STATO MAGGIORE DELLA DIFESA

Comando per le Operazione in Rete

FIRMA REMOTA SMD/COR

Servizio di Firma Remota del Ministero della Difesa

Appendice SMD/COR v.1.5

al

MANUALE OPERATIVO

Public Key Infrastructure - PKI

Firma Digitale – Autenticazione CNS – Time Stamping Authority

approvato da: **Gen. D.**

Sandro SANASI

Comandante del CORDIFESA

VERSIONE DOCUMENTO	**1.5**

Compilato da: **Serg. Marco D'AGOSTINO**	*Firmato Digitalmente da/Signed by:* MARCO D'AGOSTINO *In Data/On Date:* martedì 8 luglio 2025 08:20:40
Revisionato da: **Col. Angelo MARIANI**	*Firmato Digitalmente da/Signed by:* ANGELO MARIANI Capo Centro di Certificazione *In Data/On Date:* martedì 8 luglio 2025 13:44:44
Approvato da: **Gen. Div. Aaran Sandro SANASI**	*Firmato Digitalmente da/Signed by:* SANDRO SANASI *In Data/On Date:* martedì 8 luglio 2025 16:33:44

Sommario delle modifiche

Versione Appendice	Sezione	Descrizione	Data
1.0	//	Prima emissione.	20/03/2015
1.1	Tutte	Adozione Reg.(UE) 910/2014	23/05/2018
1.2	Tutte	Sostituzione: [DLGS196] con [GDPR] Approvatore	09/03/2020
1.3	Tutte	Cambio Revisore	01/02/2021
1.4	Tutte	Cambio Approvatore	13/01/2022
1.5	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 Remota, applicate dal **Comando per le Operazioni in Rete (Prestatore di Servizi Fiduciari Qualificati)** e relative al servizio di Firma Remota implementato all'interno della Rete Difesa (Difenet) per tutti gli utenti dotati di accesso al sistema di virtualizzazione Citryx a mezzo OTP RSA.

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.

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 Remota* implementato presso il Comando per le Operazioni in Rete e utilizzato dagli utenti abilitati appartenenti al Dicastero della Difesa.

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.

[REG 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.".

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. 6.4 - 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.1.3 del Manuale Operativo del Prestatore di Servizi Fiduciari Qualificato (Stato Maggiore Difesa - Comando per le Operazioni in Rete), per le

procedure di Firma Remota 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 abilitati a tale tipologia di servizio.

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 clienti i seguenti punti di contatto:

- Indirizzo e-mail: **info_pkiff@smd.difesa.it ; firmaremota@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**
- Sito web (intranet): **https://portalecor.difesa.it/ViceComandante/RepSicurCyberDef/uis/spki/Pagine/FirmaRemota.aspx**

3.2 Versione del manuale operativo

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

Appendice SMD/COR Vers.1.3 al Manuale Operativo Vers. 6.4 - 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 Ag.ID. (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 remota.

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 sulla procedura di certificazione, sui requisiti tecnici necessari per accedervi, sulle caratteristiche e limitazioni d'uso delle firme emesse;
4. comunica all'Ag.ID. ed ai titolari dei certificati, 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 (DPR 318/99) emanate ai sensi dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675 e successive modificazioni e integrazioni;
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 Ag.ID ogni variazione significativa delle soluzioni tecnico/organizzative da adottare;
6. comunicare tempestivamente ad Ag.ID ogni variazione significativa delle soluzioni tecnico/organizzative adottate;
7. procedere tempestivamente alla sospensione e/o alla revoca del certificato 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. 5.0 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

Il Titolare del Certificato 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, 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 Remota 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 Remota 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 firm.e*

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 di Firma Remota è costituito dalle seguenti componenti (fig.1) :

- **Appliance HSM Cosign** di ARX con firmware v. 8.2 (OCSI Certified).
- **Server Portale Firma Remota** *Atos.RADS.WebInterface – Portale dell'Utente di Firma Remota.*
  Utilizza CoSign Firma Remota per eseguire le operazioni di firma e Atos.PKI.SL per eseguire le operazioni sul sistema.
- **Server Interno** ✓✓ *Atos.PKI.WebInterface – Portale Amministrazione Creazione utenti.*
  Utilizza Atos.PKI.SL per eseguire le operazioni sul sistema.
  ✓✓ *Atos.RADS.WsInterface – XML Web Service di Firma Remota.*
  Utilizza Atos.PKI.SL per ottenere le informazioni sui chiamanti e CoSign Firma Remota per eseguire le operazioni di firma.
  ✓✓ *Atos.PKI.SL – Application Logic Firma Remota*.

Richiama la RA (Atos.UCAI- web della PKI) per emettere certificati e cambiare il loro stato e CoSign Firma Remota per eseguire le operazioni sugli utenti (creazione utenti, cancellazione utenti, attivazione, generazione CSR, ecc…

- **Strong Authentication** *RSA SecurID Service*.

1.2 Descrizione delle funzioni

Come descritto nella figura 1 si sviluppano le seguenti fasi:

FASE 1 – Creazione dell'utente

L'amministratore si connette al portale di amministrazione per inserire l'utente che ha fatto richiesta di abilitazione al servizio di firma remota e/o associarlo ad un sistema esterno (protocollo, documentale,..)

FASE 2 – Generazione del certificato - Enrollment

L'utente utilizzando le credenziali di dominio si connette al portale di firma remota (http://firmaremota.servizi.difesa.it).

Alla prima connessione gli verrà richiesto di cambiare la password digitando la nuova password ed il codice OTP RSA.

Dopo aver cambiato la password il sistema chiede all'utente di avviare la procedura per la generazione del proprio certificato.

La generazione del certificato comporta l'inserimento della password (precedentemente scelta) e del codice OTP.

Il portale di firma remota contatta l'Application Logic di firma remota (CoSign Server) per la verifica delle credenziali dell'utente (username/password).

Per la verifica del valore del OTP RSA l'Application Logic contatta il Server Radius.

Verificate tutte le credenziali, l'Application Logic genera un token e lo invia, insieme alla username e alla password dell'utente, al HSM CoSign.

HSM CoSign confronta le credenziali dell'utente con il database utenti locali ed il valore del token con quello presente sul server radius al suo interno.

Verificate positivamente le credenziali, HSM CoSign genera la coppia di chiavi da associare all'utente e con queste firma il PKCS10 (richiesta di certificato) che invia all'Application Logic.

L'Applicatin Logic comunica il PKCS10 ricevuto alla R.A. di Front-End della PKI di Firma Digitale che, per il tramite della R.A. di Back-End, passa la richiesta alla CA di Firma Digitale, la quale genera il certificato firmandolo con la propria chiave privata presente sul HSM PKI.

Il certificato, seguendo i passaggi inversi, viene restituito e scritto all'interno del HSM.

FASE 3 – Firma di un documento

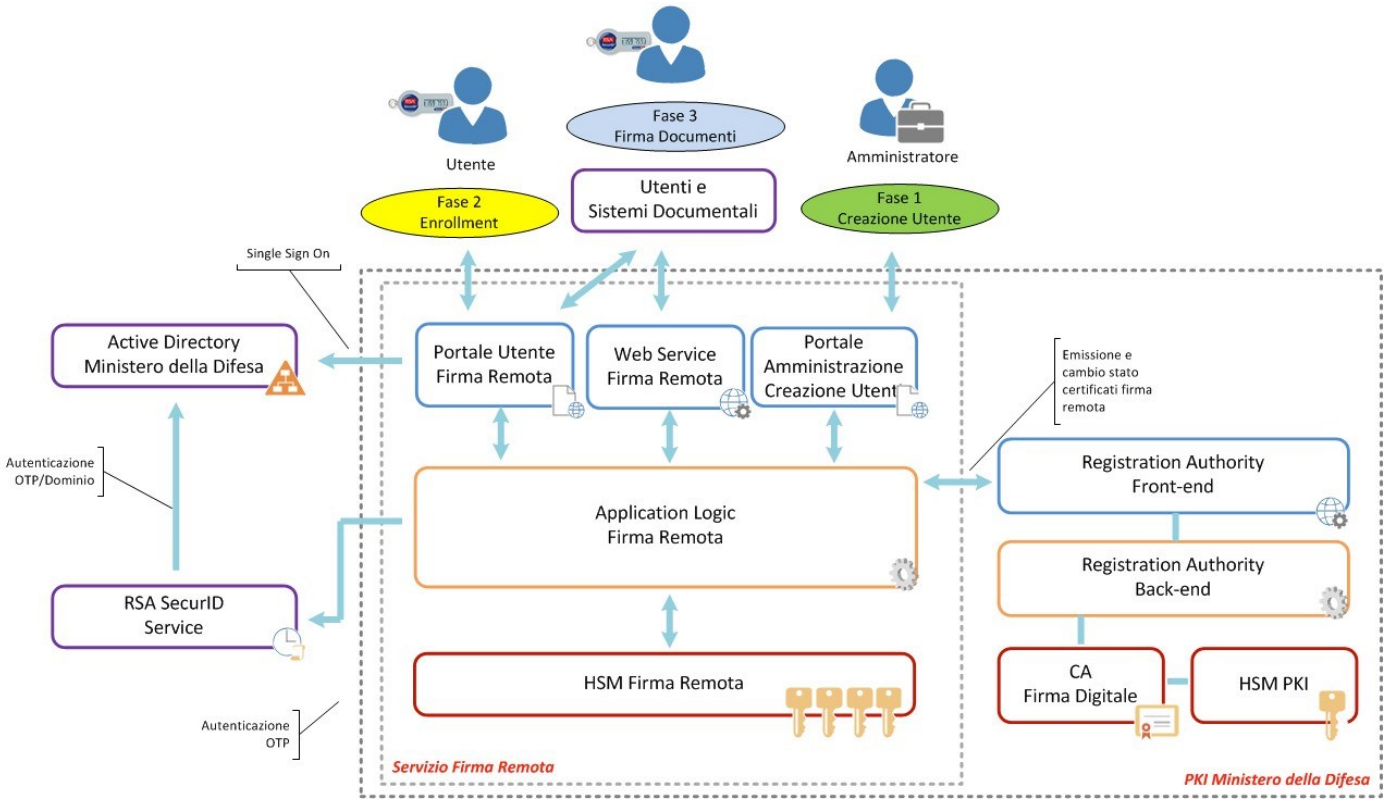
La logica della Fase 3 è molto simile a quella della Fase 2. Una volta che l'utente si è *loggato* al portale di firma remota (http://firmaremota.servizi.difesa.it) ed ha selezionato i documenti da firmare ed il tipo di firma da appore, clicca sul pulsante Firma ed inserisce la password e il codice OTP RSA.

Le credenziali dell'utente (username/password e codice OTP) e hash del documento vengono inviate all'Application Logic di firma remota.

Le credenziali fornite seguono lo stesso iter di verifica descritto alla Fase 2.

Una volta verificate positivamente le credenziali, HSM CoSign "sblocca" l'utilizzo del certificato di firma associato all'utente e la relativa chiave privata, consentendo la firma del documento.

Qualora la firma remota venisse richiesta da un utente attraverso un sistema documentale esterno, il procedimento di firma è similare ma l'accesso al sistema avviene attraverso il Web Services anziché attraverso il Portale.



- Figura 1 -

1.3 Sicurezza fisica

L'apparato di firma digitale remota (HSM ARX CoSign) è situato all'interno 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 Remota è parte integrante dell'infrastruttura PKI del Prestatore di Servizi Fiduciari Qualificati. E' 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 remota è raggiungibile unicamente da postazioni attestate sulla rete Difesa (Difenet) o attraverso il sistema di virtualizzazione Citryx della Difesa.

Le credenziali di accesso all'HSM sono definite dall'utente in fase di enrollment del certificato mentre la Strong Authentication, associata ad ogni utente a mezzo Token OTP-RSA, viene gestita dal Servizio Operatività ICT del Comando per le Operazioni in Rete.

2 Guida per gli utenti del servizio di firma remota

Il processo di richiesta di abilitazione alla firma remota prevede le sottonotate azioni:

1. ***Richiesta***: il titolare richiede l'emissione di un certificato di firma remota a suo nome. Il richiedente compila il modulo di richiesta validandolo con la propria firma digitale e lo invia all'indirizzo firmaremota@smd.difesa.it . Il modulo è scaricabile al seguente link: **https://portalecor.difesa.it/ViceComandante/RepSicurCyberDef/uis/spki/Pagine/FirmaRemota.aspx**
2. ***Autorizzazione***: i dati della richiesta vengono validati dal Centro di Certificazione Difesa, viene creato l'utente e viene restituita una mail di conferma al titolare. A questo punto l'utente, collegandosi al portale di firma remota (http://firmaremota.servizi.difesa.it), può iniziare la procedura di enrollment: attivazione utente, scelta della password e successiva creazione del Certificato.

3. ***Enrollment***: al primo accesso al portale di firma, l'utente dovrà necessariamente attivare il proprio account di Firma Remota scegliendo una password di firma e confermandola a mezzo codice OTP ottenuto dal proprio token RSA (Fig.2)

Figura 2 -

Al termine dell'operazione comparirà un messaggio riportante l'esito della procedura (Fig.3):

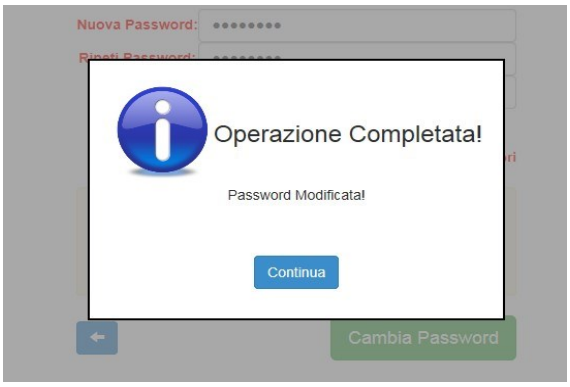
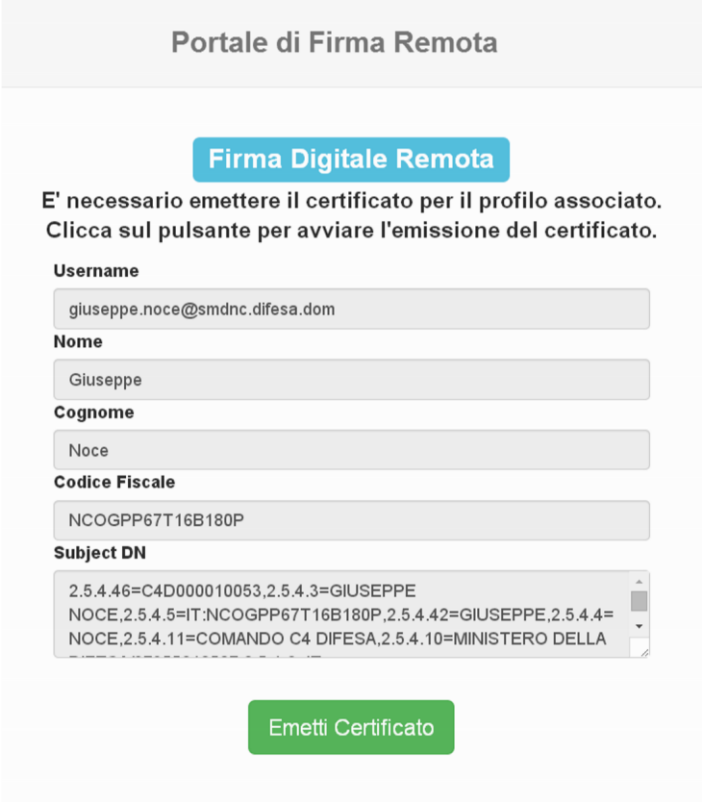


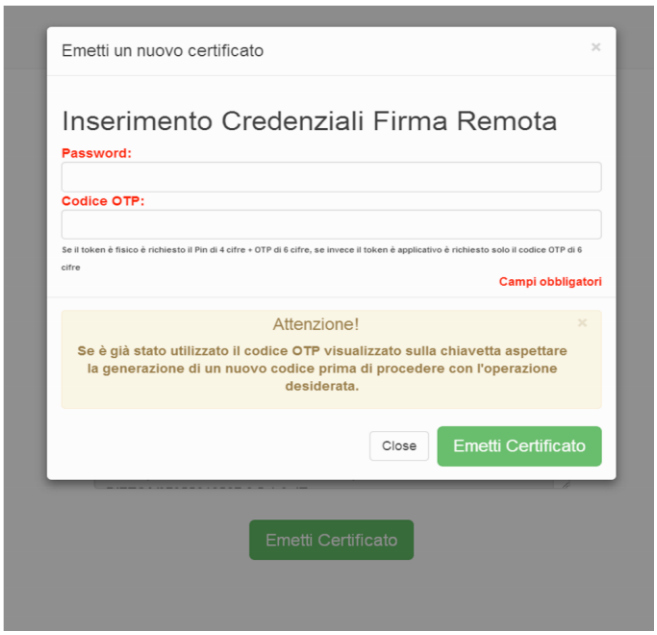
Figura 3 -

Subito dopo l'attivazione dell'account di Firma Remota, si procederà all'emissione del certificato di Firma Remota. L'utente valuterà la correttezza dei dati presentati dal sistema e procederà alla richiesta di emissione premendo il tasto **Emetti Certificato** (Fig.4):



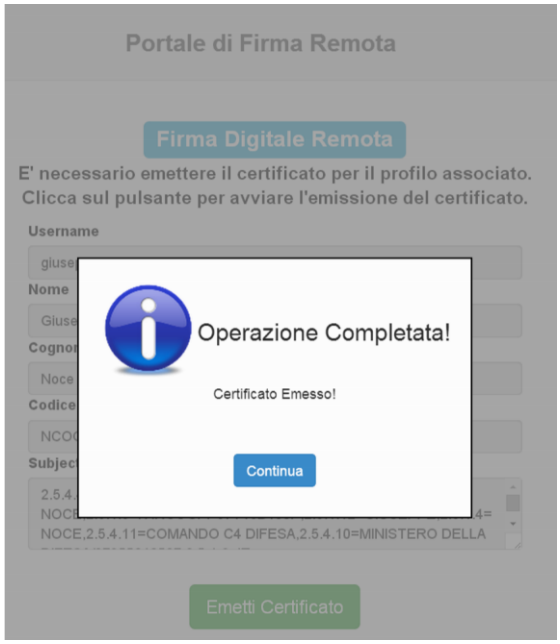
- Figura 4 -

Il sistema richiederà l'inserimento della password di Firma Remota (scelta in precedenza) e del codice OTP (Fig.5)



- Figura 5 -

Al termine dell'operazione comparirà un messaggio riportante l'esito dell'operazione e cliccando su ***Continua*** (Fig.6)



- Figura 6 -

si avrà accesso al portale e si potrà iniziare ad utilizzare il servizio (Fig.7):

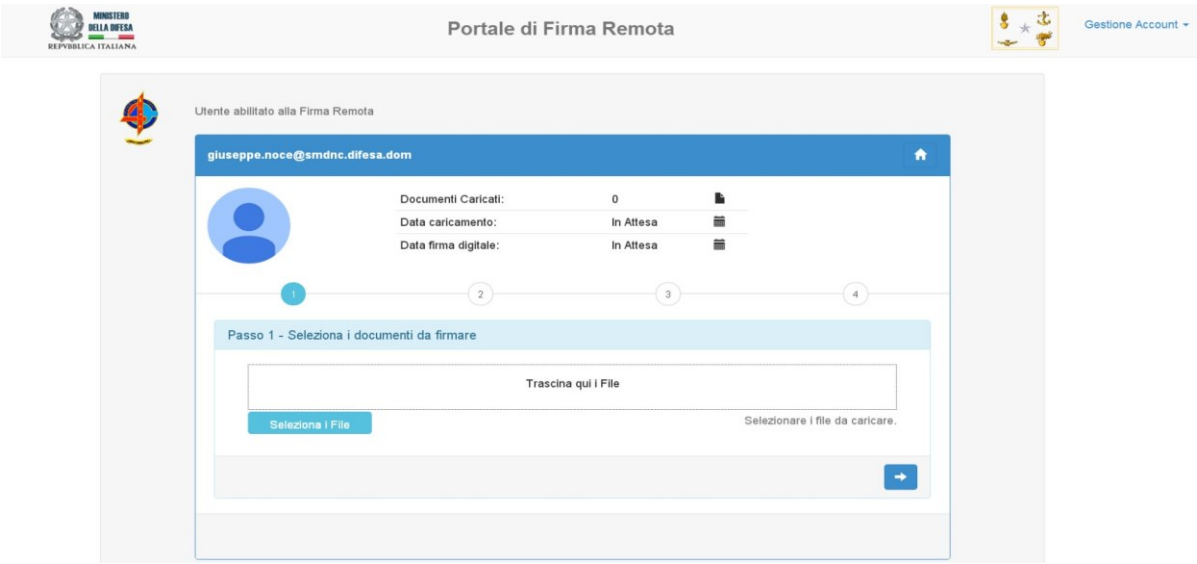


Figura 7 -

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. Il modulo di revoca è scaricabile al seguente link:
https://portalecor.difesa.it/ViceComandante/RepSicurCyberDef/uis/spki/Pagine/FirmaRemota.aspx