Excel 2003	Normalmente associato dal sistema operativo Windows alla gestione dei file con estensione **.xls**
Adobe Acrobat 8.0	Normalmente associato dal sistema operativo Windows alla gestione dei file con estensione **.pdf**
Adobe Reader 8.0	Normalmente associato dal sistema operativo Windows alla gestione dei file con estensione **.pdf**

A.1 MS Word 2003 e MS Excel 2003

Macro
Il termine Macro sta ad indicare una procedura che permette di eseguire un insieme di comandi applicativi in sequenza attraverso un unico evento scatenante, quale ad esempio l'apertura del documento o il singolo click del mouse.
Queste componenti sono caratterizzate da un elevato livello di criticità in quanto possono accedere a tutte le funzionalità del sistema operativo.
Per verificare che all'interno di Office 2003 sia attivata la protezione da Macro è sufficiente seguire i seguenti passi:

1. Scegliere la voce **Opzioni** dal menù **Strumenti**.
2. Fare click sulla scheda **Protezione**.
3. Scegliere **Protezione macro** nella sezione **Protezione macro**.
4. Fare click sulla scheda **Livello di protezione.**
5. Selezionare quindi il livello di protezione desiderato in base a quanto riportato nella descrizione associata al relativo livello.

Si noti che pur impostando il livello di protezione ai valori **Elevato** o **Molto elevato** le Macro continueranno a persistere all'interno del documento e pertanto sottoscrivendo digitalmente il file verranno firmate anche le relative Macro. Per tale ragione si consiglia di impostare il livello di protezione delle Macro su **Medio** in modo da avere l'evidenza della presenza delle stesse.
Per approfondimenti circa il comportamento di MS Word 2003 e MS Excel 2003 in presenza di Macro si consiglia la consultazione della Guida in linea dei prodotti alle voci **Sommario → Protezione e riservatezza → Macro**.

MS Word 2003: Codici automatici
I codici automatici o codici di campo di Word sono delle componenti che vengono inserite in un documento per far in modo che Word vi inserisca del testo recuperando le relative informazioni in modo automatico dal contenuto del documento (indici, sommari, riferimenti), dalle sue proprietà (numero di pagine, autore del documento) o da quelle della macchina (data e ora di sistema).
Per visualizzare/nascondere i campi in Word seguire i seguenti passi:

1. Scegliere la voce **Opzioni** dal menù **Strumenti**.
2. Fare click sulla scheda **Visualizza**.
3. Attivare la check box **Codici di campo**.
4. Selezionare dal sottostante menù **Ombreggiatura campo: Sempre**.

MS Excel 2003: Formule
Le formule Excel sono delle componenti che eseguono calcoli e permettono di valorizzare automaticamente determinate sezioni del foglio di lavoro su cui sono inserite.
Per visualizzare tutte le formule contenute in un foglio Excel seguire i seguenti passi:

1. Scegliere la voce **Opzioni** dal menù **Strumenti**.
2. Fare click sulla scheda **Visualizza**.
3. Attivare la check box **Formule**.

Per nascondere tutte le formule seguire la stessa procedura e disattivare il check box **Formule**.

A.2 Adobe Reader e Acrobat (8.0)

E' possibile che documenti PDF (Portable Document Format) contengano al loro interno codice Javascript che, una volta interpretato dal Adobe Reader o Adobe Acrobat vada a modificare dinamicamente quanto riportato a video all'utente finale.

Per disattivare nell'Adobe Acrobat o Adobe Reader la possibilità di esecuzione di codice Javascript contenuto nei file pdf si possono seguire i seguenti passi:

1. Selezionare il menù **Modifica**.
2. Scegliere **Preferenze**.
3. Nella listbox a sinistra della finestra **Preferenze** posizionarsi con il mouse sopra la voce **Javascript** ed evidenziarla con un click.
4. Deselezionare la checkbox **Abilita JavaScript di Acrobat**.
5. Da questo momento l'eventuale presenza di Javascript verrà segnalata da un messaggio.

A.3 File HTML

Infine, 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.

Appendice B Procedura di Firma Digitale con autorizzazione all'utilizzo delle chiavi di sottoscrizione attraverso tecniche di tipo grafometrico

Come indicato in § 4.5.3 le chiavi di firma possono essere generate e conservate anche in un HSM remoto. Per firmare il titolare dovrà accedere all'HSM utilizzando opportuni applicativi web (e non) e, una volta verificato il documento o i documenti da firmare, avviare la procedura di sottoscrizione.
Di norma, per questa tipologia di servizi, l'accesso all'HSM viene gestito attraverso l'impiego di soluzioni di strong authentication come ad esempio l'OTP.
In questo paragrafo viene descritto un meccanismo di accesso/autorizzazione basato su tecnica grafometrica inteso come metodo alternativo per garantire il controllo esclusivo delle coppie di chiavi di sottoscrizione conservate all'interno degli HSM.

B.1 Procedura di enrollment

In questa fase viene richiesto all'utente di apporre in successione più firme attraverso l'utilizzo di una specifica penna e di uno specifico tablet.
Per ogni firma apposta il sistema, grazie ad uno specifico software, è in grado di trasporre in *specimen* una serie di informazioni relative al modo di firmare del Titolare.
Nel caso in cui una o più firme apposte dovessero risultare incongruenti con quelle già registrate, il sistema richiederebbe di effettuare nuovi tentativi fino ad arrivare ad un numero sufficiente di campioni in grado di abilitare la generazione di un profilo consistente per l'utente.
Questo meccanismo è legato alla necessità di minimizzare, in fase di verifica delle firme, queste due quantità:

- **False Match Rate (FMR):** Rappresenta la percentuale di false accettazioni all'interno del sistema biometrico. Nel caso specifico delle firme biometriche, questo rappresenta la percentuale di firme non valide accettate dal sistema;
- **False Non-Match Rate (FNMR):** Rappresenta la percentuale di false non-accettazioni all'interno del sistema biometrico. Nel caso specifico delle firme biometriche, questo rappresenta la percentuale di firme valide rigettate erroneamente dal sistema;

Ricordiamo inoltre che il match di una firma grafometrica, contrariamente a quanto potrebbe lasciar intendere il termine, non avviene in base al solo aspetto grafico ma, per una corretta verifica, concorrono più fattori, tra cui:

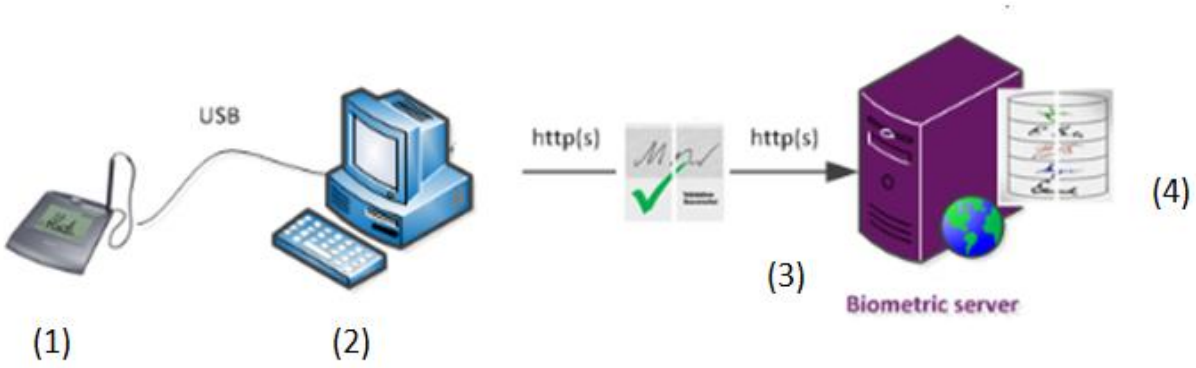
- Velocità,
- Accellerazione,
- Ritmo,
- Pressione,
- Movimento aereo.

Infine il sistema riesce anche a gestire il costante aggiornamento (enrollment continuo di nuovi *specimen* in fase di verifica della firma grafometrica) del profilo registrato al fine di far fronte alla necessità di seguire nel tempo le modifiche nel modo di firmare dell'utente (ad esempio un giovane che diventa adulto o ad un anziano che inevitabilmente potrebbe avere una scrittura più incerta).

B.1.1 Aspetti di sicurezza nel processo di Enrollment

L'intero processo di enrollment è progettato per garantire la massima sicurezza ai Titolari.

Segue una breve illustrazione del processo in cui viene posta enfasi agli aspetti collegati alla sicurezza:



- Il Tablet (1) comunica con l'applicazione Client (2) utilizzando un canale cifrato.
  L'applicazione Client potrebbe essere un applicativo Arubapec piuttosto che un applicazione di sportello (Banca, Assicurazione o ambito sanitario);

- Il Client (2) comunica poi con il Server(3), il server designato a verificare la validità delle firme appena apposte e della gestione delle procedure di enrollment precedentemente descritte. Anche in questo caso tutte le connessioni sono protette e cifrate via HTTPs;

- Il Server (3) si appoggia ad un Database (4) dove sono memorizzati (cifrati) tutti i profili dei Titolari. Questi profili potranno essere recuperati al momento opportuno, decifrati nella memoria del Server ed una volta utilizzati immediatamente rilasciati senza che alcunché di tale profili possa essere modificato in maniera dolosa e/o colposa.
  Sarà sempre il Server che ritornerà al Client l'esito del confronto (Verify_Match/Verify_NoMatch)

Oltre a quanto appena descritto altri aspetti di sicurezza vengono gestiti dall'applicazione, fra questi:

- Vengono utilizzati solo dispositivi Tablet in grado di instaurare comunicazioni cifrate;
- Tutte le comunicazioni fra i vari sistemi coinvolti sono cifrate;
- I dati grafometrici non sono mai in chiaro ma sempre cifrati;
- Il codice del software che gestisce i dati grafometrici è protetto da rischi di code injection;
- Tutti gli accesi ai sistemi vengono registrati nell'audit log del sistema.

B.2 Modalità di firma

Il titolare, al momento della firma, sarà stato identificato da un incaricato dell'Ente Certificatore (ad esempio caso in cui una Banca o un'Assicurazione svolgono, per conto di Arubapec, le attività di CDRL o IR).

Una volta che questo nuovo riconoscimento sarà stato effettuato ed una volta che il titolare avrà esaminato il/i documento/i da firmare potrà attivare il processo di Firma Digitale apponendo una firma su un dispositivo tablet con caratteristiche simili a quello utilizzato nel processo di enrollment.

Una misurazione delle caratteristiche collegate alla firma appena apposta, determinerà se questa è congruente o meno con il profilo registrato e associato all'utente.
Se la firma apposta sarà ritenuta congruente con il profilo, ed in considerazione del fatto che il Titolare si trova dinnanzi ad un incaricato della CA, la procedura di Firma Digitale potrà essere avviata.
Qualora invece la firma appena apposta ed il profilo registrato non dovessero essere congruenti, nonostante l'identificazione appena effettuata, verrà richiesto all'utente di apporre con maggiore attenzione una nuova firma.

Questo perché probabilmente il mancato match può essere dovuto a errori anche banali ma immediatamente rilevati dal sistema (mancanza di una lettera , omissione di vocali accentate …).
La nuova apposizione eseguita con maggior attenzione ha normalmente successo.