STATO MAGGIORE DELLA DIFESA

Comando per le Operazione in Rete

FIRMA AUTOMATICA SMD/COR
Servizio di Firma Automatica e Sigillo Elettronico del Ministero della Difesa

Appendice SMD/COR
Firma Automatica e Sigillo v.1.3

al
MANUALE OPERATIVO
Public Key Infrastructure – PKI
Firma Digitale – Autenticazione CNS – Time Stamping Authority

VERSIONE DOCUMENTO	**1.3**

Compilato da: **RESPONS. CONDUZ. TECNICA DEI SISTEMI** **Serg. Marco D'AGOSTINO**	*Firmato Digitalmente da/Signed by:* MARCO D'AGOSTINO *In Data/On Date:* martedì 8 luglio 2025 08:19:30
Revisionato da: **RESP. SERVIZIO CERTIFICAZIONE E VALIDAZIONE TEMPORALE** **Col. Angelo MARIANI**	*Firmato Digitalmente da/Signed by:* ANGELO MARIANI Capo Centro di Certificazione *In Data/On Date:* martedì 8 luglio 2025 13:42:50
Approvato da: **CERTIFICATORE** **Gen. D. Sandro SANASI**	*Firmato Digitalmente da/Signed by:* SANDRO SANASI *In Data/On Date:* martedì 8 luglio 2025 16:33:10

Sommario delle modifiche

Versione Appendice	Sezione	Descrizione	Data
1.0	//	Prima emissione.	22/11/2021
1.1	Tutte	Cambio Approvatore	13/01/2022
1.2	Tutte	Cambio Gruppo di Certificazione Cambio Certificatore	24/03/2025
1.3	Tutte	Cambio Gruppo di Certificazione	30/06/2025

I N D I C E

PARTE 1^

NORME GENERALI

1 PREMESSA

Il presente Manuale definisce le procedure, di Firma Digitale Automatica e Sigillo Elettronico Qualificato, applicate dal **Comando per le Operazioni in Rete (Prestatore di Servizi Fiduciari Qualificati)** e relative al servizio di Firma Automatica e Sigillo Elettronico implementato all'interno della Rete Difesa (Difenet) per tutti gli utenti in possesso di un certificato di Firma Automatica e/o Sigillo Elettronico Qualificato.

Il documento, inoltre, descrive l'organizzazione messa in atto dal Prestatore di Servizi Fiduciari Qualificati, nell'esercizio delle sue funzioni ed evidenzia i processi necessari per la generazione, la pubblicazione, la sospensione e la revoca dei certificati e sigilli.

Il presente Manuale è da considerarsi INTEGRATIVO al Manuale Operativo "PKI di Firma Qualificata" edito dal Certificatore e pubblicato sul sito dell'Agenzia per l'Italia Digitale.

2 GENERALITA'

2.1 Scopo del documento

Il Manuale Operativo illustra le procedure, le regole ed i criteri di tipo tecnico, organizzativo e operativo tramite i quali il Ministero della Difesa, nella figura dello Stato Maggiore della Difesa – Comando per le Operazioni in Rete (Prestatore di Servizi Fiduciari Qualificati), certifica il servizio di *Firma Automatica e Sigillo Elettronico Qualificato* implementato presso il Comando per le Operazioni in Rete e utilizzato dagli utenti abilitati appartenenti al Dicastero della Difesa e dai Ministeri, Enti/P.A. che hanno sottoscritto un accordo di collaborazione.

2.2 Riferimenti alle norme di legge:

[DPR445] 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.

[DPCM2009] 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 n.129 del 6 giugno 2009.

[eIDAS] Regolamento (UE) del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari nelle transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.

[GDPR] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016.

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

[DLGS82] Decreto Legislativo 7 marzo 2005, n. 82: "Codice dell'amministrazione digitale", pubblicato nella Gazzetta Ufficiale. n. 112 del 16 maggio 2005.

[DLGS159] 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.

[AGID121/19] Determinazione AGID 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", Pubblicato nella Gazzetta Ufficiale (serie generale) n.130 del 05-06-2019.

[DPCM2013] 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 n. 117 del 21 maggio 2013.

[AGID63/14] Determinazione Commissariale n.63/2014. Modalità di attuazione dell'articolo 19, comma 7, del DPCM 22 febbraio 2013 recante "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.".

[eIDAS2] Regolamento (EU) N. 1183/2024 del Parlamento Europeo e del Consiglio del 11 Aprile 2024 che modifica il Regolamento (EU) N. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

2.3 Riferimenti agli standard

[LDAP3] Wahl, M., Kille, S. and T. Howes, "Lightweight Directory Access Protocol (v3)", RFC 2251, December 1997.

[PKCS1] B. Kaliski, "PKCS#1: RSA Encryption - Version 1.5", Internet RFC 2313, March 1998.

[PKCS10] B. Kaliski, "PKCS#10: Certification Request Syntax - Version 1.5", Internet RFC 2314, March 1998.

[SHA1] ISO/IEC 10118-3:1998, "Information technology - Security techniques - Hashfunctions - Part 3: Dedicated hash-functions", May 1998.

[SHA2] ISO/IEC 10118-3:2004, "Information technology - Security techniques - Hashfunctions - Part 3: Dedicated hash-functions", February 2004.

[X500] ITU-T Recommendation X.500 (1997 E), "Information Technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services", August 1997.

[X509] ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

[RFC 3161] Adams, C., Cain, P., Pinkas, D. and Zuccherato, R., "Time-Stamp Protocol (TSP)", RFC 3161, August 2001.

[RFC 5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[ETSI 280] ETSI TS 102 280 v 1.1.1 – "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons", March 2004.

[ETSI 862] ETSI TS 101 862 v.1.3.2 – "Qualified Certificate profile", June 2004.

2.4 Glossario

Vedasi il para 1.4 del **"Manuale Operativo – PKI di Firma Qualificata" v. 6.8 - OID (1.3.6.1.4.1.14031.1.2.1)**

3 INTRODUZIONE

3.1 Dati identificativi del Prestatore di Servizi Fiduciari Qualificati

Il presente Manuale costituisce l'Appendice COR v.1.1 del Manuale Operativo del Prestatore di Servizi Fiduciari Qualificato (Stato Maggiore Difesa - Comando per le Operazioni in Rete), per le procedure di **Firma Automatica e Sigillo Elettronico Qualificato** implementate dallo stesso Prestatore di Servizi Fiduciari Qualificati presso il Comando per le Operazioni in Rete e fruibili da

tutti gli utenti del Dicastero Difesa e dai Ministeri, Enti, P.A. abilitati a tale tipologia di servizio. Per Titolare si intende, nel caso di Firma Automatica la *persona fisica*, nel caso del Sigillo Elettronico Qualificato invece si intende la *persona giuridica* dell'entità rappresentata.

Il soggetto giuridico responsabile nei confronti degli utenti del servizio di certificazione è individuato nel:

STATO MAGGIORE DELLA DIFESA

Comando per le Operazione in Rete
Via Stresa, 31/B 00135 ROMA

Il Centro di Certificazione, deputato alla gestione dell'infrastruttura tecnologica (PKI) ed alla condotta operativa del servizio di certificazione, è ubicato presso:

STATO MAGGIORE DELLA DIFESA

Comando per le Operazione in Rete

Centro di Certificazione

Servizio Conservazione e Identità Digitale

Via Stresa, 31/B 00135 ROMA

Il Centro di certificazione mette a disposizione per i servizi offerti e per l'assistenza utenti i seguenti punti di contatto:

- Indirizzo e-mail: **info_pkiff@smd.difesa.it ;**
- Indirizzo ldap per l'accesso al registro dei certificati: **ldap://ldappkiff.difesa.it**
- Indirizzo web per l'accesso al registro delle crl: **http://www.pki.difesa.it**
- Sito web: **https://pki.difesa.it/tsp**

3.2 Versione del manuale operativo

La versione della presente Appendice al Manuale Operativo è identificata dalla sigla:

Appendice SMD/COR Vers.1.1 al Manuale Operativo Vers. 6.8 - OID: 1.3.6.1.4.1.14031.1.2.1

Il presente documento è pubblicato sul sito web del Centro di Certificazione Difesa https://pki.difesa.it/tsp ed è quindi consultabile telematicamente ai sensi dell'art. 40, comma 2, delle regole tecniche.

Come versione corrente del Manuale Operativo si intenderà esclusivamente la versione in formato elettronico disponibile sul sito web del servizio di certificazione https://pki.difesa.it/tsp oppure quella pubblicata sul sito web di AGID. (Agenzia per l'Italia Digitale - www.agid.gov.it).
In caso di discordanza, farà fede la versione pubblicata sul sito web dell'Agenzia.
Il documento viene inoltre pubblicato in formato **PAdES**, in modo da garantirne l'origine e l'integrità.

3.3 Responsabile del manuale operativo

Il responsabile del presente Manuale Operativo è lo Stato Maggiore della Difesa - Comando per le Operazioni in Rete, nella persona del Comandante che si avvale del Capo del Centro di Certificazione.

4 DISPOSIZIONI GENERALI

4.1 Obblighi della Certification Authority

Il Comando per le Operazioni in Rete, in funzione di Prestatore di Servizi Fiduciari Qualificati, espleta tutte le attività di emissione, pubblicazione, sospensione e revoca dei Certificati Qualificati per la firma digitale automatica e sigillo elettronico.

Nello svolgimento dell'attività il Certificatore, per il tramite del Centro di Certificazione:

1. adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
2. assicura che il dispositivo sicuro per la generazione delle firme (HSM) abbia le caratteristiche ed i requisiti di sicurezza previsti dalle regole tecniche;
3. informa i titolari di certificato e sigillo sulla procedura di certificazione, sui requisiti tecnici necessari per accedervi, sulle caratteristiche e limitazioni d'uso delle firme emesse;
4. comunica all'AGID ed ai titolari dei certificati e sigilli, con un preavviso di almeno sessanta giorni, la cessazione dell'attività, la conseguente rilevazione della documentazione da parte di altro Prestatore di Servizi Fiduciari Qualificati o il suo annullamento;
5. si attiene alle misure minime di sicurezza per il trattamento dei dati personali (GDPR 679/2016);
6. conserva le richieste di registrazione e di certificazione per un periodo di 20 anni dalla data di scadenza del certificato emesso.

Nello svolgimento dell'attività di certificazione, il Prestatore di Servizi Fiduciari Qualificati deve:

1. generare le coppie di chiavi di firma dei Titolari all'interno dei dispositivi di firma;
2. non rendersi depositario di chiavi private di firma dei Titolari;

3. generare la coppia di chiavi asimmetriche mediante apparati e procedure che assicurino, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata;
4. verificare, prima di emettere il certificato, l'effettiva esistenza della coppia di chiavi privata e pubblica e verificare, nei limiti concessi dall'attuale tecnologia, il corretto funzionamento della coppia di chiavi;
5. comunicare per iscritto ad AGID ogni variazione significativa delle soluzioni tecnico/organizzative da adottare;
6. comunicare tempestivamente ad AGID ogni variazione significativa delle soluzioni tecnico/organizzative adottate;
7. procedere tempestivamente alla sospensione e/o alla revoca del certificato e/o sigillo in caso di richiesta espressamente formulata da parte del Titolare o da parte della Registration Authority;
8. dare immediata pubblicazione della revoca e della sospensione dei certificati.

4.2 Registration Authority

Tutti i compiti, le funzioni e le attribuzioni di Registration Authority, riportati nel Manuale Operativo Vers. 6.6 OID: 1.3.6.1.4.1.14031.1.2.1, vengono svolti dalla stessa Certification Authority.

4.2.1 Obblighi del Titolare del certificato di Firma Automatica/Sigillo

Il Titolare del Certificato/Sigillo deve:

1. fornire, alla Registration Authority, tutte le informazioni necessarie garantendone, sotto la propria responsabilità, l'attendibilità ai sensi della legge n. 15 del 1968 e successive modifiche ed integrazioni;
2. conservare e proteggere, con la massima diligenza, le credenziali di accesso alla firma e gli eventuali devices a corredo;
3. sporgere denuncia, in caso di smarrimento o sottrazione delle credenziali di accesso alla firma, alle Autorità di Polizia Giudiziaria;
4. procedere all'immediata comunicazione alla Registration Authority della necessità di sospendere/revocare il proprio certificato/sigillo, qualora si verifichino le circostanze quali furto o smarrimento, che comportino la compromissione della sicurezza della chiave privata.
5. redigere per iscritto le richieste di revoca e/o sospensione specificando le motivazioni e la prevista decorrenza;

4.3 Aspetti normativi e legislativi

L'organizzazione e l'erogazione del servizio di certificazione sono sottoposte alla legislazione italiana ed europea, nonché alle eventuali norme attuative emanate in ambito Ministero Difesa e Stato Maggiore Difesa.

4.4 Normativa in vigore

Il presente Manuale fa riferimento ed è conforme alle regole previste dalla normativa vigente in ambito nazionale e comunitario in materia di "firma digitale", come riportato al para 2.2.

4.5 Avvisi

Il sistema di Firma Automatica / Sigillo assolve già le funzioni di "Firma Verificata" disposte dall'Agenzia per l'Italia Digitale con la Determinazione Commissariale n. 63/2014.

All'interno del Certificato di Firma Automatica e Sigillo Elettronico è presente la codifica

dei seguenti elementi:

a. PolicyIdentifier object identifier (OID) 1.3.76.16.3;

b. i seguenti userNotice di tipo explicitText:

- *The Qualified Certification Service Provider that issued this certificate ensures that the signatures based on this certificate have been generated during the period of validity of the certificate.*

- *Il Prestatore di Servizi Fiduciari Qualificati garantisce che le firme basate su questo certificato qualificato sono valide in quanto il certificato ad esse associato era valido al momento della generazione delle firme.*

- *Il presente certificato è valido solo per firme apposte con procedura automatica. The certificate may only be used for unattended/automatic digital signature.*

Il Prestatore di Servizi Fiduciari Qualificati si riserva di pubblicare sul proprio sito, all'indirizzo https://pki.difesa.it/tsp i riferimenti di legge e, nella misura concessa dalle norme sul *copyright*, i relativi testi più significativi nonché di apportare le modifiche che si rendessero necessarie al presente Manuale, previa approvazione da parte dell'Ag.ID..

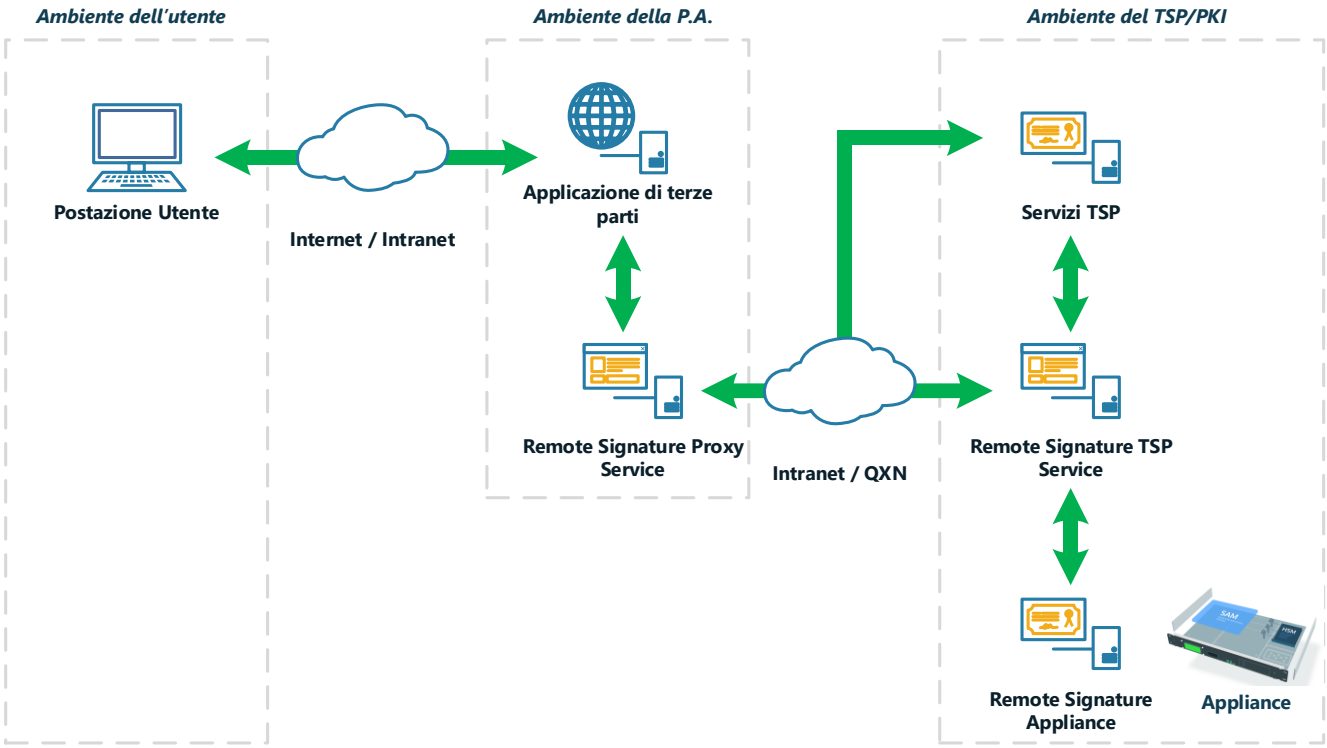
PARTE 2^

ASPETTI OPERATIVI

1 Descrizione del sistema

1.1 Componenti

Il sistema offerto dal TSP per erogare i servizi di Firma Automatica e Sigillo Elettronico Qualificato, con chiavi private e certificati ospitati su apparati presso il TSP stesso, è rappresentato nell'immagine seguente:

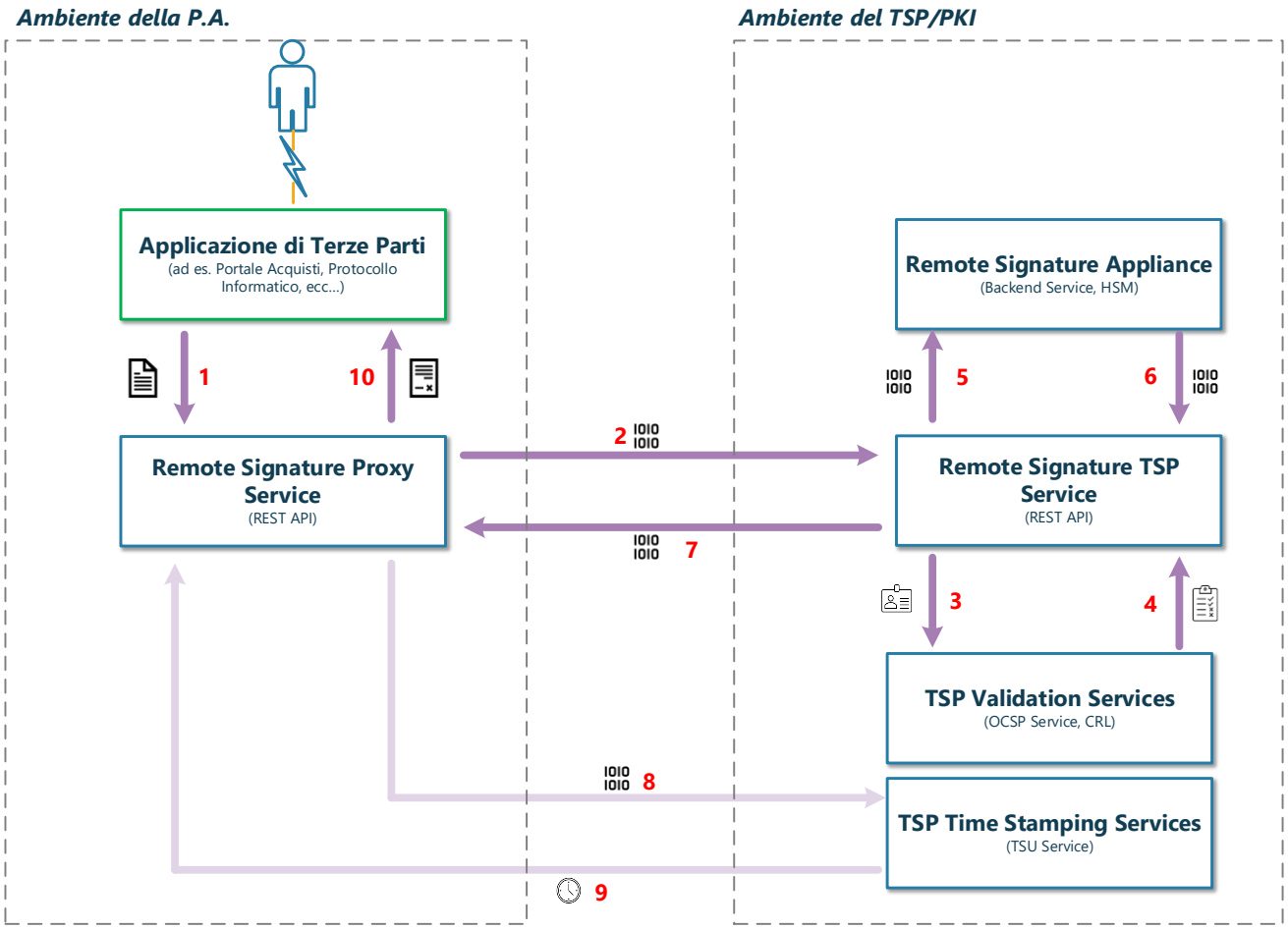


Si identificano tre ambienti operativi:

- L'ambiente tecnico dell'Ente/P.A. (Pubblica Amministrazione) che ospita l'applicazione al cui interno sono integrati i servizi di firma/sigillo (solitamente un portale web o un sistema di back-end) e una particolare componente chiamata Remote Signature Proxy Service.
- L'ambiente del TSP/PKI stesso che ospita apparati e servizi accreditati secondo il regolamento eIDAS (CA di Firma Digitale, servizio di Marcatura Temporale, apparati HSM di firma e sigillo, software di back-end Remote Signature TSP Service).
- L'ambiente dell'utente, che solitamente corrisponde alla propria postazione di lavoro con cui si collega al sistema/portale della P.A.

L'operazione di firma/sigillo dei documenti avviene utilizzando due componenti software: **Remote Signature Proxy Service**, presente nell'ambiente tecnico della P.A., si occupa di eseguire operazioni di imbustamento, calcolo degli hash da firmare e completamento delle buste crittografiche. **Remote Signature TSP Service**, presente nell'ambiente tecnico del TSP, si occupa di ricevere richieste di firma/sigillo di hash anonimi ed eseguire l'operazione tramite le chiavi private e certificati immagazzinati su appositi Appliance HSM certificati/accreditati a tale scopo. In questo modo i documenti degli Enti/P.A. non escono mai dall'ambiente dell'Ente/P.A. stesso; il tutto porta così a benefici sia in termini di privacy che di prestazioni, in quanto i documenti non vengono mai inviati al TSP nella loro forma completa, bensì solo hash anonimi e di piccole dimensioni. L'**Applicazione di Terze Parti** della P.A. (sistema/portale), comunica quindi solo con il Remote Signature Proxy Service per firmare/sigillare i documenti.

Con le componenti indicate, di seguito il processo di firma/sigillo:



1. L'Applicazione della P.A. invia a Remote Signature Proxy Service una richiesta indicante il/i documento/i da firmare/sigillare, le caratteristiche della firma da produrre (formato busta, aspetto grafico, profilo di firma, altre caratteristiche tecniche) e le credenziali dell'utenza di firma/sigillo.
2. Remote Signature Proxy Service crea una versione preliminare della busta crittografica, calcola gli hash che devono essere effettivamente firmati/sigillati con la chiave privata e invia tale lista di hash al Remote Signature TSP Service tramite la rete Intranet/QXN.
3. Remote Signature TSP Service riceve la richiesta e controlla lo stato di validità del certificato utente (stato di revoca, validità nel tempo).
4. Tramite i sistemi TSP Validation Services (OCSP o CRL), viene recuperato lo stato di validità del certificato.
5. Nel caso il certificato sia valido e non revocato/sospeso, il Remote Signature TSP Service demanda al Remote Signature Appliance la firma degli hash sbloccando l'operazione tramite le credenziali utente fornite.

6. Il Remote Signature TSP Service ottiene le firme corrispondenti e le restituisce al Remote Signature Proxy Service.
7. Il Remote Signature Proxy Service riceve le firme e procede con il completamento dell'imbustamento.
8. Eventualmente, se richiesto, Remote Signature Proxy Service chiede una marcatura temporale ai TSP Time Stamping Services del TSP stesso.
9. Il Remote Signature TSP Service riceve la marcatura temporale e la allega alla busta crittografica.
10. Infine, Remote Signature TSP Service ritorna il documento firmato secondo la busta crittografica richiesta all'Applicazione della P.A. che potrà procedere con i propri processi interni

1.2 Descrizione delle funzioni

Di seguito la descrizione della richiesta da parte del titolare, della creazione Utente, la generazione del certificato di Firma Automatica e Sigillo Elettronico, e l'invio delle credenziali al titolare

FASE 1 – Richiesta da parte del Titolare

Il titolare del certificato e/o sigillo compila un modulo preformattato PDF con all'interno i dati relativi alla richiesta e le informazioni che saranno incluse nel certificato (ad es. Cognome, Nome, Codice Fiscale per la Firma Automatica, mentre per il Sigillo nome descrittivo, organizzazione, codice AOO, ecc.). Il titolare firma digitalmente il modulo PDF appena compilato con il proprio Modello ATe (il certificato di firma digitale è stato emesso dal medesimo TSP) in formato PAdES e lo invia al TSP.

FASE 2 – Analisi della richiesta

L'operatore del TSP, ricevuto il modulo con l'ausilio di strumenti informatici, verifica il modulo ricevuto in termini di:

- Validità della firma digitale del modulo;
- Presenza dei dati obbligatori al suo interno;
- Correttezza dei dati al suo interno rispetto a quelli relativi all'identità del certificato di firma e dell'utente stesso (ad es. corrispondenza con l'atto di nomina, email istituzionale, ecc...).

FASE 2 – Generazione del certificato - Enrollment

Il sistema in automatico:

- Crea l'utenza sull'appliance di firma (HSM) generando dei segreti in modo univoco per ogni utente all'interno del sistema (password e PIN dispositivo nel caso di firma automatica).

- Avvia la generazione della chiave privata sull'appliance (HSM).
- Ottiene la richiesta di certificato (CSR) firmata con la chiave appena generata.
- Sottopone la richiesta alla Certification Authority di firma ottenendo come risposta il relativo certificato utente
- Scrive il certificato così ottenuto sull'appliance (HSM).

In caso di successo quindi, il sistema crea una busta cieca digitale PDF contenente i segreti e cifra tale busta (in formato PKCS#7 Enveloped Data) utilizzando come certificato destinatario quello corrispondente all'utente che ha firmato il modulo di richiesta (il certificato viene recuperato in automatico dalla directory LDAP del TSP).

Infine, il sistema invia una email al titolare/utente con la comunicazione dell'emissione del servizio e allegata la busta cieca digitale cifrata. In questo modo solo l'utente che ha richiesto il certificato/sigillo può visualizzare i contenuti della busta dopo averla decifrata tramite il proprio Modello ATe e uno strumento quale il Kit di Firma. Il certificato di cifra/decifra del Modello ATe è protetto ovviamente dal PIN Carta di cui solo il titolare è a conoscenza.

FASE 3 – Utilizzo del certificato

L'utente titolare del certificato di Firma Automatica o Sigillo Elettronico utilizza il sistema/portale dell'Ente/P.A. su cui esegue le proprie attività, dopo essersi opportunamente autenticato secondo le policy del sistema/portale suddetto.

Nel momento in cui il processo operativo del sistema/portale richiede l'apposizione della firma o del sigillo in modalità automatica/massiva, l'utente inserisce le proprie credenziali e avvia il processo.

Il sistema/portale richiede al Remote Signature Proxy Service di eseguire l'operazione su uno o più documenti/hash, fornendo i parametri riguardanti la busta crittografica e le credenziali dell'utenza di firma automatica o sigillo elettronico. Si avvia quindi il processo di firma/sigillo con i dettagli tecnici indicati nella sezione precedente. Al termine del processo, il sistema/portale avrà firmato/sigillato tutti i documenti e potrà procedere secondo le fasi del proprio processo interno.

1.3 Sicurezza fisica

L'apparato di firma digitale Automatica e Sigillo (HSM ARX CoSign) è situato all'interno di armadi RITTEL della Public Key Infrastructure (PKI) del Centro Elaborazione Dati del Comando per le Operazioni in Rete ed è soggetto alle medesime misure di sicurezza fisica implementate per l'infrastruttura PKI ed esplicitate nel "Piano della Sicurezza", depositato presso l'Agenzia per l'Italia Digitale (AGID).

1.4 Sicurezza logica

L'infrastruttura di Firma Automatica e Sigillo Elettronico Qualificato è parte integrante dell'infrastruttura PKI del Prestatore di Servizi Fiduciari Qualificati. È soggetta, pertanto, alle medesime regole di sicurezza logica implementate per la PKI ed esplicitate nel "Piano della Sicurezza", depositato presso l'Agenzia per l'Italia Digitale (AgID).

Il servizio di firma Automatica e Sigillo è raggiungibile unicamente da sistemi/portali di back-end abilitati verso la rete Difesa (Difenet).

Le credenziali di accesso all'HSM sono conosciute esclusivamente dall'utente titolare del certificato associato alle chiavi private.

L'autenticazione tra l'Applicazione degli Enti/P.A. ed il servizio Remote Signature Proxy Service avviene esclusivamente tramite HTTPS a mutua autenticazione sulla rete interna dell'Ente/P.A.: ogni Applicazione della P.A., infatti, è dotata di un certificato X.509 web client con il quale si autentica sul Proxy. Il Remote Signature Proxy Service accetta quindi chiamate esclusivamente da certificati abilitati al servizio. L'autenticazione tra i vari Remote Signature Proxy Service e il Remote Signature TSP Service avviene esclusivamente tramite HTTPS a mutua autenticazione sulla rete Intranet/QXN: ogni Remote Signature Proxy Service, infatti, è dotato di un certificato X.509 web client con il quale si autentica sul Remote Signature TSP Service. Il Remote Signature TSP Service accetta quindi chiamate esclusivamente da certificati di Proxy abilitati al servizio.

2 Guida per gli utenti del servizio di firma automatica sigillo

Il processo di richiesta di abilitazione alla firma remota (automatica e/o sigillo) prevede le sottonotate azioni:

1. ***Richiesta***: il titolare richiede l'emissione di un certificato di firma automatica/sigillo a suo nome. Il richiedente compila il modulo di richiesta validandolo con la propria firma digitale e lo invia all'indirizzo: info_pkiff@smd.difesa.it
2. ***Autorizzazione***: i dati della richiesta vengono validati dal Centro di Certificazione Difesa, viene creato l'utente e attraverso l'automatismo del sistema viene creato il Certificato e/o Sigillo Elettronico nonché la busta cieca cifrata con i codici del certificato.
3. **Invio:** l'operatore del TSP invia la busta cieca cifrata al titolare con le istruzioni per l'uso del servizio.

3 Procedura di revoca dei certificati di Firma Remota

Le procedure per la revoca di un Certificato di Firma Remota, su iniziativa del Prestatore di Servizi Fiduciari Qualificati, su richiesta da parte del titolare oppure su richiesta da parte di un terzo interessato, seguono le medesime procedure previste per la revoca di un certificato di Firma Digitale - Dpcm 22 febbraio 2013 - e sono riportate all'interno del Cap. 5 del Manuale Operativo della PKI v.6.1.