STATO MAGGIORE DELLA DIFESA

Comando per le Operazione in Rete

Appendice SGD v.1.8

al

MANUALE OPERATIVO

Public Key Infrastructure

Firma Digitale - Autenticazione CNS – Time Stamping Authority

Firma Automatica del Sistema di Protocollo della Difesa

VERSIONE DOCUMENTO	**1.8**

Compilato da: **Funz.Tec. Raffaele GONNELLA**	*Firmato Digitalmente da/Signed by:* RAFFAELE GONNELLA *In Data/On Date:* lunedì 7 luglio 2025 13:21:11
Revisionato da: **Col. Angelo MARIANI**	*Firmato Digitalmente da/Signed by:* ANGELO MARIANI Capo Centro di Certificazione *In Data/On Date:* lunedì 7 luglio 2025 13:34:51
Approvato da: **Gen. Div. AAran Sandro SANASI**	*Firmato Digitalmente da/Signed by:* SANDRO SANASI *In Data/On Date:* martedì 8 luglio 2025 16:32:42

Sommario delle modifiche

Versione Appendice	Sezione	Descrizione	Data
1.0	//	Prima emissione.	20/02/2014
1.1	// 2.4 3.2	Cambio Certificatore Aggiornamento OID Manuale Operativo	21/07/2015
1.2	Tutte	C.A. e R.A.	16/05/2018
1.3	// 2.1	Cambio revisore GDPR	22/05/2019 22/05/2019
1.4	//	Cambio Denominazione Ente ed Approvatore	09/03/2020
1.5	Tutte	Aggiornamento riferimenti normativi	06/04/2021
1.6	//	Cambio Certificatore	13/01/2022
1.7	//	Cambio Certificatore	24/03/2024
1.8	//	Cambio Gruppo di Certificazione	30/06/2025

Indice

PARTE 1^

NORME GENERALI

1 PREMESSA

Il presente Manuale definisce le procedure, di Firma Digitale Automatica della Difesa, applicate dal **Prestatore di Servizi Fiduciari Qualificati (QTPS) dello Stato Maggiore Difesa - Comando per le Operazioni in Rete** fornite con gli apparati HSM gestiti presso il Segretariato Generale della Difesa (SEGREDIFESA) ubicati **nel comprensorio di via Marsala n. 104 in Roma.**

Il documento, inoltre, descrive l'organizzazione messa in atto dal **Prestatore di Servizi Fiduciari Qualificati (QTPS)**, 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 "Public Key Infrastructure" edito dal Prestatore di Servizi Fiduciari Qualificati (QTPS) e pubblicato sul sito dell'Agenzia per l'Italia Digitale.

2 GENERALITA'

2.1 Scopo del documento

Il presente Manuale illustra le procedure, le regole ed i criteri di tipo tecnico, organizzativo e operativo tramite i quali il Ministero della Difesa, nella figura del **Prestatore di Servizi Fiduciari Qualificati dello Stato Maggiore Difesa - Comando per le Operazioni in Rete** eroga (art. 3 comma 5 del DPCM 22 febbraio 2013) il servizio di *Firma Automatica della Difesa* presso "terzi" ovvero presso il **Segretariato Generale della Difesa** (**SEGREDIFESA**)

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.

[REG] Regolamento UE N.910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 relativa in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno che abroga la direttiva 1999/93/CE.

[GDPR] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

[DM] Decreto 2 luglio 2004, "Competenza in materia di certificatori di firma elettronica" pubblicato sulla G. U. 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 e s.m.i."

[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.

[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.

2.2 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 - Hash-functions - Part 3: Dedicated hash-functions", May 1998.

[SHA2] ISO/IEC 10118-3:2004, "Information technology - Security techniques - Hash-functions - 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.

2.3 Glossario

Fare riferimento al **"Manuale Operativo – Public Key Infrastructure"**
(OID 1.3.6.1.4.1.14031.2.1)

3 INTRODUZIONE

3.1 Dati identificativi del Prestatore di Servizi Fiduciari Qualificati.

Il presente Manuale costituisce l'Appendice v.1.2 *del Manuale Operativo del Prestatore di Servizi Fiduciari Qualificati dello Stato Maggiore Difesa - Comando per le Operazioni in Rete, per le procedure di Firma Automatica della Difesa* in conformità all'art. 40 delle regole tecniche.

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
Sezione Certificazione e conservazione
Via Stresa, 31 B
00135 ROMA

Il Prestatore di Servizi Fiduciari Qualificati mette a disposizione per i servizi offerti e per l'assistenza agli 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 Vers.1.5 al Manuale Operativo

OID: 1.3.6.1.4.1.14031.2.1

Il presente documento è pubblicato sul sito web del Centro di certificazione http://www.pkiff.difesa.it e 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 http://www.pkiff.difesa.it oppure quella pubblicata sul sito web di Ag.ID. (Agenzia per l'Italia Digitale - www.agid.gov.it).
In ogni caso, 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, che si avvale per la sua redazione integrale del dipendente ***Centro di Certificazione e della Registration Authority*** (R.A.).

4 DISPOSIZIONI GENERALI

4.1 Obblighi della Certification Authority (C.A.).

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

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

1. adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
2. informa i Titolari di certificato sulla procedura di certificazione, sulle caratteristiche e limitazioni d'uso delle firme emesse;
3. 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;

4. 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;
5. 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. 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;
2. 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;
3. dare immediata pubblicazione della revoca e della sospensione dei certificati.

4.2 Registration Authority (R.A.).

Per la particolare tipologia del servizio implementato (Firma Automatica della Difesa) il Prestatore di Servizi Fiduciari Qualificati ha rilasciato mandato a svolgere le funzioni di Registration Authority al Segretariato Generale della Difesa, che tramite formale Atto di nomina, incarica un Responsabile della R.A. di S.G.D. per lo svolgimento dei compiti previsti dal presente Manuale:

In particolare la Registration Authority di S.G.D. deve:

- identificare con certezza il Titolare del certificato;
- registrare tutti i dati personali del Titolare ed attuare la procedura di enrollment;
- generare le coppie di chiavi di firma dei Titolari all'interno dei dispositivi di firma;
- non rendersi depositario di chiavi private di firma dei Titolari;
- 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;
- assicurare che il dispositivo sicuro per la generazione delle firme (HSM) abbia le caratteristiche ed i requisiti di sicurezza previsti dalla regole tecniche;
- valutare l'opportunità o la necessità, sulla base delle normative vigenti, di richiedere/sospendere/revocare i certificati digitali;
- comunicare per iscritto ad al Prestatore di Servizi Fiduciari Qualificati ogni variazione significativa delle soluzioni tecnico-organizzative adottate;
- comunicare per iscritto ad al Prestatore di Servizi Fiduciari Qualificati eventuali altri applicativi che si avvalgono del servizio di Firma Automatica della Difesa con le relative procedure tecnico-organizzative adottate

- controfirmare i moduli di domanda di rilascio/sospensione/revoca dei certificati degli utenti della Firma Automatica garantendo la loro identità;
- inoltrare al Centro di Certificazione le richieste di emissione/sospensione/revoca dei certificati con le modalità e i tempi indicati dal Prestatore di Servizi Fiduciari Qualificati;
- chiedere, tramite gli strumenti e le procedure previste dal servizio di certificazione, l'immediata sospensione dei certificati per i quali si siano verificate delle circostanze che possano compromettere la sicurezza della chiave privata o per le quali sia oggettivamente necessario privare il Titolare del potere di firma. La domanda di sospensione, qualora risultino confermate le valutazioni formulate, dovrà essere seguita dalla domanda di revoca;
- chiedere per iscritto l'immediata revoca dei certificati relativi alle chiavi contenute in dispositivi di firma di cui il Titolare abbia perduto il possesso o che siano risultati difettosi facendo precedere tale provvedimento dall'esecuzione della prevista procedura per la sospensione immediata del certificato interessato;
- fornire tutte le informazioni richieste dal Prestatore di Servizi Fiduciari Qualificati; garantendo, sotto la propria responsabilità, la loro attendibilità;
- redigere per iscritto le richieste di revoca specificando le motivazioni e la prevista decorrenza;
- redigere per iscritto le richieste di sospensione specificando le motivazioni ed il periodo durante il quale la validità dei certificati in questione deve essere sospesa;
- custodire con cura copia del documento riepilogativo dei dati inoltrata al Prestatore di Servizi Fiduciari Qualificati e tutte le comunicazioni da questi ricevute, sia in formato cartaceo che elettronico;

  conservare le richieste di registrazione e di certificazione per un periodo di 20 anni dalla data di scadenza del certificato emesso.

4.2.1 Obblighi del Titolare del certificato

Il Titolare del Certificato deve:

1. fornire, alla R.A di S.G.D., tutte le informazioni necessarie garantendone, sotto la propria responsabilità, l'attendibilità ai sensi del DPR 445/2000 e s.m.i.;
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 R.A di S.G.D della necessità di sospendere 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 Firma Automatica 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 al Regolamento UE 910/2014 eIDAS.

4.5 Avvisi

Il Prestatore di Servizi Fiduciari Qualificati si riserva di pubblicare sul proprio sito, all'indirizzo http://www.pkiff.difesa.it e 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

Il sistema di firma automatica, è costituito dalle seguenti componenti:

- appliance HSM Cosign FIPS 4U di ARX;
- un'applicazione di firma elettronica centralizzata denominata *FirmaRemota*.

1.1 Sicurezza fisica

L'apparato di firma digitale automatica (HSM ARX CoSign) è situato all'interno del Centro Elaborazione Dati del Segretariato Generale della Difesa, ubicato nel comprensorio di via Marsala n. 104 in Roma. Il centro Elaborazione Dati è regolamentato dalle procedure generali di accesso al comprensorio stesso.

Il personale dell'Amministrazione Difesa, che presta abitualmente servizio presso il comprensorio di via Marsala, accede al comprensorio stesso attraverso un sistema di riconoscimento che prevede l'utilizzo del Modello ATe.

Il personale estraneo all'Amministrazione, invece, accede al comprensorio solo dopo aver effettuato la procedura di identificazione da parte dell'Ufficio passi.

L'accesso al RACK dove è custodito il dispositivo per l'applicazione di Firma Automatica della Difesa ed il relativo HSM è consentito unicamente al Responsabile della R.A di S.G.D nominato dal Segretariato. Inoltre l'HSM è fornito di chiusura a chiave. La chiave di impiego è custodita dal Responsabile della Registration Authority mentre la chiave di riserva è custodita in busta chiusa e sigillata in cassaforte.

Nessuna persona estranea al CELD può avere accesso all'interno del locale se non dopo essere stata debitamente riconosciuta, autorizzata ed accompagnata. L'accesso di tutte le persone estranee al CELD deve essere trascritto su apposito registro.

1.2 Sicurezza logica

La sicurezza logica è garantita dall'infrastruttura di rete (DIFENET) gestita dal Comando per le Operazioni in Rete attraverso la quale il sistema HSM effettua tutte le operazioni previste e con ulteriori implementazioni di sicurezza da parte della R.A di S.G.D.

Il servizio di firma automatica è raggiungibile unicamente da postazioni attestate sulla rete DIFENET/EINET

L'applicazione *FirmaAutomatica* integra la soluzione di firma digitale HSM CoSign di ARX, ed include un ulteriore layer di indipendenza dal dispositivo di firma basato sull'interfaccia standard PKCS#11.

FirmaAutomatica ha un'interfaccia di amministrazione e di controllo accessibile tramite browser. Tutte le attività sono registrate in un giornale di controllo conforme alle regole tecniche di cui al DPCM 22 febbraio 2013.

FirmaAutomatica è un sistema modulare con funzionalità attivabili separatamente. I moduli attivati sono i seguenti:

- **MODULO BASE: funzioni di amministrazione**, configurazione e gestione HSM multipli, sistema di logging sicuro con marcatura quotidiana dei file di log;
- **ENROLL: enrollment dei certificati qualificati**. Il modulo consente l'enrollment dei certificati qualificati delle Certification Authority italiane con procedure conformi alla normativa;
- **SIGN: API di firma** disponibili via Web Services per firme singole o multiple con o senza marcatura temporale

1.3 Processo di enrollment dei certificati

Il processo di enrollment prevede le sottonotate azioni:

1. ***Richiesta***: il titolare del certificato richiede l'erogazione di un certificato a suo nome, compilando il previsto modulo digitale PDF/A, disponibile sul sito della PKI, e lo firma digitalmente con il certificato di firma del proprio Mod. ATe, garantendo in questo modo l'identità del richiedente;

2. ***Autorizzazione***: i dati della richiesta vengono controllati e validati, con firma digitale apposta con il kit di firma della Difesa, dal Referente Informatico della Registration Authority e contestualmente viene effettuata la richiesta di certificato per l'Utente;

3. ***Erogazione* del certificato**: il personale indicato della R.A di S.G.D. genera le chiavi di firma nel dispositivo HSM ed invia alla Certification Authority la richiesta di emissione del certificato (PKCS#10 in formato PEM). La Certification Authority emette il certificato, lo invia al succitato personale il quale lo inserisce all'interno del dispositivo associandolo all'Utente richiedente.

1.3.1 Erogazione del certificato

L'erogazione dei certificati qualificati può avvenire in due modalità entrambe conformi alla legislazione vigente: User Self Enrollment e CA Enrollment.

Il sistema HSM CoSign, al momento attuale, opera in modalità manuale, non integrato con un sistema di Directory di dominio e con la CA esterna residente presso il Comando per le Operazioni in Rete.

Gli Utenti, quindi, saranno inseriti manualmente all'interno del sistema ed ogni Utente titolare verrà creato senza certificato associato.

Per l'enrollment del certificato viene adottata la modalità di seguito descritta:

1. Il Responsabile della R.A di S.G.D., esegue una verifica di completezza e correttezza dei dati del richiedente; in caso di incongruenza comunica l'anomalia al richiedente che provvederà a correggere o integrare il modulo;
2. Il Responsabile della R.A di S.G.D. una volta verificato il modulo, provvede alla creazione della relativa utenza nell'HSM. Tale procedura avvia la creazione del file CSR verso il titolare, con il conseguente rilascio dei codici di disattivazione. Tali informazioni vengono inviate nella casella postale del titolare del certificato dichiarata nel modulo di richiesta e inserita nell'HSM all'atto della creazione della utenza.
3. Il titolare, attraverso le informazioni ricevute via mail attiva la propria utenza sull'HSM e genera il file CSR.
4. Il CSR generato al punto precedente viene inviato dal titolare al Responsabile della R.A di S.G.D., alla medesima casella postale deputata alla ricezione della modulistica di richiesta, che viene comunicata direttamente al titolare da parte del Responsabile della R.A di S.G.D. che provvede a trasmettere il file CSR e il modulo di richiesta certificato alla R.A di S.G.D.
5. La C.A., dopo aver verificato la corretta della richiesta, genera il certificato e lo restituisce al Responsabile della R.A di S.G.D. che provvede alla trasmissione alla casella postale del titolare indicata nel modulo di richiesta il file trasmesso dalla C.A.
6. Il titolare provvederà, con le informazioni ricevute a suo tempo via mail, all'inserimento e all'attivazione del certificato di firma automatica ricevuto.
7. La mancata attivazione del certificato da parte del titolare entro cinque giorni dalla trasmissione comporta la revoca del certificato. Il Responsabile della R.A di S.G.D. verifica tale evento e ne informa la C.A.
8. La revoca può avvenire su richiesta della C.A., su richiesta del titolare, trasmettendo via mail la richiesta accompagnata dal codice di revoca inviato a suo tempo, o via telefono.
9. Di norma la richiesta di revoca viene soddisfatta entro le 48 ore successive alla ricezione della stessa. Eventuali motivi ostativi a tale attività' che non consentono di rispettare tale termine vengono comunicatiti con immediatezza al richiedente la revoca.

PARTE 3^

SPECIFICHE DISPOSIZIONI PER L'ATTIVITA' DI CERTIFICATION AUTHORITY E REGISTRATION AUTHORITY

In ottemperanza a quanto previsto dall'art. 3 para 5 del DPCM 22 febbraio 2013:

1 La Certification Authority assicura:

- l'avvenuto accreditamento dell'infrastruttura presso l'Agenzia per l'Italia Digitale;
- l'avvenuta comunicazione ad Ag.ID del luogo di ubicazione dei dispositivi di firma automatica;
- l'esecuzione di verifiche periodiche (anche con personale di Ag.ID, se da quest'ultima richiesto) sulla corretta applicazione di tutte le procedure contenute nella presente Appendice al Manuale Operativo;
- la redazione dei verbali dell'attività di verifica e, qualora richiesto, l'inoltro di copia dei suddetti verbali alla stessa Ag.ID al fine di consentire l'attività di cui all'art. 31 del CAD;

2 La Registration Authority assicura:

- La raccolta e conservazione dei Verbali/Atti di nomina dei Responsabili della R.A. di S.G.D. per la Firma Automatica della Difesa (da inviare, al Prestatore di Servizi Fiduciari Qualificati - QTPS);
- La raccolta e conservazione dei Verbali/Atti di nomina:
  - dei Responsabili del Servizio di protocollo Titolari del certificato di firma automatica;
  - dei responsabili di altri applicativi, che utilizzano il certificato di firma automatica (da inviare, su richiesta, al Prestatore di Servizi Fiduciari Qualificati – QTPS);
- La raccolta e conservazione dei Moduli di Richiesta di Firma Automatica firmati digitalmente dal Titolare e dal Responsabile della R.A. di S.G.D. con marcatura temporale incorporata;
- La raccolta e conservazione dei Moduli di Consegna delle Credenziali di Firma al Titolare, firmati digitalmente.

  La raccolta e conservazione dei LOG di Sistema e Giornale di Controllo (da conservare a cura del Responsabile della R.A. di S.G.D. per un periodo di 20 anni dalla data di scadenza del certificato emesso.)

Tabella degli acronimi

Acronimo	Descrizione
AD	Amministrazione Difesa
Ag.ID	Agenzia per l'Italia digitale
AOO	Area Organizzativa Omogenea
CA	Certification Authority
CED	Centro Elaborazione Dati
CSR	Certificate Signing Request
DPCM	Decreto del Presidente del Consiglio dei Ministri
DGW	Default Gateway
DNS	Domain Name System
eIDAS	Reg. UE 910/2014 del Parlamento Europeo e del Consiglio
HSM	Hardware Security Module
FIPS	Federal Information Processing Standards
IDS	Intrusion Detection System
IR	Incaricato della Registrazione
IPS	Intrusion Prevention System
NTP	Network Time Protocol
OTP	One Time Password
QTSP	Qualified Trust Service Provider
REG	Regolamento Europeo
RDBMS	Relational Database Management System
RDS	Responsabile del Servizio