STATO MAGGIORE DELLA DIFESA

Comando per le Operazione in Rete

Public Key Infrastructure – PKI

“Firma Digitale - Autenticazione CNS – Time Stamping Authority ”

Manuale Operativo

VERSIONE DOCUMENTO	**6.8**

Compilato da: **RESP. CONDUZ. TECNICA DEI SISTEMI** **Serg. Marco D'AGOSTINO**	*Firmato Digitalmente da/Signed by:* MARCO D'AGOSTINO *In Data/On Date:* martedì 8 luglio 2025 08:26:23
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 15:26:31
Approvato da: **CERTIFICATORE** **Gen. D. Sandro SANASI**	*Firmato Digitalmente da/Signed by:* SANDRO SANASI *In Data/On Date:* martedì 8 luglio 2025 16:31:38

Sommario delle modifiche

Versione	Sezione	Descrizione	Data
Versione 1.0	Tutte	Primo rilascio ufficiale manuale operativo.	01/07/2006
Versione 2.0	Tutte	Secondo rilascio a seguito: - della generazione del nuovo certificato di *Time Stamping Authority* emissione 2009; - modifica policy di emissione del certificato di *Time Stamping Unit*; - definizione dell'OID per i certificati con limitazioni d'uso.	22/06/2010
Versione 3.0	Tutte	Terzo rilascio a seguito aggiornamento normativo al DPCM 30 marzo 2009 ed alla Deliberazione CNIPA n. 45 del 21 maggio 2009.	29/10/2010

Versione 4.0	_____ 3.1 5.2.1 5.2.2 5.2.8 5.3.5 5.5 5.8.3 5.14 5.15.2	Quarto rilascio a seguito: - installazione del servizio OCSP e definizione dell'OID del certificato OCSP *Responder*; - Inserimento URL del nuovo Sito (Intranet) della PKI-FF; - Inserimento di una nuova tipologia di coppie di chiavi generate dal servizio di certificazione: chiavi di firma del OCSP *Responder*; - Inserimento del nuovo OID 1.3.6.1.4.1.14031.1.3 (certificato di firma del OCSP *Responder*) alle Policy del Centro di Certificazione; - Generazione della chiave privata del certificato di firma del OCSP *Responder*; - Modalità di emissione del certificato di firma del OCSP *Responder*; - Periodo di validità delle chiavi e del certificato di firma del OCSP *Responder*; - Rinnovo dei certificati di firma del OCSP *Responder*; - Servizio OCSP - Servizio OCSP in fase di verifica della firma	19/04/2012
Versione 4.1	_____	- Aggiornamento al DPCM 22 febbraio 2013 - Cambio Certificatore	06/09/2013

Versione 4.2	5.2.2	- Inserito OID di Firma Remota con procedura Automatica - Appendici	20/02/2014
Versione 5.0	Tutte	- Manuale Operativo nuova infrastruttura PKI.	13/07/2013
Versione 5.1	// 5.1.2	- Cambio Certificatore - Aggiornamento Policy OID InfrastrutturaPKI CMD2	21/07/2015
Versione 6.0	Tutte	- Aggiunti gli OID delle nuove CA eIDAS	13/02/2017
Versione 6.1	Tutte	- Variati Responsabile Periferico e Responsabile Trattamento Dati	11/05/2018
Versione 6.2	Tutte	- Variato DLGS196 in GDPR] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016; - Cambio Certificatore	09/03/2020
Versione 6.3	Tabella INFRASTRUTTURA PKI CMD-2 sezione 5.1.2	- Aggiunta nota sugli OID	24/06/2020
Versione 6.4	5.1.2 //	- Aggiunta Profilo di Sigillo Digitale - Cambio Gruppo di Certificazione	06/04/2021
Versione 6.5	5.1.2	- Aggiunta Profilo di Firma Automatica COR	22/11/2021
Versione 6.6	//	- Cambio Certificatore	13/01/2022

Versione 6.7	1.1.2	- Aggiunta norma Regolamento (EU) N. 1183/2024 – eIDAS 2	24/03/2025
	//	- Cambio Gruppo di Certificazione - Cambio Certificatore	
Versione 6.8	//	- Cambio Gruppo di Certificazione	30/06/2025

Indice

PREMESSA

Il presente documento descrive l'organizzazione implementata, dallo Stato Maggiore della Difesa - Comando per le Operazioni in Rete - nell'esercizio delle funzioni di Certificatore accreditato presso l'Agenzia per l'Italia Digitale (Ag.I.D.), per il rilascio dei certificati di firma digitale, di autenticazione CNS e di marcatura temporale.

Inoltre, lo stesso documento, descrive i processi necessari per la generazione, la pubblicazione, la sospensione e la revoca dei certificati.

La firma digitale e l'autenticazione CNS vengono installati su supporto fisico *(smartcard*) e, più precisamente, a corredo del Mod. ATe della Difesa, una *smartcard* che contiene i certificati digitali e le relative coppie di chiavi dei titolari.

Tale *smartcard*, rilasciata ai sensi del DPR 851/1967, del DPCM 24 maggio 2010 e del DPCM 10 maggio 2012, ha anche valore di tessera di riconoscimento elettronico (Mod. ATe)**.**

Ai fini dell'acquisizione dei dati, necessari per l'emissione dei certificati di Firma digitale ed autenticazione CNS, la PKI-Difesa impiega, in funzione di Registration Authority (R.A.), il circuito di emissione del mod. ATe (denominato CMS Unico) e delle relative organizzazioni periferiche di Forza Armata (Local Registration Authority - L.R.A.).

Attraverso tale circuito viene, inoltre, rilasciato a corredo del Mod. ATe un certificato di cifra.

1 GENERALITA'

1.1 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 (di seguito denominato **Prestatore di Servizi Fiduciari Qualificati- QTSP**) offre, avvalendosi di un centro tecnico di certificazione denominato **Servizio di Conservazione ed Identità Digitale**, il servizio di certificazione di chiavi pubbliche denominato **PKI-Ministero della Difesa**.

1.2 Riferimenti alle norme di legge

[eIDAS] Regolamento (EU) 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/EC.

[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.

[DIR] Direttiva del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche (Gazzetta Ufficiale delle Comunità europee L. 13 del 13 dicembre 1999).

[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.

[DLB45/09] Deliberazione CNIPA n.45 del 21 maggio 2009, “Regole per il riconoscimento e la verifica del documento informatico”, Pubblicato nella Gazzetta Ufficiale n. 282 (serie generale) del 3 dicembre 2009.

[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.

[GDPR] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27.04.2016 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.

[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.

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.

1.3 Glossario

Applicazione del Prestatore di Servizi Fiduciari Qualificati: è la parte dell’applicazione WEB, mediante la quale il Prestatore di Servizi Fiduciari Qualificati, o il funzionario autorizzato alla validazione dei dati, richiede l’emissione di un certificato di Firma.

Autenticazione (mediante certificato): è il processo che fa uso del certificato digitale del titolare e attraverso l’impiego della corrispettiva chiave privata garantisce l’autenticità del possessore.

CA-TSA (Time Stamping Authority): Certification Authority finalizzata alla sola generazione di certificati di firma utilizzati dalla TSU (Time Stamping Unit) per la firma di marcature temporali.

Certificato (o certificato digitale): è l’elemento di corrispondenza tra una chiave pubblica e il soggetto Titolare cui essa appartiene. Ad una chiave pubblica è sempre associata una corrispondente chiave privata appartenente solo al Titolare medesimo (l’associazione chiave pubblica chiave privata è univoca).

Prestatore di Servizi Fiduciari Qualificati (QTSP): è l'entità che certifica la corrispondenza del Titolare alla sua chiave pubblica. Il certificatore delle chiavi pubbliche rende disponibile una lista aggiornata delle chiavi in uso e pubblica quelle revocate o sospese.

Certificazione: è il risultato della procedura informatica, applicata alla chiave pubblica, attraverso la quale si garantisce la corrispondenza biunivoca tra la chiave pubblica e la chiave privata in possesso del soggetto Titolare, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo Certificato.

Cifratura di un file: La cifratura di un file è l'operazione mediante la quale, applicando un algoritmo di cifratura con l'impiego di una chiave, si ottiene un file non intelligibile.

Chiave privata: è l'elemento della coppia di chiavi asimmetriche, di esclusivo possesso del soggetto Titolare, mediante il quale si appone la firma digitale sul documento informatico, si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica, oppure si procede all'autenticazione.

Chiave pubblica: elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal Titolare delle chiavi asimmetriche oppure si cifrano i documenti informatici da trasmettere al Titolare delle predette chiavi.

Chiavi asimmetriche: coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici.

Crittografia asimmetrica: tipologia di operazione matematica mediante la quale, utilizzando apposite chiavi tra loro differenti e specifici algoritmi, dal risultato della cifratura di un file ottenuta con una chiave è possibile risalire al file originario unicamente applicando a tale risultato lo stesso algoritmo con l'utilizzo dell'altra chiave.

Dispositivo di firma: supporto elettronico programmabile solo all'origine, utilizzato dal Titolare, sul quale viene generata la coppia di chiavi asimmetriche, quella pubblica e quella privata, e tale da conservare in modo protetto (sicuro) le chiavi private e di generare al suo interno la firma digitale.

Documento informatico: il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.

Ente di registrazione o Registration Authority (RA): è l'entità che si occupa delle procedure di identificazione/registrazione dell'utente e trasmette i dati di competenza al Certificatore tramite un canale sicuro. La RA è tenuta ad identificare con certezza gli utenti che desiderino essere Certificati. Il ruolo di RA è svolto da soggetti esplicitamente autorizzati dal Prestatore di Servizi Fiduciari Qualificati.

Firma digitale: un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Funzione di HASH: funzione matematica che genera, a partire da una generica sequenza di simboli binari, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali.

Hardware Security Module (HSM): insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche.

Infrastruttura chiave pubblica: è l'insieme delle leggi, dei regolamenti, degli standard e dei sistemi preposti al rilascio e alla gestione del ciclo di vita dei certificati digitali e delle corrispettive chiavi.

Impronta di un file: risultato di un'operazione di *HASHING* applicata al file originario.

Lista dei Certificati Revocati (CRL): è la lista firmata digitalmente, tenuta ed aggiornata dal Certificatore, contenente i certificati emessi dallo stesso e successivamente revocati. La revoca è un'operazione definitiva sul certificato.

Manuale Operativo (o Policy di Emissione dei Certificati): documento che definisce le procedure applicate dal Certificatore nello svolgimento della propria attività.

Modello ATe: è la *smartcard* rilasciata al personale Militare e Civile della Amministrazione della Difesa (A.D.) che contiene, tra l'altro, i certificati digitali e le chiavi pubbliche e private.

OCSP *(Online Certificate Status Protocol)*: Protocollo per il controllo on-line dello stato dei certificati digitali.

Postazione di Acquisizione: è la parte dell'applicazione WEB specifica che permette la registrazione dei dati del titolare del certificato necessari per l'emissione del Mod. ATe.

Profilo di una richiesta di certificazione: identifica quali tipologie di certificati si desidera ottenere per il soggetto interessato ad una richiesta di certificazione. I possibili profili sono predefiniti. All'atto della registrazione è definito il profilo della richiesta di certificazione.

Registrazione: procedura con la quale si identifica con certezza un soggetto per il quale si richiede un certificato e si procede al caricamento dei suoi dati nei sistemi informatici per l'immagazzinamento dei dati allo scopo di emettere il Mod. ATe ed i relativi certificati.

Registro dei Certificati: è il sistema informatico sul quale sono immagazzinati i certificati emessi, revocati e sospesi.

Funzionario Autorizzato alla validazione dei dati: è il soggetto deputato, presso un generico Ente/Unità dell'Organizzazione di Forza Armata e/o Ente della P.A., alla identificazione dei soggetti, per i quali si intende rilasciare i mod. ATe, ed i relativi certificati, nonché deputato alla compilazione e all'inoltro delle richieste di emissione/sospensione/revoca degli stessi certificati. Si identifica di massima con il Comandante di Corpo di un Ente/Unità (o suo delegato) e con un Dirigente/Funzionario di un Ente della P.A..

Operatore Autorizzato all'inserimento dei dati: è la persona presso l'Ente che svolge la funzione di coadiuvare il futuro titolare del certificato a rilasciare i dati necessari per il rilascio del certificato

stesso. E' anche responsabile della corretta identificazione del futuro titolare. L'Operatore autorizzato all'inserimento dei dati è dotato di apposito strumento per l'apposizione della propria firma qualificata.

Revoca del certificato: Operazione con cui il Certificatore annulla la validità del certificato da un dato momento in poi.

Rinnovo del certificato: Operazione con cui viene rinnovato un certificato di firma digitale e/o di cifratura presente sul mod. ATe.

Servizi di Certificazione: sono, nel loro insieme, i servizi forniti dal Centro di Certificazione PKI Difesa. In particolare i servizi disponibili sono i seguenti:

- emissione, revoca e sospensione dei certificati;
- disponibilità dell'accesso al Registro dei Certificati, ove avviene la pubblicazione dei certificati e delle CRL.
- disponibilità dell'accesso al Servizio OCSP *Responder* per la verifica dello stato del certificato qualificato;
- disponibilità dell'accesso al Server TSU per la richiesta di marche temporali.

Servizio Conservazione e Identità Digitale (Centro di Certificazione PKI Difesa): è l'Ufficio che include il personale, i materiali e le procedure per l'erogazione dei servizi di certificazione.

Sistema di validazione: sistema informatico e crittografico in grado di generare ed apporre la firma digitale o di verificarne la validità.

Smart-card: tessera in materiale plastico/policarbonato, di formato simile ad una carta di credito, dotata di un microchip (apparato elettronico incorporato), programmabile solo all'origine, in grado di contenere informazioni in modo sicuro.

Sospensione del certificato: Operazione con cui il Certificatore sospende la validità del certificato, da un dato momento, e per un determinato periodo di tempo.

Titolare di un certificato: soggetto al quale, previa identificazione da parte dell'Ente di registrazione, sono rilasciati i Certificati digitali dal Certificatore che sono associati in modo univoco alle chiavi pubbliche e private. Il Titolare del certificato digitale è una persona fisica o una macchina.

Time Stamping Unit (TSU): sistema attraverso il quale è possibile rilasciare, su richiesta dell'utente, un riferimento temporale univoco associato ad un documento elettronico. Il riferimento temporale univoco è la" marcatura temporale" ed è firmata con il certificato rilasciato dalla **CA-TSA**.

Utenti dei servizi di certificazione: sono i soggetti che, in qualità di Titolari di certificati o di Utilizzatori dei certificati, accedono ai servizi messi a disposizione per il mod. ATe.

Utilizzatore: è il soggetto che accede agli archivi mantenuti dal Prestatore di Servizi Fiduciari Qualificati per richiedere e verificare i Certificati digitali.

Validità del certificato: periodo di tempo durante il quale la chiave pubblica e gli altri dati contenuti nel certificato risultano validi ed utilizzabili da terzi con la garanzia del Certificatore.

2 INTRODUZIONE

2.1 Dati identificativi del Prestatore di Servizi Fiduciari Qualificati

- **PKI - Public Key Infrastructure del Ministero della Difesa**
  SMD - Comando per le Operazioni in Rete - via STRESA n.31/b - 00135 Roma.
- **Infrastruttura di Disaster Recovery**
  Comando per le Operazioni in Rete (COR) - via Guido RENI n.22 - 00196 Roma.

- **Soggetto Giuridico**

STATO MAGGIORE DELLA DIFESA

COMANDO PER LE OPERAZIONE IN RETE

Via Stresa, 31 B

00135 ROMA

Il **Centro di Certificazione PKI Difesa**

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

Via Stresa, 31 B

00135 ROMA

Il Centro di Certificazione PKI Difesa 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: **http://www.pkiff.difesa.it** e **https://pki.difesa.it/tsp**

2.2 Versione del Manuale Operativo

La versione del presente Manuale Operativo è identificata dalla sigla:

Manuale Operativo v 6.8 - 1.3.6.1.4.1.14031.2.1

Il presente Manuale viene pubblicato ai sensi dell'art. 40, comma 2, del [DPCM_22-02-2013].

- sul sito web del servizio di certificazione Difesa (https://pki.difesa.it/tsp/ e http://www.pki.difesa.it)
- sul sito web dell'Agenzia per l'Italia Digitale – Ag.ID. (http://www.agid.gov.it)

Come versione corrente del Manuale Operativo si intenderà esclusivamente la versione in formato elettronico disponibile sul sito web del servizio di certificazione o, in alternativa, la versione pubblicata sul sito web di Ag.ID..

Qualora le due versioni pubblicate risultino non congruenti, la versione pubblicata sul sito web dell'Ag.I.D. avrà valore predominante rispetto a quello pubblicato sul sito del Certificatore.

Il documento è inoltre pubblicato in formato **PAdES**, in modo da assicurarne l'origine e l'integrità.

2.3 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 ed aggiornamento del dipendente Centro di Certificazione PKI Difesa.

3 DISPOSIZIONI GENERALI

3.1 Note sull'organizzazione del personale

Il personale preposto all'erogazione e controllo del servizio di certificazione è organizzato nel rispetto dell'art. 38 comma 1 del [DPCM_22-02-2013].

In particolare, sono definite le seguenti figure organizzative:

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

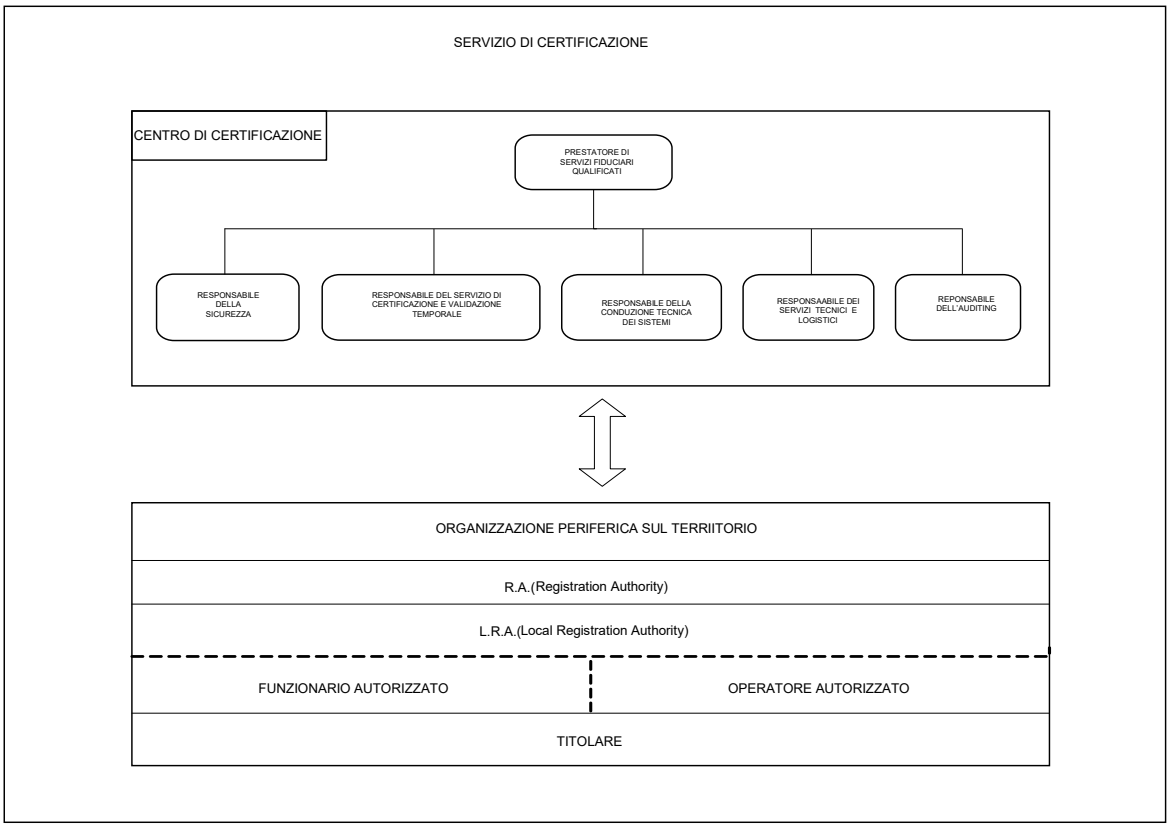
In ottemperanza al citato decreto non sono attribuite, al medesimo soggetto, più funzioni tra quelle sopraelencate (art. 38/2 del [DPCM_22-02-2013]).

Per le funzionalità organizzative del servizio di certificazione, il **Responsabile del servizio di certificazione e validazione temporale** è anche **"Capo del Centro di Certificazione PKI Difesa"** e risponde al Prestatore Servizi Fiduciari Qualificati, quale suo delegato, dell'applicazione delle norme vigenti il processo di certificazione, del corretto funzionamento dei servizi tecnologici e della corretta conduzione del servizio.

Nell'attività di certificazione sono coinvolte altresì le seguenti figure:

- Funzionario autorizzato alla validazione dei dati (figura professionale destinata presso l'Ente che richiede l'emissione dei certificati qualificati per il titolare).
- Operatore autorizzato all'inserimento dei dati (figura professionale destinata presso l'Ente che coadiuva il futuro titolare dei certificati nella fase di presentazione dei dati necessari al rilascio dei certificati stessi. E' responsabile della corretta identificazione del futuro titolare).
- Titolare (soggetto al quale sono rilasciati i certificati qualificati da parte del Certificatore)
- Utilizzatore (una qualsiasi entità, figurata o reale, che fa uso di un certificato qualificato per verificare la validità della firma digitale o dell'autenticazione)

Lo schema di seguito riportato, sintetizza l'organizzazione del servizio:



3.2 Definizione degli obblighi del Prestatore di Servizi Fiduciari Qualificati, dei Funzionari autorizzati alla validazione dei dati, degli Operatori autorizzati all'inserimento dei dati, dei Titolari e degli Utilizzatori

3.2.1 Obblighi del Prestatore dei Servizi Fiduciari Qualificati e della Registration Authority

Nello svolgimento dell'attività di registrazione il Prestatore dei Servizi Fiduciari Qualificati si avvale della Registration Authority (R.A.) e controlla, per il tramite del Centro di Certificazione PKI Difesa, che vengano rispettate tutte le sottonotate prescrizioni delle quali rimane, comunque, direttamente responsabile:

1. adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri (art. 32, comma 2, DLGS 82/2005 e successive modificazioni);
2. identificare, *de visu,* la persona che fa richiesta della registrazione ai fini della certificazione (art. 32, comma 3, lett. A, DLGS 82/2005 e successive modificazioni);
3. comunicare all'Ag.I.D. 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 Certificatore o il suo annullamento (art.37, comma 1, DLGS 82/2005 e successive modificazioni), specificando che tutti i certificati non scaduti al momento della cessazione devono essere revocati;
4. attenersi alle regole tecniche di cui all'art.32, comma 3 e comma 4, DLGS 82/2005 e successive modificazioni;
5. attenersi al D.P.C.M. 18 gennaio 2016 "Modifiche al decreto del Presidente del Consiglio dei ministri del 24 maggio 2010, recante: «Regole tecniche delle Tessere di riconoscimento (mod. AT) di cui al decreto del Presidente della Repubblica 28 luglio 1967, n. 851, rilasciate con modalità elettronica dalle Amministrazioni dello Stato, ai sensi dell'articolo 66, comma 8, del DLGS 82/2005 e successive modificazioni;
6. accertare l'autenticità delle richieste di certificazione (art. 18, comma 1, lett. a), DPCM 22-02-2013);
7. attenersi alle misure minime di sicurezza per il trattamento dei dati personali emanate ai sensi del DLGS 196/2003 e s.m.i. e del Reg. (EU) 679/2016 (GDPR), (art. 32, comma 5, DLGS 82/2005)];
8. conservare le richieste di registrazione e di certificazione per un periodo di 20 anni dalla data di scadenza del certificato emesso (art. 32, comma 3, lett. j, DLGS 82/2005).

Nello svolgimento dell'attività di certificazione, il Certificatore deve:

1. generare le coppie di chiavi di firma dei Titolari all'interno dei dispositivi di firma (art. 6, comma 1 e 2, DPCM 22-02-2013);

2. non rendersi depositario di chiavi private di firma dei Titolari (art. 32, comma 3, DLGS 82/2005 e s.m.i.);
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 (art. 6, comma 1, DPCM 22-02-2013);
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 (art. 18, comma 1, DPCM 22-02-2013);
5. rilasciare e rendere pubblici i certificati in conformità alle caratteristiche fissate dagli artt. 34 e 42 del DPCM 22-02-2013;
6. attenersi alle regole tecniche di cui all'art. 71, DLGS 82/2005 e s.m.i;
7. comunicare per iscritto ad Ag.I.D. ogni variazione significativa delle soluzioni tecnico-organizzative da adottare (Circolare CNIPA/CR/48, 6 settembre 2005);
8. comunicare tempestivamente ad Ag.I.D. ogni variazione significativa delle soluzioni tecnico-organizzative adottate (Circolare CNIPA/CR/48, 6 settembre 2005);
9. procedere tempestivamente alla sospensione e/o alla revoca del certificato in caso di richiesta espressamente formulata da parte del Titolare o da parte del relativo Funzionario Autorizzato alla validazione dei dati o in caso di acquisizione da parte dello stesso Certificatore della conoscenza di cause limitative della capacità del Titolare, di sospetti abusi o falsificazioni con le modalità di cui agli artt. 20, 23, 24, 25, 27, 28 e 29 del DPCM 22-02-2013;
10. dare immediata pubblicazione della revoca e della sospensione dei certificati relativi alle coppie di chiavi asimmetriche (art. 22 e 26 del DPCM 22-02-2013).

3.2.2 **Obblighi del Funzionario Autorizzato alla validazione dei dati**

Il Funzionario Autorizzato alla validazione dei dati che abbia tra i suoi dipendenti dei Titolari di certificati deve:

1. Valutare l'opportunità o la necessità, sulla base delle normative vigenti, di richiedere/sospendere/revocare i certificati digitali per i propri dipendenti;
2. controfirmare i moduli di domanda di rilascio/sospensione/revoca dei propri dipendenti verificando e garantendo la loro identità;
3. inoltrare al Centro di Certificazione PKI Difesa le richieste di emissione/sospensione/revoca dei certificati con le modalità e i tempi indicati dal Certificatore;
4. 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 in tali circostanze, dovrà essere seguita dalla domanda di revoca;

5. 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 (art. 8, comma 5, lett. c) e lett. e) del DPCM 22-02-2013), facendo precedere tale provvedimento dall'esecuzione della prevista procedura per la sospensione immediata del certificato interessato;
6. fornire tutte le informazioni richieste dal Certificatore garantendo, sotto la propria responsabilità, la loro attendibilità. Le informazioni richieste dal Certificatore sono quelle indicate sulla modulistica prevista dal presente Manuale;
7. redigere per iscritto le richieste di revoca specificando le motivazioni e la prevista decorrenza (art. 25, DPCM 22-02-2013);
8. 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 (art. 29, DPCM 22-02-2013);
9. custodire con cura copia del documento riepilogativo dei dati inoltrata al Certificatore e tutte le comunicazioni da questi ricevute, sia in formato cartaceo che elettronico.

3.2.3 **Obblighi dell'Operatore Autorizzato all'inserimento dei dati**

L' Operatore autorizzato all'inserimento dei dati deve:

1. intraprendere le attività necessarie al rilascio dei dati per la richiesta di certificazione;
2. procedere ad autenticare il futuro titolare del certificato tramite un valido documento di identità personale;
3. firmare i moduli di domanda di rilascio delle persone che fanno richiesta di certificato;
4. firmare digitalmente le richieste da inoltrare al Funzionario autorizzato alla validazione dei dati.

3.2.4 **Obblighi del Titolare del certificato**

Il Titolare del Certificato deve:

1. fornire tutte le informazioni necessarie all'Operatore autorizzato all'inserimento dei dati/ Funzionario autorizzato alla validazione dei dati garantendone l'attendibilità, consapevole delle sanzioni penali richiamate ai sensi dell'art. 76 del D.P.R. n.445/2000, in caso di dichiarazioni mendaci;

2. conservare, con la massima diligenza, la chiave privata ed il dispositivo che la contiene al fine di garantire l'integrità e la massima riservatezza (art. 8, comma 5, lett. a, DPCM 22-02-2013);
3. conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave (art. 8, comma 5, lett. b, DPCM 22-02-2013);
4. sporgere denuncia, in caso di smarrimento o sottrazione del dispositivo di firma, alle Autorità di Polizia Giudiziaria;
5. procedere alla immediata comunicazione al servizio di certificazione, tramite gli organi e le procedure da questo definiti, 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.
6. redigere per iscritto le richieste di revoca specificando le motivazioni e la prevista decorrenza (art. 24, DPCM 22-02-2013);
7. 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 (art. 28, DPCM 22-02-2013).

3.2.5 **Obblighi dell'utilizzatore del certificato**

L'utilizzatore del Certificato per accertare in modo inconfutabile la *"non ripudiabilità"* da parte del Titolare delle firme digitali da lui apposte su un documento informatico deve controllare mediante specifici applicativi di verifica :

- l'attendibilità del certificato, cioè la certezza che sia stato firmato digitalmente con la chiave di certificazione del Certificatore;
- la validità del certificato, cioè verificare che il certificato non risulti sospeso, revocato o scaduto. In particolare che il certificato non compaia nelle liste di revoca/sospensione pubblicate dal servizio stesso;
- l'esistenza di eventuali limitazioni nell'uso del certificato utilizzato dal Titolare.

Saranno considerate attendibili unicamente le verifiche di firme digitali eseguite con gli applicativi le cui case produttrici ne dichiarano espressamente la conformità alla normativa vigente in materia di firma elettronica qualificata/firma digitale.

3.3 **Definizione delle responsabilità del Prestatore di Servizi Fiduciari Qualificati, della Registration Authority, dei Funzionari Autorizzati alla validazione dei dati, degli Operatori Autorizzati all'inserimento dei dati, dei Titolari e degli Utilizzatori.**

Nell'espletamento dei servizi di certificazione e nell'utilizzo operativo della firma qualificata, il Prestatore di Servizi Fiduciari Qualificati, la Registration Authority, il Funzionario Autorizzato alla validazione dei dati, l'Operatore Autorizzato all'inserimento dei dati, i Titolari e gli Utilizzatori hanno le responsabilità di seguito esplicitate.

3.3.1 **Responsabilità del Prestatore di Servizi Fiduciari Qualificati e della Registration Authority**

Nello svolgimento dell'attività di registrazione il Prestatore di Servizi Fiduciari Qualificati, avvalendosi della Registration Authority e per il tramite del Centro di Certificazione PKI Difesa, è responsabile:

- della certa identificazione del personale destinatario dei certificati;
- del corretto funzionamento del sistema informatico per l'esecuzione delle proprie attribuzioni;
- del possesso dei privilegi d'accesso alle funzionalità del sistema unicamente da parte del personale preposto, salvo dolo da parte degli stessi operatori;
- della corretta implementazione dei privilegi di accesso ai sistemi, da parte dei propri operatori, alle sole funzionalità necessarie all'espletamento delle attività previste per le loro funzioni;
- della corretta generazione delle coppie di chiavi;
- della corretta attivazione dei dispositivi di firma;
- della segretezza dei codici di attivazione (PIN e PUK di Firma) dei dispositivi di firma e del Codice di Emergenza da consegnare al Titolare;
- del rispetto delle procedure descritte nel presente Manuale;
- della corretta erogazione del servizio di certificazione;
- del corretto funzionamento del Servizio di marcatura temporale;
- del corretto funzionamento del Servizio OCSP;
- del corretto funzionamento dell'infrastruttura tecnologica;
- della sicurezza dei dati contenuti nei propri sistemi;
- della corretta formalizzazione ed implementazione delle politiche di sicurezza sui sistemi tecnologici e sulle procedure di lavoro;
- dell'esatta corrispondenza dei dati relativi ai Titolari dei certificati, riportati sui moduli di domanda prodotti e vidimati dai relativi Responsabili Periferici, con quelli immessi nei propri archivi e riportati sui certificati;
- della consistenza e integrità dei dati contenuti nei propri archivi;

- della tempestiva variazione dello stato dei certificati e del conseguente aggiornamento del Registro dei Certificati, a seguito del verificarsi di eventi che, segnalati dagli stessi Titolari o dai Responsabili Periferici, comportino il cambiamento dello stato dei certificati.

3.3.2 **Responsabilità del Funzionario Autorizzato alla validazione dei dati**

Il Funzionario Autorizzato alla validazione dei dati del soggetto per il quale si richiede un certificato, o che già ne sia Titolare, è responsabile:

- della certa identificazione del soggetto;
- della veridicità dei dati riportati sulle domande di certificazione, revoca e sospensione;
- dell'indottrinamento del soggetto interessato circa obblighi e responsabilità a lui derivanti dall'utilizzo dei dispositivi di firma;
- del trattamento dei dati personali del soggetto interessato;
- dell'inoltro delle domande di certificazione, sospensione o revoca dei certificati;
- della corretta conservazione e custodia delle copie in originale delle domande di certificazione, sospensione e revoca inoltrate, nonché di tutte le comunicazioni, in formato cartaceo e/o elettronico, pervenute dal Centro di Certificazione PKI Difesa;
- dell'immediata comunicazione al Centro di Certificazione PKI Difesa della necessità di procedere con immediatezza alla sospensione dei certificati per i quali sussista la oggettiva possibilità della compromissione della chiave privata o ai cui Titolari sia necessario revocare immediatamente il potere di firma;
- della corretta applicazione, nell'ambito di propria competenza, delle norme attuative riguardo alle determinazioni di quali soggetti debbano essere Titolari di certificati di firma digitale;
- del pronto inoltro, nei casi previsti da specifiche norme interne all'Amministrazione Difesa, delle richieste di certificazione, sospensione o revoca;
- della definizione e della corretta applicazione delle norme e procedure di lavoro, interne alla propria organizzazione, che prevedano la generazione di firme digitali.

3.3.3 **Responsabilità dell'Operatore Autorizzato all'inserimento dei dati**

L'Operatore Autorizzato all'inserimento dei dati, nominato dal Funzionario Autorizzato alla validazione dei dati, è responsabile:

- della certa identificazione del richiedente il certificato;
- della corretta acquisizione dei dati.

3.3.4 Responsabilità del Titolare del certificato

Il Titolare di un certificato per firma digitale è responsabile:

- della corretta comunicazione dei propri dati personali al Funzionario autorizzato alla validazione dei dati;
- della corretta custodia del dispositivo di firma e dei relativi codici di attivazione (PIN e PUK) e del codice di emergenza;
- del corretto utilizzo del dispositivo di firma;
- della corretta applicazione delle norme e procedure di lavoro che prevedano l'impiego di firma digitale;
- della pronta comunicazione al Funzionario autorizzato alla validazione dei dati di possibili malfunzionamenti riscontrati sul dispositivo di firma;
- della pronta comunicazione al Funzionario autorizzato alla validazione dei dati o, qualora non sia immediatamente contattabile (es. fuori orario di servizio), direttamente al servizio di Call Center tel. 0649914444, di circostanze che determinino una possibile compromissione della chiave privata (es. furto o smarrimento del dispositivo, sospetti di avvenuta clonazione, riscontro di attacchi di pirateria informatica indirizzati al dispositivo di firma, ecc.) al fine di procedere alla sospensione immediata del corrispondente certificato.

3.3.5 Responsabilità dell'Utilizzatore

L'Utilizzatore di un certificato, ovvero colui che utilizza un certificato per verificare una firma digitale è responsabile:

- del controllo della attendibilità del certificato tramite verifica della firma dello stesso da parte dell'Autorità di Certificazione indicata;
- della verifica della validità del certificato mediante la consultazione, in tempo reale, delle liste di revoca/sospensione dal Registro dei Certificati reso disponibile dal Certificatore.

3.4 Aspetti normativi e legislativi

L'organizzazione e l'erogazione del servizio di certificazione sono sottoposte alla legislazione italiana ed europea. Inoltre, laddove non in disaccordo con la normativa di legge, vengono applicate le norme attuative emanate in ambito Ministero Difesa e Stato Maggiore Difesa (Pubb. SMD-I-009).

3.5 Normativa in vigore

Il presente Manuale fa riferimento alla normativa vigente in ambito nazionale e comunitario in materia di "firma digitale e autenticazione CNS".

3.6 Avvisi

Il Prestatore di Servizi Fiduciari Qualificati si riserva di pubblicare sul proprio sito, all'indirizzo http://www.pki.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 di Ag.ID.

4 ASPETTI OPERATIVI

4.1 Modalità di identificazione e registrazione dei titolari

Il processo di registrazione dei Titolari avviene attraverso una procedura informatica. Di seguito sono evidenziate le modalità di acquisizione per il personale - militare e civile - appartenente alla Difesa ed agli Enti della P.A..

4.1.1 Acquisizione dei Dati

La procedura di acquisizione dei dati (*enrollment*), avviene presso i Locali Centri di Registrazione (LRA) ed ha inizio solo dopo la presentazione della richiesta cartacea debitamente compilata dal richiedente e firmata dal Comandante di Corpo/Delegato o Dirigente/Funzionario abilitato.

L'Operatore Autorizzato all'inserimento dei dati effettuata l'identificazione *de visu* del richiedente e attraverso un valido documento di riconoscimento, e procede:

- all'acquisizione dei dati anagrafici, militari, amministrativi e biometrici, attraverso specifiche procedure, verificando anche che sull'allegato "A" sia stato inserito l'indirizzo mail istituzionale
- fa confermare all'interessato, con firma grafometrica, i dati raccolti;
- convalida i dati raccolti controfirmandoli con la propria firma digitale.

Terminata la procedura di inserimento, il Funzionario Autorizzato alla validazione dei dati della LRA convalida i dati attraverso una apposita procedura di approvazione apponendo la propria firma digitale e provvede all'invio dei dati al CMS che esegue una verifica dei dati pervenuti, richiede l'emissione dei certificati alla C.A. e stampa il mod. ATe.

4.1.2 Emissione, consegna e attivazione del mod. ATe e dei Certificati Digitali

Allo scopo di delineare sommariamente il processo di emissione del mod. ATe, in gran parte automatizzato, si enumerano, di seguito, i passi logici fondamentali compresi in tale procedura.

Il personale del Centro di Registrazione (RA) preposto all'emissione, dopo aver verificato il corretto funzionamento della carta, avvia il processo di emissione:

- genera all'interno della carta la prima coppia di chiavi e inoltra alla CA CNS una richiesta di

certificato di autenticazione. La CA rilascia il certificato di autenticazione CNS e lo pubblica sul proprio sito (LDAP). Il certificato CNS viene quindi installato a bordo del mod. ATe;

- genera all'interno della carta la seconda coppia di chiavi e inoltra alla CA di Firma una richiesta di certificato di firma digitale. La CA rilascia il certificato di firma digitale e lo pubblica sul proprio sito (LDAP). Il certificato di Firma Digitale viene quindi installato a bordo del mod. ATe;
- genera all'interno della carta la terza coppia di chiavi e inoltra alla CA di Cifra una richiesta di certificato di cifra. La CA rilascia il certificato di cifra e memorizza in un proprio database la chiave privata corrispondente (procedura di *escrew*). Il certificato di Cifra viene quindi installato a bordo del mod. ATe;
- inserisce i dati personali del Titolare nel chip e personalizza la carta graficamente;
- ad operazione ultimata con successo, il CMS pone la carta in stato "prodotta" ed invia, automaticamente, una email al Titolare della carta con le informazioni di *"carta prodotta"*.
- La LRA provvede al ritiro del mod. ATe prodotto ed il CMS invia, automaticamente, al Titolare della carta una seconda email di "*carta consegnata"* alla LRA e disponibile per il ritiro. In tale email saranno presenti un CODICE DI EMERGENZA (da conservare per tutto il periodo di validità della carta), un codice per il ritiro del mod. ATe presso la LRA (da utilizzare una sola volta) ed il memorandum di sicurezza per l'utilizzo della Carta stessa;
- Il Titolare riceve il mod. ATe dalla LRA che ne ha richiesto l'emissione ed il CMS invia, automaticamente, una terza ed ultima email di *"carta distribuita"*. In tale email il Titolare troverà il *link di collegamento* al portale di attivazione della Carta ed un CODICE DI VISUALIZZAZIONE (utilizzabile una sola volta);
- il Titolare, attraverso la rete INTRANET e con il mod. ATe inserito nel lettore, collegandosi al predetto link potrà accedere alla propria AREA RISERVATA e visionare i codici PIN/PUK relativi ai certificati presenti nel chip della Carta stessa.

NOTA BENE: Tutte le comunicazioni effettuate dal Certificatore/Registration Authority/Local Registration Authority saranno inviate all'indirizzo di posta istituzionale (p.es. nome.cognome@marina.difesa.it) comunicato dal Titolare all'atto dell'acquisizione dei dati e sottoscritto sul modulo di richiesta di emissione della carta.

In fase di consegna della carta, inoltre, il Titolare dovrà confermare la presa visione del **memorandum di utilizzo** ricevuto, contestualmente all'invio delle credenziali, all'indirizzo di posta elettronica istituzionale.

5 Tipologia, generazione e gestione delle coppie di chiavi

5.1.1 Tipologia

Le coppie di chiavi generate dal servizio di certificazione in questione appartengono alle seguenti tipologie:

- Chiavi di CA di Firma;
- Chiavi di CA Autenticazione CNS
- Chiavi di CA-TSA;
- Chiavi di firma digitale utente;
- Chiavi di autenticazione CNS utente;
- Chiavi di marcatura temporale TSU;
- Chiavi di firma del OCSP;
- Chiavi per applicazioni a supporto della PKI.

5.1.2 **Policy supportate**

Il profilo del certificato è conforme alla [DLB45/09]. Attributi ed estensioni facoltativi possono variare in rapporto alle specifiche policy utilizzate.

Vengono riportati, di seguito, le policy relative alle 2 Infrastrutture di CA del Ministreo della Difesa (PKI/CMD-1 E PKI/CMD-2).

L'Infrastruttura denominata PKI/CMD-1 è stata dismessa nell'anno 2019 a seguito della revoca dell'ultimo certificato in circolazione ed è stata esposta l'ultima CRL in data 20/10/2019.

La CA/CMD-1 esporrà l'ultima CRL fino alla data di scadenza della CA stessa (6 settembre 2023).

Pertanto, le policy del Centro di Certificazione PKI Difesa saranno identificate dagli OID presenti nell'estensione *CertificatePolicie*s così come di seguito specificati:

INFRASTRUTTURA PKI/CMD-1

Policy OID	**Descrizione**
1.3.6.1.4.1.14031	Stato Maggiore della Difesa - Comando per le Operazioni in Rete
1.3.6.1.4.1.14031.1	Certification Service Provider (CSP)
1.3.6.1.4.1.14031.1.1	Policy di sicurezza dei certificati di Firma Qualificata e Marcatura Temporale
1.3.6.1.4.1.14031.1.2	Policy di sicurezza dei certificati di Firma Qualificata con limitazioni d'uso
1.3.6.1.4.1.14031.1.3	Policy di sicurezza dei certificati di firma del OCSP *Responder*
1.3.6.1.4.1.14031.1.4	Policy di sicurezza dei certificati di Firma Remota con procedura Automatica

1.3.6.1.4.1.14031.1.1.1	Manuale Operativo

INFRASTRUTTURA PKI CMD-2

Policy OID	Descrizione
1.3.6.1.4.1.14031	Stato Maggiore della Difesa - Comando per le Operazioni in Rete
1.3.6.1.4.1.14031.2	Certification Service Provider (CSP)
1.3.6.1.4.1.14031.2.1	Manuale Operativo

Policy OID	Descrizione
1.3.6.1.4.1.14031.2.1.1	OID certificato CA di Firma
1.3.6.1.4.1.14031.2.1.1.1	OID certificato OCSP CA di Firma
1.3.6.1.4.1.14031.2.1.1.2	OID certificato di Firma Utente
1.3.6.1.4.1.14031.2.1.1.3	OID certificato di Firma con limitazioni d'uso[1]
1.3.6.1.4.1.14031.2.1.1.4	OID certificato di Firma Remota per Test
1.3.6.1.4.1.14031.2.1.1.5	OID certificato di Firma Remota
1.3.6.1.4.1.14031.2.1.1.6	OID certificato di Firma Utente per Test
1.3.6.1.4.1.14031.2.1.1.7	OID certificato di Firma Automatica per Test
1.3.6.1.4.1.14031.2.1.1.8	OID certificato di Firma Automatica
1.3.6.1.4.1.14031.2.1.1.12	OID certificato di Firma eIDAS su Ate
1.3.6.1.4.1.14031.2.1.1.13	OID certificato di Firma eIDAS con limitazioni d'uso [2]
1.3.6.1.4.1.14031.2.1.1.14	OID certificato di Firma Remota eIDAS per Test
1.3.6.1.4.1.14031.2.1.1.15	OID certificato di Firma Remota eIDAS
1.3.6.1.4.1.14031.2.1.1.16	OID certificato di Firma Utente eIDAS per Test
1.3.6.1.4.1.14031.2.1.1.17	OID certificato di Firma Automatica per Test
1.3.6.1.4.1.14031.2.1.1.18	OID certificato di Firma Automatica eIDAS SGD
1.3.6.1.4.1.14031.2.1.1.19	OID certificato di Firma Automatica eIDAS COR-DIFESA
1.3.6.1.4.1.14031.2.1.1.23	OID certificato di Sigillo Digitale eIDAS

[1] Si fa presente che fino alla data del 30 Giugno 2017 è stato utilizzato l'OID 1.3.6.1.4.1.14021.2.1.1.3
[2] Si fa presente che dalla data del 1 Luglio 2017 al 22 Giugno 2020 è stato utilizzato l'OID 1.3.6.1.4.1.14021.2.1.1.13

1.3.6.1.4.1.14031.2.1.1.28	OID certificato di Sigillo Digitale AUTOREMOTE eIDAS

Policy OID	Descrizione
1.3.6.1.4.1.14031.2.1.2	OID certificato CA Autenticazione CNS
1.3.6.1.4.1.14031.2.1.2.1	OID certificato OCSP di Autenticazione CNS
1.3.6.1.4.1.14031.2.1.2.2	OID certificato Autenticazione Test
1.3.6.1.4.1.14031.2.1.2.3	OID certificato Autenticazione Utente

Policy OID	Descrizione
1.3.6.1.4.1.14031.2.1.3	OID certificato CA Time Stamping Authority - TSA
1.3.6.1.4.1.14031.2.1.3.1	OID certificate OCSP per la CA TSA
1.3.6.1.4.1.14031.2.1.3.2	OID certificato di Time Stamping Unit- TSU

5.1.3 **Generazione delle chiavi di certificazione (CA di Firma – CA Auth CNS – CA TSA)**

Policy OID	Descrizione
1.3.6.1.4.1.14031.2.1.7	OID certificato CA Time Stamping Authority eIDAS- TSA
1.3.6.1.4.1.14031.2.1.7.1	OID certificate OCSP per la CA TSA eIDAS
1.3.6.1.4.1.14031.2.1.7.2	OID certificato di Time Stamping Unit eIDAS – TSU eIDAS

Le chiavi private delle CA di Firma, CNS e TSA vengono generate nelle partizioni del modulo Hardware Security Module (HSM) durante la cerimonia di generazione delle chiavi (Key Ceremony).

Nella partizione dedicata del modulo HSM, il giorno della cerimonia, viene generata la coppia di chiavi (pubblica e privata). Per l'attivazione del modulo HSM sono necessari i codici di accesso alle partizioni ed apposite Pin Entry Device (PED-Key), "chiavi" USB contraddistinte da colori diversi (blu, rosso, nero, verde) a seconda delle funzioni che consentono di svolgere (login all'HSM, login alla partizione, gestione del dominio, sicurezza e audit).

Le chiave private delle CA sono conservate all'interno delle partizioni del modulo HSM.

5.1.4 Generazione delle chiavi di sottoscrizione

Allo scopo di garantire la protezione delle chiavi asimmetriche, il processo di generazione avviene all'interno del chip della singola *smart-card* (mod. ATe) durante il processo di *enrollment*.

5.1.5 Chiavi per applicazioni a supporto della PKI

La generazione delle chiavi asimmetriche per i certificati di autenticazione client e server per le applicazioni a supporto della PKI avviene a livello software su supporti specifici presso le stesse macchine.

5.1.6 Chiavi per marcatura temporale TSU

La chiave privata del certificato di Time Stamping Unit (TSU) è generata nella partizione dedicata del modulo HSM durante le normali operazioni di rinnovo del certificato.

5.1.7 Chiavi di firma del OCSP *Responder*

La chiave privata del certificato di firma del OCSP *Responder* è generata nella partizione dedicata del modulo HSM durante le normali operazioni di rinnovo del certificato.

5.1.8 Distribuzione delle chiavi pubbliche del certificatore ai titolari

Il Prestatore di Servi Fiduciari Qualificati (CA) possiede una coppia di chiavi (pubblica e privata) di certificazione e garantisce l'attendibilità dei certificati da lui emessi firmandoli digitalmente con la propria chiave privata di certificazione.

La chiave pubblica è contenuta nel Certificato dell'Autorità di Certificazione (Certificato di CA).

5.1.9 Hardware e software di generazione delle chiavi

Le chiavi di sottoscrizione del mod. ATe vengono generate all'interno della Carta stessa. Le chiavi della CA vengono generate sul modulo HSM, le chiavi a supporto della PKI vengono generate su dispositivi sicuri (HSM o *smartcard*).

5.1.10 Protezione delle chiavi private e Standard del dispositivo di generazione delle chiavi

L'HSM, che contiene la chiave privata della CA, è certificato CC EAL 4+. 140-1 Level 3.

Il mod. ATe, che contiene la chiave privata per la Firma Qualificata e per l'Autenticazione CNS impiega un chip con a bordo il sistema operativo *ST Safe Dive.* La *smartcard* è certificata ITSEC E4-HIGH (sia per il microchip che per il sistema operativo).

I moduli crittografici usati per conservare le chiavi private delle macchine e applicazioni a supporto della PKI sono gli HSM o *smartcard*.

5.1.11 **Estrazione della chiave privata dai dispositivi di firma**

I criteri di sicurezza adottati per le *smartcard* sono tali per cui non è praticamente possibile - allo stato attuale della tecnologia - l'estrazione della chiave privata dai dispositivi di firma.

5.1.12 **Deposito e conservazione della chiave privata**

La chiave privata della CA è generata e conservata su un supporto di memoria (token) caratteristico dell'HSM impiegato.

La chiave privata del Certificato di Firma è generata e memorizzata solo sul mod. ATe, le cui caratteristiche di sicurezza garantiscono l'impossibilità di esportarne la chiave privata.

La chiave privata delle macchine e delle applicazioni a supporto della PKI di Firma è generata e conservata nei moduli crittografici HSM ovvero sulla *smartcard* del Titolare del certificato.

5.1.13 **Backup della chiave privata**

Il Backup delle chiavi private delle CA è effettuato su un ulteriore HSM.

Il Backup della chiave privata, relativo al Certificato di Firma e di Autenticazione del mod. ATe, non esiste in quanto la chiave privata viene generata internamente al chip del mod. ATe e non è possibile estrarla.

Il Backup della chiave privata, relativo al server TSU, al server OCSP e delle applicazioni a supporto della PKI, non viene effettuato.

5.1.14 **Modalità di attivazione della chiave privata**

La chiave privata delle CA viene attivata tramite il modulo HSM specifico attraverso le chiavi (PADKey) ed i relativi codici di attivazione (PIN).

Le chiavi private per la Firma e per l'Autenticazione sono contenute nel mod. ATe.
L'attivazione della chiave privata della Firma viene eseguita dal titolare tramite l'applicativo di firma, dopo che lo stesso ha visualizzato i codici del mod. ATe (PIN/PUK) con la procedura comunicata a mezzo e-mail.

Si ribadisce che il "codice di emergenza" è valido per tutta la durata della carta, mentre il codice di visualizzazione solo una volta.
I PIN FIRMA e PIN CARTA sono diversi fra loro e vengono generati, in modo casuale, al momento della personalizzazione del mod. ATe e trasmessi in maniera univoca al Titolare dal CMS/R.A.
Al momento del rilascio, la carta viene consegnata con la firma bloccata. Per sbloccare la firma deve essere effettuata la procedura di sblocco descritta nel Manuale di Impiego del Software.

I Codici PIN e PUK vengono a conoscenza del Titolare tramite apposita procedura Web disgiuntamente al mod. ATe.

5.1.15 **Modalità di disattivazione della chiave privata**

La chiave privata delle CA viene disattivata se il Prestatore di Servizi Fiduciari Qualificati decide di interrompere l'emissione dei certificati (attraverso procedure specifiche di disattivazione).

La chiave privata relativa al Certificato di Firma del mod. ATe nella fase di attivazione viene resa inutilizzabile dopo tre tentativi errati.

5.1.16 **Modalità di distruzione della chiave privata**

Alla scadenza di validità del certificato inserito nel mod. ATe, la *smartcard* deve essere distrutta a mezzo rottura del microchip. Il verbale di distruzione deve essere conservato dal CMS/Registration Authority.

Per quanto attiene alle altre chiavi private (CA Firma, CA CNS, CA-TSA, TSU, OCSP e applicazioni a supporto della PKI) il modulo specifico effettua una cancellazione della stessa.

5.1.17 **Archiviazione delle chiavi pubbliche**

La chiave pubblica è conservata all'interno del certificato e quindi la sua archiviazione avviene con la pubblicazione del relativo certificato sulla Directory LDAP raggiungibile all'indirizzo: ldap://ldappkiff.difesa.it.

5.2 **Tipologie e modalità di emissione dei certificati**

5.2.1 **Tipologia**

I Certificati generati dal servizio di certificazione in questione appartengono alle seguenti tipologie:

- Certificato di CA di Firma;
- Certificato di CA Autenticazione CNS;

- Certificato di CA-TSA;
- Certificato di firma digitale utente;
- Certificato di autenticazione CNS utente;
- Certificato di marcatura temporale TSU;
- Certificato di firma del OCSP;
- Certificati per applicazioni a supporto della PKI.

5.2.2 **Modalità di emissione del certificato di Certificazione delle CA**

L'operazione di inizializzazione delle CA (Firma – CMS e TSA) prevede la generazione della coppia di chiavi (pubblica e privata) tramite il modulo HSM, la creazione della richiesta di certificato e l'emissione del certificato di CA in modalità *Self-signed*.

5.2.3 **Modalità di emissione del certificato di Marca Temporale (TSU)**

L'operazione prevede la generazione della coppia di chiavi (pubblica e privata) tramite il modulo HSM della TSU, la generazione della richiesta di certificato firmata con la stessa chiave privata, secondo lo standard PKCS#10 e l'invio della richiesta (PKCS#10) alla CA-TSA per la generazione del certificato di firma temporale Time Stamping Unit (TSU)

5.2.4 **Modalità di emissione del certificato di firma del OCSP *Responder***

L'operazione prevede la generazione della coppia di chiavi (pubblica e privata) tramite il modulo HSM del server OCSP, la generazione della richiesta di certificato firmata con la stessa chiave privata secondo lo standard PKCS#10 e l'invio della richiesta (PKCS#10) alla CA per la generazione del certificato di firma del OCSP *Responder*.

5.2.5 **Modalità di emissione dei certificati di Firma digitale**

Un'apposita applicazione presente presso il CMS (R.A.), contestualmente alla generazione della coppia di chiavi (pubblica e privata), crea la richiesta di certificazione, firmata digitalmente con la stessa chiave privata secondo lo standard PKCS#10. Prima dell'invio alla CA, la postazione CMS genera un file secondo lo standard PKCS#7, contenente il PKCS#10, e lo firma con la sua chiave privata. Il PKCS#7 viene inoltrato alla CA che verifica la firma ed il mittente e sottopone il PKCS#10 alla generazione del certificato. A questo punto la CA restituisce il certificato firmato al CMS che dopo aver eseguito la verifica della firma e del certificato lo inserisce nel mod. ATe.

5.2.6 **Modalità di emissione dei certificati delle applicazioni a supporto della PKI di Firma**

Un'apposita applicazione presente presso il CMS, contestualmente alla generazione delle chiavi (pubblica e privata), crea la richiesta di certificazione PKCS#10, firmata digitalmente con la chiave privata dell'applicazione a supporto della PKI. Tale richiesta viene inoltrata alla CA che rilascia lo specifico certificato.

5.3 Codici assegnati al titolare di un mod. ATe

Il Titolare dei certificati contenuti all'interno della carta riceverà i codici necessari per l'utilizzo della stessa, in particolare:

- **PIN Carta/Autenticazione CNS**: da utilizzare per abilitare l'accesso al mod. ATe ed ai processi applicativi che richiedono l'esecuzione delle operazioni di autenticazione;
- **PUK Carta/Autenticazione CNS**: da utilizzare per lo sblocco del PIN Carta (avvenuto dopo 3 tentativi errati di inserimento del PIN, dopo 10 inserimenti errati del codice PUK l'accesso alla carta viene bloccato definitivamente);
- **PIN di Firma**: da utilizzare per abilitare l'accesso ai processi applicativi che richiedono l'esecuzione delle operazioni di Firma qualificata;
- **PUK di Firma**: da utilizzare per lo sblocco del PIN di Firma (avvenuto dopo 3 tentativi errati di inserimento del PIN, dopo 10 inserimento errati del codice PUK la firma viene bloccata definitivamente)

Il Titolare riceverà inoltre un **CODICE DI EMERGENZA** da utilizzare in caso di richiesta telefonica di sospensione.

5.4 Periodi di validità delle chiavi e dei relativi certificati

A seconda delle tipologie delle coppie di chiavi è prevista una diversa frequenza nella sostituzione delle chiavi e nella validità dei relativi certificati. Da notare che la sostituzione di una coppia di chiavi con una nuova non implica necessariamente la perdita di validità del certificato relativo alla coppia sostituita. In particolare:

- Le chiavi di certificazione vengono sostituite con cadenza ventennale, mentre i relativi certificati hanno una validità temporale di **30 anni**;
- Le chiavi di marcatura temporale vengono sostituite con cadenza non superiore a tre mesi mentre i relativi certificati hanno validità temporale di **5 anni**;
- Le chiavi di firma del OCSP *Responder* vengono sostituite con cadenza non superiore a due anni mentre i relativi certificati hanno una validità temporale di **5 anni**;
- Le chiavi di firma digitale e autenticazione CNS sono sostituite contestualmente al rinnovo dei relativi certificati e/o dei mod. ATe ed hanno un periodo di validità di **10 anni**;
- Le chiavi delle **applicazioni** a supporto della CA sono sostituite contestualmente al rinnovo dei relativi certificati ed hanno un periodo di validità di **5 anni**.

5.5 Modalità di sospensione e revoca dei certificati

5.5.1 Generalità

Il mod. ATe, in quanto "carta valori" dello Stato e tessera di riconoscimento personale (ai sensi del Decreto del Presidente del Consiglio 24 maggio 2010), deve essere oggetto della massima attenzione da parte del Titolare. Essa è una carta "elettronica" e la sua validità è fondata sull'efficienza del chip e sulla legittimità dei dati memorizzati oltre che di quelli serigrafati sul supporto plastico. Nel chip sono memorizzati tre certificati primari: uno relativo alla "Firma digitale", uno di "autenticazione CNS" del titolare e l'altro di "cifratura". Mentre il processo di sospensione/revoca dei certificati di firma e di cifra non inficia la validità della carta, che continua nella sua funzione di riconoscimento del Titolare, la sospensione/revoca del certificato di autenticazione CNS annulla l'efficacia della carta che dovrà essere riemessa con nuovi certificati. Pertanto le procedure di sospensione/revoca del mod. ATe sono da riferirsi alla validità dei certificati ivi contenuti.

5.5.2 Sospensione dei certificati

Cause di sospensione possono essere:

- furto/smarrimento della carta (previa denuncia all'Autorità Giudiziaria);
- compromissione/perdita dei codici PIN e PUK;
- inefficienza del chip;

ogni altro motivo che possa dare adito ad un uso improprio della carta.

5.5.3 Procedure per la sospensione di un certificato

La richiesta di sospensione è presentata, di norma, personalmente dal Titolare presso una qualunque Local Registration Authority (LRA) o, in alternativa, via WEB o telefonicamente al Call Center n. 064691444 comunicando il proprio "CODICE DI EMERGENZA" e presentando successivamente una motivata richiesta scritta. La LRA nella figura del Funzionario Autorizzato alla validazione dei dati, provvederà a far pervenire la richiesta al CMS Unico (RA).
La LRA ed il CMS possono, ove ne ricorrano giustificati motivi, procedere autonomamente alla procedura di sospensione dandone notizia e motivazione al Titolare.
La sospensione di un certificato ha una durata limitata nel tempo (definita dal Prestatore di Servizi Fiduciari Qualificati), dopodiché, ove non siano cessate le condizioni di sospensione, si procede alla sua revoca. Il Prestatore di Servizi Fiduciari Qualificati provvederà a tenere aggiornata una lista pubblica dei certificati sospesi (CRL).

5.5.4 Riattivazione di un certificato sospeso

Il Funzionario Autorizzato alla validazione di dati, dopo aver appurato il venir meno delle motivazioni che hanno determinato la sospensione, informerà il CMS/RA indicando gli estremi della carta (numero seriale, cognome, nome). Successivamente, riceverà comunicazione della avvenuta riattivazione da parte del CMS/RA.

5.5.5 **Revoca di un certificato**

Un Certificato si può revocare per uno dei seguenti motivi:

- compromissione o sospetta compromissione della relativa chiave privata;
- cambio di almeno uno dei dati pubblicati nel certificato o dati errati;
- il Titolare ha violato apertamente i suoi obblighi relativi alla titolarità del certificato;
- smarrimento o distruzione del dispositivo che contiene la relativa chiave privata (mod. ATe).

5.5.6 **Procedure per la revoca di un certificato**

La richiesta di revoca è presentata, di norma, personalmente dal Titolare presso una qualunque Local Registration Authority (LRA) o, in alternativa, via WEB o telefonicamente alla LRA di competenza, comunicando il proprio "Codice di Emergenza" e presentando successivamente una motivata richiesta scritta. La LRA nella figura del Funzionario Autorizzato alla validazione dei dati, provvederà a far pervenire la richiesta al CMS Unico (RA).
La LRA ed il CMS possono, ove ne ricorrano giustificati motivi, procedere autonomamente alla procedura di revoca dandone notizia e motivazione al Titolare.
Il Certificatore provvederà a tenere aggiornata una lista pubblica dei certificati revocati (CRL).

5.5.7 **Aggiornamento delle CRL (Certificate Revocation List)**

La CRL è pubblicata immediatamente a seguito di una sospensione, riattivazione o revoca per compromissione di un certificato. Diversamente la pubblicazione della CRL avviene almeno ogni 24 ore con una validità temporale di 7 giorni.

5.6 **Modalità di sostituzione delle chiavi e rinnovo dei certificati**

Per la sostituzione delle coppie di chiavi e per il conseguente rinnovo dei certificati il Prestatore di Servizi Fiduciari Qualificati prevede determinate procedure che, a partire dalla generazione delle nuove coppie di chiavi, permettono la generazione e pubblicazione dei nuovi corrispondenti certificati, pur mantenendo, in alcuni casi, la validità di quelli precedenti.

5.6.1 **Sostituzione delle chiavi di certificazione e rinnovo dei relativi certificati**

In considerazione della data di scadenza del certificato di certificazione e della durata dei certificati di sottoscrizione emessi, il Prestatore di Servizi Fiduciari Qualificati procede alla sostituzione delle chiavi di certificazione mediante:

- Generazione di una nuove coppia di chiavi di certificazione;
- Generazione e pubblicazione del relativo certificato, sottoscritto con la chiave privata della coppia appena generata;

Generazione e pubblicazione, nel Registro dei Certificati, di un certificato relativo alla nuova chiave pubblica sottoscritto con la chiave privata della vecchia coppia ed un certificato relativo alla vecchia chiave pubblica sottoscritto con la nuova chiave privata.

5.6.2 **Rinnovo dei certificati di marcatura temporale**

La procedura prevede la:

- Generazione di una nuova coppia di chiavi di marcatura temporale da parte della TSU;
- Generazione da parte della CA-TSA del certificato relativo alla nuova chiave di marcatura temporale e pubblicazione nel Registro dei Certificati.

5.6.3 **Rinnovo dei certificati di firma del OCSP *Responder***

La procedura prevede la:

- Generazione di una nuova coppia di chiavi da parte del OCSP *Responder* all'interno del HSM;
- Generazione da parte della CA del certificato relativo alle nuove chiavi e pubblicazione nel Registro dei Certificati.

5.6.4 **Rinnovo dei certificati dei titolari**

Il servizio di certificazione non prevede al momento la possibilità per i Titolari di rinnovare tramite procedure on-line i certificati qualificati.

Il servizio di certificazione, per il tramite del CMS Unico (RA), provvede ad inviare una mail al Titolare del Certificato avvisandolo dell'approssimarsi della scadenza dei certificati.

Contestualmente deve essere effettuata richiesta di emissione del nuovo mod.ATe con le metodologie già evidenziate nei capitoli precedenti.

Alla ricezione della nuovo mod.ATe, il Funzionario Autorizzato alla validazione dei dati della LRA dovrà:

- *convocare il Titolare della nuova carta;*
- *consegnare al Titolare la nuova carta e ritirare contestualmente la vecchia carta;*

- *restituire al CMS/RA la carta ritirata.*

5.7 Modalità di gestione del registro dei certificati

Il registro dei certificati è la componente del servizio di certificazione deputata alla conservazione ed alla pubblicazione dei certificati digitali emessi, di qualsiasi tipologia, dalle varie CA (Firma – CNS – TSA).

Il Registro viene implementato su idonei sistemi e configurato in modo da consentire la presenza di una copia di riferimento protetta ed una copia disponibile per l'accesso, mediante il protocollo LDAP (Lightweight Directory Access Protocol).

L'art 34 del DPCM 22 febbraio 2013 specifica che tutti i certificati sospesi o revocati **devono** essere resi pubblici mentre i certificati attivi **possono** essere resi pubblici solo su esplicita richiesta del Titolare del Certificato.

5.7.1 Informazioni contenute del registro dei certificati

Nel Registro dei Certificati vengono custoditi:

- tutti i certificati emessi dal servizio di certificazione;
- la lista aggiornata dei certificati revocati/sospesi (CRL);
- il generico certificato o la generica CRL.

5.7.2 Procedura di gestione del registro dei certificati

Il Registro dei Certificati è implementato mediante un sistema di LDAP conforme allo standard ITU-T X-500, su due sistemi di server distinti e costituenti la copia di riferimento protetta e la copia operativa di consultazione del registro stesso.

La copia di riferimento è mantenuta in locali protetti ed installata su una parte di rete protetta inaccessibile da utenti esterni. La copia operativa è invece installata su una parte di rete accessibile a tutti gli utenti della intranet DIFENET.

Periodicamente avviene il confronto e la sincronizzazione tra le due copie. Ogni discordanza viene annotata sul Giornale di Controllo.

Tutte le modifiche al contenuto del Registro dei Certificati, effettuate esclusivamente da personale autorizzato, sono registrate sul Giornale di Controllo.

La data e l'ora di inizio e fine di ogni intervallo di tempo durante il quale il Registro dei Certificati non risulta accessibile, nonché quelle relative a ogni intervallo di tempo durante il quale una funzionalità interna al Registro non risulta disponibile, sono annotate sul Giornale di Controllo.

I sistemi deputati alla generazione dei certificati e delle CRL provvedono automaticamente ad aggiornare il registro dei Certificati depositando:

- I nuovi certificati emessi;
- Le nuove CRL emesse a seguito di nuove revoche/sospensioni.

5.7.3 Modalità di accesso al registro dei certificati

Conformemente alla normativa in vigore, l'accesso al Registro dei Certificati, costituito da sistemi di directory X.500 avviene mediante protocollo LDAP conforme alla specifica RFC 1777.
Tale accesso è consentito mediante:

- Configurazione delle funzionalità LDAP, presenti in specifici applicativi, dell'indirizzo: ldappkiff.difesa.it:389

L'accesso al Registro dei Certificati (limitatamente a quelli sospesi e/o revocati o attivi ma con pubblicazione richiesta da parte del Titolare) è disponibile H-24.

5.8 Giornale di controllo

Tutte le registrazioni effettuate automaticamente dagli stessi sistemi e relative alle operazioni eseguite nei sistemi del servizio di Certificazione per l'erogazione dei servizi di certificazione costituiscono, nel loro complesso, il Giornale di Controllo.

5.8.1 Registrazione sul giornale di controllo

Nel Giornale di Controllo sono effettuate le seguenti registrazioni:

- Generazione dei certificati, siano essi relativi a chiavi di firma qualificata che a chiavi di certificazione o di firma temporale;
- Revoca dei certificati emessi;
- Sospensione dei certificati emessi;
- Entrata ed uscita dai locali protetti del sistema di generazione dei certificati;
- Inizio e fine di ciascuna sessione di lavoro inerente alla generazione dei certificati;
- Tutte le operazioni di modifica del contenuto del Registro dei Certificati, ossia l'aggiornamento delle liste di revoca/sospensione e la pubblicazione dei certificati generati;
- Data e ora d'inizio e fine di ogni intervallo di tempo durante il quale il Registro dei Certificati non risulta accessibile, nonché quelle relative a ogni intervallo di tempo durante il quale una funzionalità interna al Registro non risulta disponibile.

Tutte le registrazioni riportano l'ora e la data di esecuzione dei relativi processi, nonché l'identificativo dell'operatore che li ha avviati.

5.8.2 **Conservazione dei dati**

Le registrazioni di cui al paragrafo precedente vengono riportate dai sistemi nei quali avvengono i relativi processi in appositi "file di log". Questi vengono, a scadenze prestabilite:

- Firmati digitalmente dal Responsabile della conduzione tecnica dei sistemi;
- Sottoposti a marcatura temporale;
- Memorizzati su supporti certificati per la lunga conservazione, non modificabili e accessibili unicamente al personale del Centro di Certificazione PKI Difesa;
- Sottoposti a periodici controlli da parte del Responsabile della Sicurezza.

Tali supporti vengono conservati e custoditi per un periodo di 20 anni. La loro consultazione consente la ricostruzione, con la necessaria accuratezza, di tutti gli eventi rilevanti ai fini della sicurezza. La marcatura temporale e la firma digitale del Responsabile della conduzione tecnica dei sistemi garantisce nel tempo l'integrità delle annotazioni riportate.

5.8.3 **Verifiche**

L'integrità del Giornale di controllo è verificato con frequenza mensile.

5.9 **Modalità di protezione della riservatezza**

Il servizio di certificazione garantisce la protezione della riservatezza dei dati relativi agli utenti dei propri servizi. In particolare:

- Tutti i dati residenti sui sistemi tecnologici del servizio di certificazione sono memorizzati in database sicuri. Il trattamento dei dati, in modalità di visualizzazione e di modifica, è consentita unicamente ai processi eseguiti da operatori autorizzati, che accedono ai sistemi mediante processi di autenticazione, sulla base di ben definite politiche di sicurezza.
- I dati riportati sui moduli elettronici e sulle stampe riepilogative dei dati necessari per emettere il mod. ATe dei Titolari, sono custoditi in armadi sicuri (presso le RA/LRA) e sono consultabili sono dal personale autorizzato al loro trattamento.

Le misure di protezione adottate sono conformi alle misure minime di sicurezza per il trattamento dei dati personali.

5.10 **Procedure di gestione delle copie di sicurezza**

Al fine di consentire il ripristino del servizio a seguito di malfunzionamenti o indisponibilità temporanea o permanente dei propri sistemi, il servizio di certificazione prevede l'esecuzione di apposite procedure finalizzate a generare e custodire, su supporti di memorizzazione esterni, le copie di sicurezza dei dati contenuti nei propri database e del Registro dei Certificati.

5.11 **Servizio di marcatura temporale**

Il servizio di certificazione rende disponibile un servizio di marcatura temporale mediante il quale i Titolari di certificati di sottoscrizione possono richiedere il rilascio di marche temporali associate a documenti elettronici.

Il riferimento temporale utilizzato per la generazione delle marche temporali è ottenuto mediante l'utilizzo di un sistema in grado di rilevare il Tempo Universale Coordinato (UTC). L'ora assegnata alle marche temporali corrisponde al momento della sua rilevazione, con una differenza non superiore al 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 generazione delle marche temporali è ottenuta mediante un'operazione di sottoscrizione digitale, eseguita con una chiave di marcatura temporale, di una struttura dati contenente le seguenti informazioni:

- Identificativo dell'emittente;
- Algoritmo utilizzato per la sottoscrizione della marca temporale;
- Identificativo del certificato relativo alla chiave di verifica della marca temporale;
- Data e ora di generazione della marca temporale;
- Identificativo dell'algoritmo di HASH utilizzato per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale;
- Valore dell'impronta dell'evidenza informatica.

Le chiavi di marcatura temporale vengono generate all'interno di un apposito dispositivo crittografico del tipo HSM. Tali chiavi, univocamente associate al dispositivo HSM, vengono sostituite con cadenza non superiore a tre mesi e senza revocare il corrispondente certificato.

L'associazione di una marca temporale a documenti informatici sottoscritti digitalmente consente di prolungare la loro validità oltre il periodo di validità del certificato associato alle chiavi private con le quali sono stati sottoscritti. A tal fine, il Certificatore conserva copia delle marche generate per un periodo non inferiore a 20 anni.

L'associazione di una marca temporale ad un documento informatico garantisce la validità del documento anche in caso di compromissione della chiave di sottoscrizione, purché la marca temporale sia stata generata antecedentemente a tale evento.

5.12 **Servizio OCSP**

Il servizio di certificazione rende disponibile un servizio OCSP autoritativo per la verifica dei certificati emessi dalla infrastruttura PKI del Ministero della Difesa.

Tale servizio consente, in fase di verifica di un documento firmato digitalmente o di un certificato di autenticazione CNS, di controllare lo stato di validità del certificato utilizzato.

A differenza delle CRL il servizio OCSP fornisce informazioni esclusivamente sulla validità del certificato di cui è stato richiesto il controllo senza che l'Utente richiedente debba mantenere localmente, nel proprio software di verifica, una copia delle CRL.

Per tali motivi il Servizio OCSP elimina i problemi di latenza che spesso si verificano con le CRL di grosse dimensioni e che ne impediscono il normale download e successivo controllo.

Le informazioni sullo stato del certificato sono firmate digitalmente e vengono comunicate all'Utente richiedente attraverso il protocollo HTTP.
L'OCSP *Responder* comunica che il certificato indicato nella richiesta è 'good', 'revoked' o 'unknown' e comunica un codice di errore se non riesce a processare la richiesta.
Le chiavi di firma utilizzate per la firma digitale delle informazioni rese dal OCSP *Responder* vengono generate all'interno di un dispositivo crittografico del tipo HSM (Hardware Security Module) e sostituite con cadenza biennale e senza revocare il corrispondente certificato.

5.13 Sistema di generazione e verifica della firma digitale

Per garantire la rispondenza della procedura di firma e verifica di un documento alla normativa vigente è necessario utilizzare l'applicazione fornita dalla Difesa che, oltre alle funzioni di seguito descritte, consente di eseguire la procedura di sblocco della carta a garanzia del titolare (per dettagli sulla procedura fare riferimento al manuale utente).

L'applicazione è in grado di gestire, sia in fase di firma che in fase di verifica, i seguenti formati:

- ***CAdES*** (documenti firmati secondo le norme europee)
- ***CAdES-T*** (documenti firmati e inclusivi di marche temporali sulla firma)
- **PAdES** (firma incorporata in un documento formato "pdf")
- **XAdES (**firma di un documento in formato "xml")
- ***TSD*** (documenti Time Stamped Data)
- ***TSR*** (marche temporali Time Stamp Response)
- ***TST*** (marche temporali Time Stamp Token)
- ***ASiC*** (Associated Signature Containrs)

In riferimento al formato ASiC il Kit di Firma supporta i formati:

- In fase di generazione: ***ASiC-E CAdES*** e ***ASiC-E TST***
- In fase di verifica***: ASiC-E CAdES, ASiC-E XAdES, ASiC-E TST, ASiC-S CAdES, ASiC-S XAdES, ASiC-S TST***

5.14 Cessazione dell'attività del Prestatore di Servi Fiduciari Qualificati

Il Prestatore di Servizi Fiduciari Qualificati qualora intenda cessare l'attività deve, almeno sessanta giorni prima della data di cessazione, darne avviso ad Ag.ID. ed informare senza indugio i titolari dei certificati da lui emessi specificando che tutti i certificati non scaduti al momento della cessazione saranno revocati.

Il Prestatore di Servizi Fiduciari Qualificati comunica contestualmente la rilevazione della documentazione da parte di altro Prestatore di Servizi Fiduciari Qualificati o l'annullamento della stessa (l'indicazione di un Prestatore di Servizi Fiduciari sostitutivo evita la revoca dei certificati e della relativa documentazione). Il Prestatore di Servizi Fiduciari Qualificati indica altro depositario del registro dei certificati e della relativa documentazione [DLGS 82/2005 e s.m.i.].

6 CONTATTI UTILI E NUMERI DI EMERGENZA

Certification Authority

Tel. Linea Militare: 202454/1-2-3-4-5

Tel. Linea Civile: 06-4691454/1-2-3-4-5

Email: info_pkiff@smd.difesa.it

Registration Authority

Tel. Linea Militare: 102.5040

Tel. Linea Civile: 06-32355396

Email: ate@esercito.difesa.it

Sito Web: www.pki.difesa.it

https://pki.difesa.it/tsp/

Call center Comando per le Operazioni in Rete

Tel. Linea Militare: 2024444

Tel. Linea Civile: 06-46914444

In caso di contatto telefonico, assicurarsi di avere disponibile il "CODICE DI EMERGENZA" necessario per l'identificazione certa del chiamante.