Aruba PEC S.p.A.

Certification Practice Statement

Versione: 1.7
Data: 11/11/2021
Redazione: Alessandro Capobianco
Verificato da: Nicole Mazzoni, Federico Ciofi
Approvato da: Andrea Sassetti
Classificazione documento: pubblico

Andrea Sassetti
Firmato digitalmente
il 11/11/2021
16:43:27 CET

Versione	Data	Modifiche
1.0	24 maggio 2016	Prima versione del documento.
1.1	11 ottobre 2016	p. 1.4 Aggiornata tabella definizioni p. 2.3 Aggiornato indice versione p. 4.4.3.1 Correzioni minori (refusi) p. 4.4.3.2 Correzioni minori (refusi) p. 4.5 Inserite modalità di qualifica applicazioni e rimosso riferimento ad appendice A p. 4.6 Inserito significato acronimi p. 4.7 Corretto periodo di conservazione log p. 4.8 Aggiornato piano cessazione TSA p. 5.1.8 Aggiornate le descrizione delle figure del presente paragrafo p. 5.1.9 Aggiornati i riferimenti alle norme applicabili Appendice A Rimossa del tutto
1.2	26 maggio 2017	Aggiornamento template Aggiornata sede legale
1.3	12 luglio 2017	Adozione nuovo template con codice identificativo mga p. 1.1 Aggiornati riferimenti normativi p. 2.3 Aggiornato riferimento versione p. 2.5 Corretti riferimenti Inserito nuovo paragrafo p. 2.5.1 p. 3.1.1 Integrati obblighi relying parties p. 4.2 Inserita specifica su fornitori esterni Rimosso p. 4.2.1 p. 4.4.3.2 Aggiornata modalità gestione chiavi c.5 Corretta numerazione p. 5.1 Aggiornati obblighi utenti e rimosso refuso
1.4	23 maggio 2019	Tutto il documento: aggiornamento logo e template p. 1.3 Aggiornati riferimenti normativi p. 2.1 Aggiornato Legale Rappresentante P. 3.1 Rimosso punto 4 relativo a raccolta e trattamento dati personali P. 3.2 Inserito rimando a informativa rilasciata ai sensi dell'art.13 del GDPR P. 4.3 Rimosso Capitolo P. 5.10 Indicazione competenza foro di Arezzo
1.5	14 ottobre 2019	P. 1.3 e 4.4 – sostituiti riferimenti Deliberazione CNIPA n. 45/2009 (abrogata) P. 2.2 – inserite indicazioni sull'applicazione delle raccomandazioni emanate dall'Agenzia con Det. AgID n.121/2019 P. 3.3.2 e 3.3.5 – riformulate le limitazioni di responsabilità del prestatore
1.6	21/01/2021	P. 1.3 - Revisione dei riferimenti normativi applicabili P. 2.3 – Modifiche minori P. 4.5 – Revisione della descrizione relativa alla disponibilità del servizio; P. 4.6 – Aggiunta una specifica
1.7	11/11/2021	P. 4.6 – Aggiornato periodo di conservazione log

SOMMARIO

INDICE DELLE FIGURE

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 validazione temporale.
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) 22 Febbraio 2013, "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali", pubblicato sulla Gazzetta Ufficiale 21 Maggio 2013, n. 117, nonché del Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
In particolare, il presente documento illustra le modalità di richiesta, validazione, emissione, utilizzo delle marche temporali erogate nell'ambito del servizio di validazione temporale elettronica qualificato, nonché le responsabilità e gli obblighi del certificatore, dei richiedenti e di tutti coloro che accedono al servizio per la verifica delle firme marche temporale.
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 ai servizi fiduciari ed alla struttura PKI.
Aruba PEC S.p.A., allo scopo di consentire un corretto utilizzo del servizio di validazione temporale elettronica qualificata, oltre a raccomandare all'utente una attenta lettura del presente documento, invita tutti coloro i quali dovranno fare affidamento su di una validazione temporale elettronica qualificata e/o sulle informazioni contenute nel certificato ad essa associato, 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 validazione temporale elettronica qualificata 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 validazione temporale elettronica qualificata non sia stato modificato.

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

Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules".
ISO/IEC 15408 (parts 1 to 3): "Information technology -- Security techniques -- Evaluation criteria for IT security".
ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".
FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".
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] Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
[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, e ss.mm.ii..
[5] Decreto Legislativo (CAD) 7 marzo 2005, n. 82: “Codice dell’amministrazione digitale”, pubblicato nella Gazzetta Ufficiale. n. 112 del 16 maggio 2005.
[6] Determinazione n. 121 del 17 maggio 2019, “Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate” (Determinazione n. 121/2019).

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

[8] 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.

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

1.4 Definizioni ed acronimi

CA	Certification authority – Autorità di certificazione
CAD	Codice dell’Amministrazione Digitale
CRL	Certificate revocation list – lista dei certificati revocati
CSL	Certificate suspension list – lista dei certificati sospesi
CSR	Certificate signing request
AGID	Agenzia per l’Italia Digitale
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
ISO	International Standard Organization
ITSEC	Information Technology Security Evaluation Criteria
LDAP	Lightweight Directory Access Protocol
NTP	Protocollo di accesso a servizi di data e ora certa
OCSP	Protocollo per il controllo on-line dello stato dei certificati digitali
OID	Object Identifier
POP	Point of Presence
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
TLS	Transport Layer Security
TSA	Time Stamping Authority (sistema di marcatura temportale)
SP	Security Procedures – procedure di sicurezza Aruba PEC S.p.a
VTEQ	Validazione Temporale Elettronica Qualificata
WWW	World Wide Web
X.509	Specifica ITU-T in materia di certificazione e relativo framework di autenticazione
TSP	Trust Service Provider, Prestatore di Servizi Fiduciari

2 DATI IDENTIFICATIVI - PUBBLICAZIONE MANUALE OPERATIVO

2.1 Dati identificativi del Prestatore di Servizi Fiduciari Qualificato

Denominazione Sociale : **Aruba PEC S.p.A.**
Sede legale: **Via San Clemente, 53 – 24036 Ponte San Pietro (BG)**
Legale Rappresentante : **Giorgio Cecconi**
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 servizi fiduciari: https://ca.arubapec.it

2.2 Identificativo della policy

L'identificativo della politica di validazione temporale elettronica (time-stamp policy) descritta nel presente documento è **0.4.0.2023.1.1**, corrispondente alla "**Best practices Time-Stamp Policy**" (BTSP) definita nella norma **ETSI TS 319 421**. Includendo tale object identifier (OID) nelle marche temporali (time-stamp token), la TSA di Aruba PEC attesta la propria conformità alla policy BTSP.

Salvo diversa richiesta degli interessati, i certificati elettronici destinati ai sistemi di validazione temporale elettronica qualificata sono emessi secondo l'applicazione delle raccomandazioni emanate dall'Agenzia e volte a garantire maggiormente l'interoperabilità e la fruizione dei servizi in rete nel contesto italiano (Determinazione AgID n.121/2019, e successive modificazioni ed integrazioni). La piena applicazione delle raccomandazioni oggetto del provvedimento è dichiarata attraverso la codifica, nel campo CertificatePolicies (OID 2.5.29.32), di un elemento PolicyIdentifier con valore **agIDcert** (OID 1.3.76.16.6). Quanto indicato nel presente Time-Stamping Authority Practice Statement presuppone il pieno soddisfacimento di tali raccomandazioni.

2.3 Versione del manuale operativo

Il presente Manuale Operativo è di proprietà di Aruba PEC S.p.A., tutti i diritti sono ad essa riservati.
Il Manuale Operativo sarà aggiornato dal responsabile in presenza di significativi mutamenti tecnici o normativi che comportino una modifica del servizio. In caso di aggiornamento sostanziale verrà pubblicata una nuova versione del documento. In caso di aggiornamento minore sarà pubblicata una nuova release. Il numero di versione/release è riportato in copertina del documento ed in calce ad ogni pagina dello stesso.

2.4 Pubblicazione del manuale

Questo documento è pubblicato sulle pagine principali del web server dei servizi fiduciari indicato all'interno del paragrafo 2.1.

2.5 Responsabile del manuale operativo

Aruba PEC è responsabile della definizione, pubblicazione ed aggiornamento di questo documento.Il soggetto responsabile del presente manuale operativo all'interno di Aruba PEC è:

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

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

2.5.1 Redazione e revisione del manuale operativo

La redazione e approvazione del manuale operativo segue le procedure previste dal Sistema di Gestione Qualità aziendale.
In particolare il manuale viene riesaminato e, se necessario, aggiornato con frequenza almeno annuale e le modifiche vengono approvate dalla Direzione dei servizi di CA, previa verifica da parte delle funzioni aziendali interessate.

3 DISPOSIZIONI GENERALI

3.1 Obblighi del richiedente, del prestatore di servizi fiduciari e degli utenti

1. Il richiedente del servizio di Validazione Temporale Elettronica Qualificata è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.
2. Il prestatore di servizi fiduciari qualificato è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.
3. Il prestatore di servizi fiduciari qualificato che rilascia eroga il servizio di Validazione Temporale Elettronica Qualificata deve inoltre:
    a. Garantire che la validazione temporale elettronica qualificata collega la data e l'ora ai dati elettronici in modo da escludere ragionevolmente la possibilità di modifiche non rilevabili dei dati stessi;
    b. si basa su una fonte accurata di misurazione del tempo collegata al tempo universale coordinato;
    c. è apposta mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente;
    d. informare i richiedenti in modo compiuto e chiaro, sulla procedura di rilascio delle validazioni temporali elettroniche qualificate e sui necessari requisiti tecnici per accedervi;
    e. predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio fiduciario validazione temporale elettronica qualificata, tra cui in particolare gli esatti termini e condizioni relative all'uso della validazione temporale elettronica qualificate 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 prestatore di servizi fiduciari qualificato.

3.1.1 Obblighi di coloro che accedono alla verifica delle validazioni temporali elettroniche

Coloro che intendono utilizzare documenti a cui sono associate delle validazioni temporali elettroniche qualificate dovranno:

1. verificare che le informazioni contenute nella validazione temporale elettronica qualificata corrispondano a quelle del prestatore di servizi fiduciari qualificato;
2. verificare che il messaggio associato non sia stato modificato e/o alterato;
3. verificare che la validazione temporale elettronica qualificata sia correttamente sottoscritta dal prestatore di servizi fiduciari e che la chiave privata utilizzata per tale sottoscrizione non sia stata compromessa prima del momento dell'apposizione del riferimento temporale.

3.2 Obblighi connessi al trattamento dei dati personali

Il prestatore di servizi fiduciari qualificato raccoglie i dati personali degli Interessati esclusivamente secondo quanto previsto dall'informativa rilasciata ai sensi dell'articolo 13 del Regolamento UE 2016/679. I dati non possono essere raccolti o elaborati per finalità diverse senza l'espresso consenso della persona cui si riferiscono.

3.3 Limitazioni di Responsabilità ed eventuali limitazioni agli indennizzi

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 servizio di VTEQ e coloro i quali intendono accedere alla verifica delle VTEQ sono tenuti a consultare preventivamente ed a conoscere il presente Manuale Operativo, con particolare riferimento alle modalità in esso descritte per le operazioni di validazione temporale e di verifica. 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

Fatto salvo il caso di dolo o negligenza, la responsabilità del prestatore di servizi fiduciari qualificato sarà esclusa nel caso di eventi che esulino dalla volontà dello stesso o da cause ad esso non imputabili. Il prestatore di servizi fiduciari qualificato quindi non sarà responsabile, eccettuate le ipotesi di dolo o negligenza, 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, scioperi, incendi, azioni di guerra, epidemie, colpi di stato, terremoti e altri disastri.

3.3.3 Declinazioni e Limitazioni del Prestatore di servizi fiduciari qualificati

Il prestatore di servizi fiduciari qualificati una volta terminata l'erogazione della validazione temporale elettronica qualificata non ha alcun ulteriore obbligo di verifica della validità dei dati e delle informazioni contenute nella richiesta né sul medesimo grava alcun obbligo, anche anteriormente all'erogazione della medesima validazione temporale elettronica qualificata, di verifica della validità, correttezza ed integrità dei documenti informatici a cui l'utente vuole associare la validazione; il prestatore di servizi fiduciari qualificato non assume alcun ulteriore obbligo, garanzia o responsabilità rispetto a quanto previsto nel presente Manuale Operativo o 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 il servizio di VTEQ e l'utente che procede alla verifica delle stesse manlevano e tengono indenne il prestatore di servizi fiduciari qualificato 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 prestatore di servizi fiduciari qualificato sia chiamato a rispondere nei confronti dei terzi per fatto imputabile al richiedente e/o all'utente del servizio di VTEQ, ivi espressamente incluse, a titolo esemplificativo e non esaustivo, le responsabilità e i danni derivanti dalla eventuale invalidità, erroneità o non attualità delle informazioni o dei dati trasmessi al prestatore di servizi fiduciari qualificato e/o dal non corretto utilizzo delle procedure descritte nel presente Manuale Operativo.

3.3.5 Esclusione di risarcibilità di danni indiretti

Salvo i casi di dolo o negligenza il prestatore di servizi fiduciari qualificato 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, digitali validazioni temporali elettroniche qualificate o qualsiasi altra transazione digitale o servizio offerto o contemplato dal presente Manuale Operativo.

3.3.6 Limitazioni di responsabilità

Il servizio di validazione temporale elettronica qualificata 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.

3.3.7 Attività pericolose

Il servizio di validazione temporale elettronica qualificata 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

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

4 OPERATIVITA'

Questa sezione descrive le modalità con le quali opera il prestatore di servizi fiduciari qualificato ed in particolare le funzioni del personale addetto al servizio di certificazione validazione temporale elettronica qualificato, le modalità di richiesta delle validazioni e le modalità di comunicazione con il richiedente.

4.1 Funzioni del personale addetto al Servizio di Validazione temporale elettronica qualificata

La struttura organizzativa è definita nel rispetto degli standard ETSI EN 319 401 e in conformità con la vigente normativa italiana.
I ruoli di fiducia e le relative responsabilità sono assegnate formalmente dalla Direzione mediante lettere di incarico. I requisiti per il mantenimento dell'incarico vengono rivalutati con cadenza almeno annuale e a fronte di cambiamenti nella struttura organizzativa dell'azienda. Gli incaricati possono avvalersi, per lo svolgimento delle proprie attività, di addetti e collaboratori, nel rispetto delle disposizioni generali stabilite dall'azienda.
Le funzioni e le mansioni del personale sono distribuite in modo che una sola persona non sia in grado di eludere le misure di sicurezza a tutela dei sistemi di TSA; inoltre, i soggetti designati sono liberi da conflitti di interesse che potrebbero pregiudicare l'imparzialità delle attività loro assegnate.
Aruba PEC ha definito i seguenti ruoli di fiducia / figure di responsabilità nell'ambito del servizio di TSA:

- Security Officer: responsabile nel complesso per l'implementazione e la gestione delle procedure di sicurezza. Questa figura corrisponde al "Responsabile per la Sicurezza" previsto dalla vigente normativa italiana.
- System Administrator: responsabile per l'installazione, la configurazione e il mantenimento dei sistemi della TSA. Tra i System Administrator è ricompresa la figura del "Responsabile della Conduzione Tecnica dei Sistemi" prevista dalla vigente normativa.
- System Operator: responsabile per l'operatività quotidiana dei sistemi della TSA.
- System Auditor: responsabile della verifica degli archivi e dei log di audit dei sistemi di TSA.

Ai sensi della vigente normativa italiana, in Aruba PEC sono inoltre designate le seguenti figure di responsabilità in aggiunta a quelle sopra citate:

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

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

4.2 Rapporti con le organizzazioni esterne

Il prestatore di servizi fiduciari qualificato può avvalersi di terze parti, anche facenti parte del gruppo societario a cui appartiene Aruba PEC, a cui possono essere demandate attività per la migliore erogazione del servizio.
In tali ipotesi il prestatore di servizi fiduciari qualificato vincola, a mezzo di appositi accordi, le organizzazioni esterne:

a) al rispetto di quanto previsto nel presente Manuale Operativo;
b) al rispetto della normativa tecnica e giuridica applicabile per l'esecuzione del servizio;
c) al rispetto delle policy interne relative al trattamento dei dati personali dei clienti e degli utenti;
d) al rispetto delle policy di sicurezza, logica e fisica, adottate dal prestatore di servizi fiduciari qualificato all'interno della propria struttura;
e) al rispetto delle policy di qualità adottate dal prestatore di servizi fiduciari qualificato.

I soggetti esterni a cui possono essere demandate attività nell'ambito dei servizi fiduciari regolati dal presente Manuale Operativo sono scelti e selezionati tenuto conto di caratteristiche di esperienza, competenza e professionalità tali da assicurare il rispetto delle previsioni contenute nel presente documento e nelle normative in esso richiamate.

Alla data di redazione del presente Manuale Operativo il TSP-Q Aruba PEC non si avvale di alcun fornitore esterno al Gruppo Aruba per l'erogazione del servizio di validazione temporale qualificata.

4.3 Modalità operative per l'apposizione e la definizione della validazione temporale elettronica qualificata

4.3.1 Validazione Elettronica Temporale Qualificata

La validazione elettronica temporale qualificata 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 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.
La validazione temporale elettronica qualificata è erogata da Aruba PEC sulla base di quanto previsto dall'art. 42 del Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE e relative norme di attuazione.

4.3.2 Richiesta del servizio di validazione temporale elettronica qualificata

Il servizio di temporale validazione elettronica temporale qualificata offerto da Aruba PEC S.p.A. è fruibile attraverso protocollo HTTPS.
I formati e la codifica delle richieste accettate e delle temporali validazioni temporali elettroniche qualificate restituite dal servizio sono conformi alle strutture dati descritte nella RFC 3161 e ETSI EN 319 422.
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 Aruba PEC accetta solo ed esclusivamente richieste di marcatura temporale contenenti impronte dell'evidenza informatica da sottoporre a validazione temporale calcolate secondo l'algoritmo hash **SHA-256** (dedicated hash-function 4 definito nella norma ISO/IEC 10118-3:2004 e s.m.i).
Dopo aver autenticato l'utente e verificato la correttezza della richiesta ricevuta, viene accertata la disponibilità di marche. In caso positivo, il sistema restituisce, come risposta, la TimeStampResp (RFC3161) contenente il TimeStampToken (RFC3161) relativo all'HASH incluso nella TimeStampReq (RFC3161) fornita in fase di richiesta
Nel caso in cui il sistema TSA riceva una richiesta di temporale validazione temporale elettronica qualificata non conforme al requisito di cui sopra viene restituito un messaggio di errore.

Sintesi operativa dell'utente :

1. Avviare l'applicazione di firma e verifica
2. Selezionare la funzione di apposizione della VTEQ
3. Selezionare il file;
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 dell'apposizione della validazione temporale elettronica qualificata. Il contenuto del file potrà essere letto con programmi adeguati al formato del file stesso (esempio: i file in formato PDF saranno letti con Acrobat Reader).

La Time Stamping Authority Aruba PEC, a seguito della ricezione di una richiesta conforme al formato sopra descritto restituisce un messaggio contenente un TimeStampToken (RFC3161) codificato in DER, cosi come previsto dall'RFC 3161.

4.3.3 Sicurezza logica e fisica del sistema di validazione temporale elettronica qualificata

Gli elaboratori che offrono il servizio di VTEQ collocazione sono fisicamente protetti in modo da prevenire la possibilità di compromissioni fisiche grazie agli accorgimenti tecnici atti ad impedire accessi non autorizzati da persone e danneggiamenti da eventi accidentali.

4.3.3.1 Sicurezza fisica

Il sistema di validazione temporale elettronica qualificata 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 validazioni temporali elettroniche qualificate ed dei server di Back-end che si occupano della creazione delle validazioni temporali elettroniche qualificate e della gestione degli apparati di acquisizione e sincronizzazione del riferimento temporale.
I server del sistema di validazione temporale elettronica qualificata 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, condizionamento, etc) e gli elaboratori sono alimentati con linea elettrica preferenziale, sorretta da gruppo di continuità.

4.3.3.2 Sicurezza logica

I server di Front-end e di Back-end del sistema di validazione temporale elettronica qualificata 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 validazioni temporali elettroniche qualificate 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 e viene usato esclusivamente per il servizio di validazione temporale elettronica qualificata. 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. La coppia di chiavi e i corrispondenti certificati vengono sostituiti almeno ogni tre mesi.

4.4 Modalità operative per l'utilizzo del sistema di verifica delle validazioni temporali elettroniche qualificate

Aruba PEC ha qualificato, tramite una procedura interna di validazione del software, le applicazioni che fornisce alla propria clientela e che permettono la verifica delle validazioni temporali elettroniche qualificate 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 a cui è applicata la validazione temporale elettronica qualificata;
2. L'autenticità e l'affidabilità della validazione temporale elettronica qualificata;
3. La data ed ora in cui la validazione temporale elettronica qualificata è stata associata al documento informatico.

Sintesi operativa dell'utente:

1. Avviare l'applicazione di firma e verifica
2. Selezionare la funzione di verifica della VTEQ
3. Selezionare il file
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 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 validazioni temporali elettroniche qualificate forniti da Aruba PEC sono conformi a quanto indicato all'art. 42, commi 2 e 6 del DPCM ed ai requisiti di cui al paragrafo 5 della Determinazione n. 121/2019 [7].

L'utente deve tenere ben presente il fatto che alcuni formati di file consentono di inserire del codice eseguibile (macro o comandi) all'interno del documento informatico 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 sottoposti a validazioni temporali elettroniche qualificate non producono gli effetti di cui all'articolo 21, comma 2 del CAD [6].
È unicamente responsabilità dell'utente accertarsi, attraverso le funzionalità tipiche di ciascun prodotto, che tale condizione sia soddisfatta.

4.5 Disponibilità del servizio

Il servizio è reso disponibile 24 ore su 24, tutti i giorni della settimana festivi inclusi tramite protocollo secure HTTPS secondo i formati e le specifiche dettagliate nella RFC 3161.L'infrastruttura tecnologia, schematizzata nella figura a fianco, evidenzia come non vi siano Single Point Of Failure (SPOF) ed il sistema consenta di raggiungere un livello di servizio molto elevato.

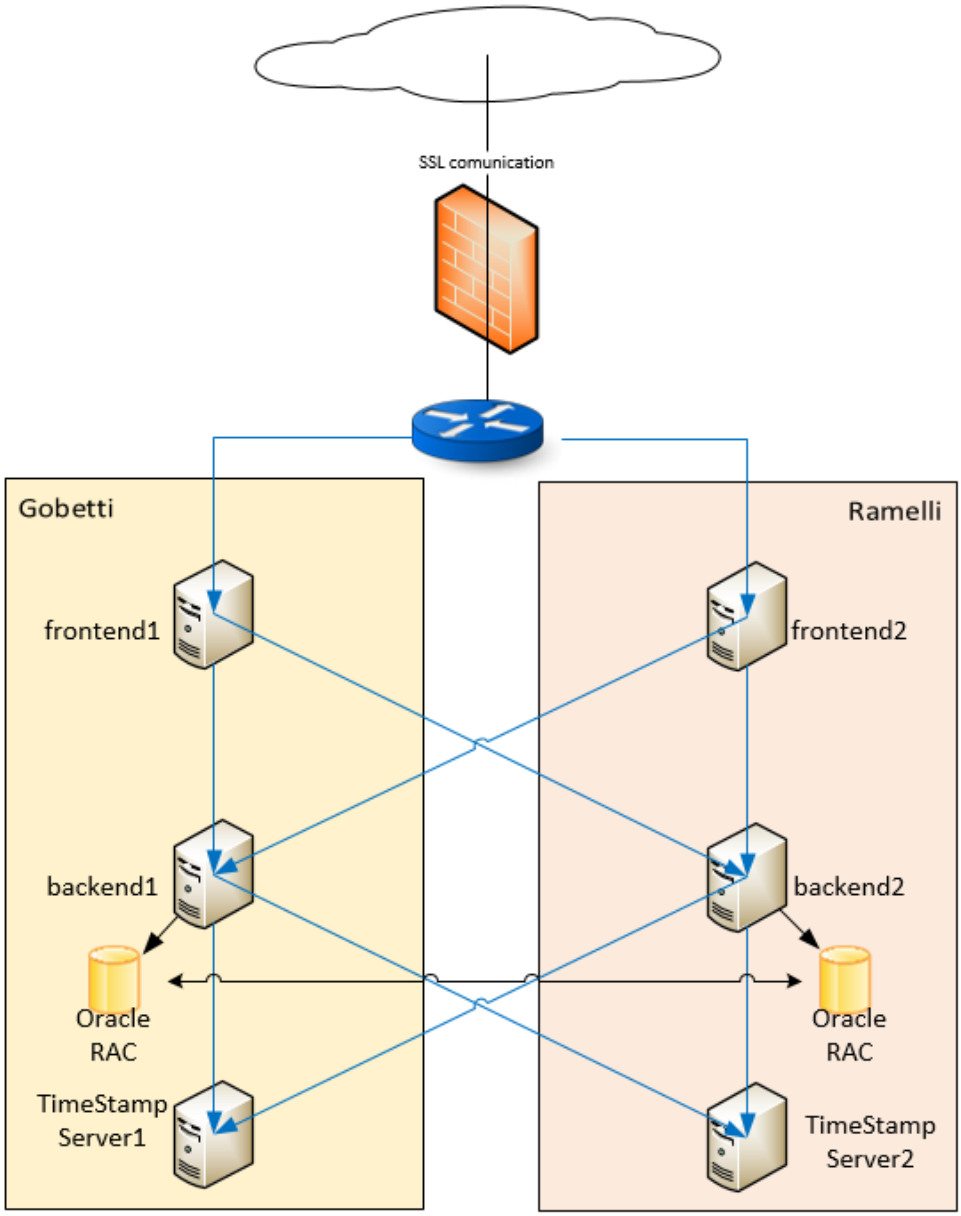

Figura 1 – schema infrastruttura

I server di frontend e back end facenti fanno parte di ambienti virtuali installati presso i due Data Center di Arezzo (IT1-IT2) sono predisposti in bilanciamento online/online in modo da svolgere il doppio compito di load balancing e business continuty in caso di guasto hardware o software.

Entrambi i front end sono in grado di interrogare i due back end che a loro volta sono in grado di interpellare entrambi i server che si occupano di apporre la Marca Temporale.

L'anagrafica che è presente nel database OracleRAC nei due datacenter permette di autenticare e tenere traccia delle richieste di marcatura.

I Time Stamp Server sono invece fisici in modo da poter ospitare al loro interno degli HSM PCI Thales Solo+ che sono stati scelti in quanto in grado di soddisfare circa 100 volte il carico atteso.

Questi HSM scelti hanno inoltre un Mean Time Between Failure (MTBF) dichiarato dal produttore di 1.105.978 ore.

4.6 Conservazione dei log

Aruba PEC conserva i log (registri elettronici) delle validazioni temporali emesse per 30 anni salvo accordo contrattuale specifico che ne stabilisca una durata diversa, comunque sempre uguale o superiore ai 20 anni previsti dalla normativa.

4.7 Piano di Cessazione della TSA

Di seguito si precisano le attività che saranno svolte qualora l'azienda decida, per qualsiasi ragione, di porre fine al servizio di marcatura temporale, ossia di cessare la propria attività di TSA.

Prima della effettiva cessazione:

- Almeno 60 giorni prima della data pianificata di cessazione del servizio, sarà inviata una informativa a tutti i clienti del servizio di TSA (o di altri servizi che includono i servizi di TSA), nonché al Supervisory Body nazionale e al Conformity Assessment Body.
- Sempre con preavviso di 60 giorni, sarà pubblicata in modo evidente una nota informativa anche sul sito web della TSA, al fine di rendere disponibile l'informazione anche alle Relying Parties.
- Sempre con preavviso di 60 giorni, la TSA invierà una comunicazione a tutti gli eventuali subappaltatori, informandoli che alla scadenza del termine non saranno più autorizzati ad eseguire attività collegate al processo di emissione di marche temporali.
- La responsabilità della conservazione delle evidenze (marche temporali, giornale di controllo, ecc.) sarà trasferita contrattualmente ad un altro soggetto affidabile che ne possa garantire la conservazione per un tempo pari ad almeno 20 anni. Sarà inoltre trasferita a tale soggetto la responsabilità di pubblicare sul proprio sito la chiave pubblica della TSA cessata nonché il mantenimento della URL della CRL.
- Si pianificherà la distruzione delle chiavi private di marcatura temporale nonché del materiale crittografico annesso (se presente) che ne consente il ripristino.

Alla data di cessazione:

- Saranno distrutte (per cancellazione logica) le chiavi private di marcatura temporale nonché il materiale crittografico annesso (se presente) che ne consente il ripristino, verbalizzando l'operazione.
- Saranno revocati i certificati di tutte le TSU facenti capo alla TSA cessata.

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 Obblighi degli Utenti

L'utente che, ai soli fini di verifica delle validazioni temporali elettroniche qualificate ha i seguenti obblighi:

- Conoscere l'ambito di utilizzo, e le eventuali limitazioni allo stesso, delle validazioni temporali elettroniche qualificate; le limitazioni di responsabilità e i limiti di indennizzo del Certificatore, riportati nel Manuale Operativo del Certificatore stesso;
- Verificare la validità del documento informatico a cui è associata una validazione temporale elettronica qualificata;
- Verificare i dati presenti nella validazione temporale elettronica qualificata ed, in particolare, che corrispondano ai dati previsti nel presente Manuale Operativo. Verificare che la validazione temporale elettronica qualificata sia correttamente sottoscritta dal prestatore di servizi fiduciari e che la chiave privata utilizzata per tale sottoscrizione non sia stata compromessa prima del momento dell'apposizione del riferimento temporale;
- Adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- Conoscere e rispettare tutte quante le misure precauzionali previste nel presente Manuale Operativo e negli altri eventuali accordi intercorsi con il prestatore di servizi fiduciari, ivi comprese le limitazioni di responsabilità ed i limiti di indennizzo.

5.2 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.

5.3 Interpretazione

Salvo disposizioni diverse, questo Manuale Operativo dovrà essere interpretato in conformità alla correttezza, buona fede ed a quanto ragionevole anche in virtù della legislazione italiana ed europea ad esso applicabile e degli usi commerciali internazionali.

5.4 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.

5.5 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.

5.6 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.

5.7 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.

5.8 Violazioni e altri danni materiali

Gli utenti del servizio oggetto del presente manuale rappresentano e garantiscono che la loro presentazione al TSP qualificato (Aruba PEC) e l'utilizzo delle informazioni relative alla richiesta del servizio di validazione temporale elettronica qualificata 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 servizio 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.
Gli utenti del servizio oggetto del presente manuale si obbligano a manlevare e indennizzare il TSP qualificato (Aruba PEC) contro qualunque perdita o danno derivanti da una tale interferenza o infrazione.

5.9 Norme Applicabili

I servizi fiduciari qualificati oggetto del presente Manuale Operativo sono disciplinati dalle norme giuridiche dell'ordinamento Italiano e dell'Unione Europea.
Il fine è garantire uniformità di trattamento e mutuo riconoscimento all'interno dell'ordinamento Comunitario.

5.10 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, con esclusione di qualsiasi altro foro competente e con esclusione delle ipotesi in cui la legge preveda la competenza del foro del consumatore.

(FINE DOCUMENTO)