STATO MAGGIORE DELLA DIFESA

Comando C4 Difesa

“PKI di Firma qualificata ”

Manuale Operativo

Approvato da: **Generale di Brigata**
Umberto Maria CASTELLI
Comandante del Comando C4 Difesa

CASTELLI UMBERTO MARIA

Firmato digitalmente da CASTELLI UMBERTO MARIA
ND: c=IT, o=Ministero della Difesa/97355240587, ou=Esercito, ou=SIGE, sn=CASTELLI, givenName=UMBERTO MARIA, serialNumber=IT:CSTMRT60M08B474Y, dnQualifier=AA0184166, cn=CASTELLI UMBERTO MARIA
Data: 2014.02.27 09:02:30 +01'00'

VERSIONE DOCUMENTO	**4.0**

Compilato da:	**1° Mar. Lgt. Michele FATO**
Revisionato da:	**C.F. Giuseppe NOCE**
Approvato da:	**Gen.B. Umberto Maria CASTELLI**

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 *Time Stamp 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	Quarto rilascio a seguito: - istallazione 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	19/04/2012

	5.5 5.8.3 5.14 5.15.2	Responder; - Rinnovo dei certificati di firma del OCSP responder; - Servizio OCSP - Il Servizio OCSP in fase di verifica della firma	
Versione 4.1	_____	- Aggiornamento al DPCM 22 febbraio 2013 - Cambio Certificatore	06/09/2013
Versione 4.2	5.2.2 6	- Inserito OID di Firma Remota con procedura Automatica - Appendici	20/02/2014

Indice

1 PREMESSA

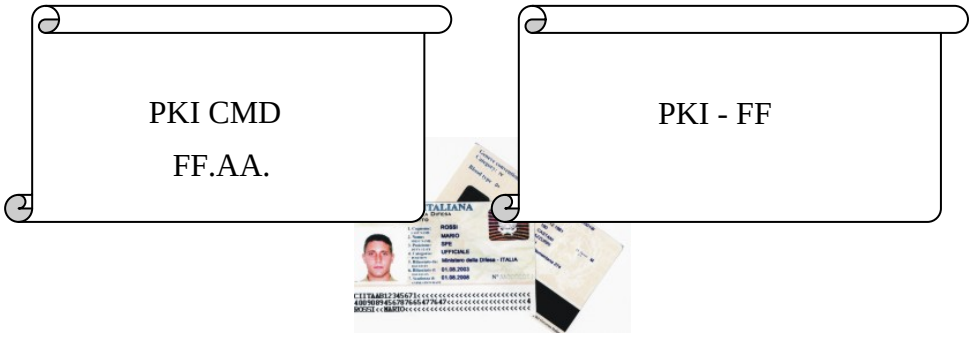
Il presente documento descrive l'organizzazione messa in atto dallo Stato Maggiore della Difesa - Comando C4 Difesa nell'esercizio delle funzioni di Certificatore accreditato presso DigitPA al rilascio di certificati di firma qualificata. Inoltre lo stesso documento descrive i processi necessari per la generazione, la pubblicazione, la sospensione e la revoca dei certificati.

L'elemento a supporto della PKI-FF-Difesa è la Carta Multiservizi della Difesa (CMD), una smartcard che contiene i certificati digitali e le relative coppie di chiavi dei titolari. Ai sensi del DPCM - 24 maggio 2010 - G.U. n. 182 del 06/08/2010, la CMD ha inoltre valore di tessera di riconoscimento**.**

Ai fini dell'acquisizione dei dati, necessari per l'emissione dei certificati di Firma qualificata, la PKI-FF utilizza il circuito di emissione della CMD. Attraverso tale circuito vengono inoltre rilasciati certificati di autenticazione e cifra, prodotti dalla PKI CMD.

Pertanto in ambito difesa sono operative due PKI: la PKI-CMD-FF.AA., per l'emissione di certificati di Autenticazione e Cifra e la PKI-FF-Difesa per il rilascio di certificati di Firma qualificata.

I certificati sopra citati e le relative chiavi vengono archiviati all'interno di un comune supporto (CMD) e gestiti con le modalità previste dalle norme in materia.



2 GENERALITA'

2.1 Scopo del documento

Il Manuale Operativo illustra le procedure, le regole ed i criteri di tipo tecnico, organizzativo e operativo tramite i quali il Ministero della Difesa nella figura dello Stato Maggiore della Difesa – Comando C4 Difesa (di seguito definito **Certificatore**) offre, avvalendosi di un centro tecnico denominato **Centro di Certificazione**, il servizio di certificazione di chiavi pubbliche denominato **PKI-FF-Difesa**.

2.2 Riferimenti alle norme di legge

[DPR445] Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445, "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", pubblicato sul Supplemento Ordinario alla Gazzetta Ufficiale n. 42 del 20 febbraio 2001.

[DPCM2009] Decreto del Presidente del Consiglio dei Ministri (DPCM) 30 marzo 2009, "Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici", pubblicato sulla Gazzetta Ufficiale n.129 del 6 giugno 2009.

[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).

[DLGS196] Decreto Legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", pubblicato nel Supplemento Ordinario n.123 della Gazzetta Ufficiale n. 174, 29 luglio 2003.

[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.

2.3 Riferimenti agli standard

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

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

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

[SHA1] ISO/IEC 10118-3:1998, "Information technology - Security techniques - 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.

2.4 Glossario

Applicazione del Certificatore: è la parte dell’applicazione WEB, mediante la quale il Certificatore, o il responsabile periferico, 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.

Carta Multiservizi della Difesa (CMD): è la smartcard rilasciata al personale Militare e Civile dell’ Amministrazione della Difesa (A.D.) che contiene, tra l’altro, i certificati digitali e le chiavi pubbliche e private.

Centro di Certificazione: è il centro che include il personale, i materiali e le procedure per l'erogazione dei servizi di certificazione.

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 associata la corrispondente chiave privata appartenente solo al Titolare medesimo (l'associazione chiave pubblica chiave privata è univoca).

Certificatore: 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 di 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 ed il soggetto Titolare cui essa appartiene, 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 o 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 o 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: è la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (con applicabilità da definirsi).

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 Certificatore.

Firma digitale: il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario 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.

Infrastruttura chiave pubblica (PKI-FF): 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.

Lista dei Certificati Sospesi (CSL): è la lista firmata digitalmente, tenuta ed aggiornata dal Certificatore, contenente i certificati emessi dallo stesso e successivamente sospesi. La sospensione ha carattere provvisorio.

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

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 militare necessari per l'emissione della CMD.

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 la CMD ed i relativi certificati.

Registro dei Certificati: è il sistema informatico sul quale sono immagazzinati i certificati emessi, revocati e sospesi ed è accessibile a qualsiasi soggetto attestato sulla rete INTERNET/DIFENET.

Responsabile Periferico: è il soggetto deputato, presso un generico Ente/Unità dell'Organizzazione di Forza Armata, alla identificazione dei soggetti, per i quali si intende rilasciare le CMD, 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 con un Ufficiale da lui delegato.

Responsabile per il trattamento 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. Il Responsabile per il Trattamento 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 sulla CMD.

Servizi di Certificazione: sono, nel loro insieme, i servizi forniti dal Centro di Certificazione. 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.

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

Smart-card: tessera, di formato simile al Bancomat, dotata di 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**.

Trust Center: luoghi con particolari caratteristiche di sicurezza fisica ed organizzativa dove vengono rilasciate le CMD.

Utenti dei servizi di certificazione: sono i soggetti che, in qualità di Titolari di certificati o di Utilizzatori dei certificati, accedono ai servizi resi dai servizi messi a disposizione per la CMD.

Utilizzatore: è il soggetto che accede agli archivi mantenuti dal Certificatore per richiedere e verificare 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.

3 INTRODUZIONE

3.1 Dati identificativi del certificatore

L'infrastruttura di PKI di Firma Qualificata della Difesa è ubicata presso il Comando C4 Difesa sito in via Stresa 31b, 00135 Roma.

L'infrastruttura per il Disaster Recovery della PKI di Firma Qualificata è ubicata presso il Re.S.I.A (Reparto Sistemi Informativi Automatizzati - dell'Aeronautica Militare) Acquasanta sito in via Appia Pignatelli 123, 00178 Roma. Tale infrastruttura non è organizzata al fine di fornire un servizio di **"business continuity"** ma sarà attivata in caso di necessità ed allineata alla struttura principale grazie ad un servizio di backup periodico dei dati.

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

STATO MAGGIORE DELLA DIFESA

COMANDO C4 DIFESA

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 C4 DIFESA

Centro di Certificazione

Via Stresa, 31 B

00135 ROMA

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

- Indirizzo e-mail: **info_pkiff@smd.difesa.it**

- 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**
- Sito web (intranet): **http://c4d.difesa.it/Sicurezza/PKI-Firma-Digitale/Pagine/default.aspx**

3.2 Versione del manuale operativo

La versione del presente Manuale Operativo è identificata dalla sigla: **Manuale Operativo v 4.0 - 1.3.6.1.4.1.14031.1.1.1**.

Questo documento è pubblicato sul sito web del servizio di certificazione http://www.pkiff.difesa.it ed è quindi consultabile telematicamente ai sensi dell'art. 40, comma 2, del [DPCM_22-02-2013].
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 AgID (Agenzia per l'Italia Digitale) (www.digitpa.gov.it). In ogni caso, farà fede la versione pubblicata sul sito web di AgID.
Il documento è inoltre pubblicato in formato **PAdES**, in modo da assicurarne l'origine e l'integrità.

3.3 Responsabile del manuale operativo

Il responsabile del presente Manuale Operativo è lo Stato Maggiore della Difesa - Comando C4 Difesa, che si avvale per la sua redazione integrale del dipendente Centro di Certificazione.

4 DISPOSIZIONI GENERALI

4.1 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].

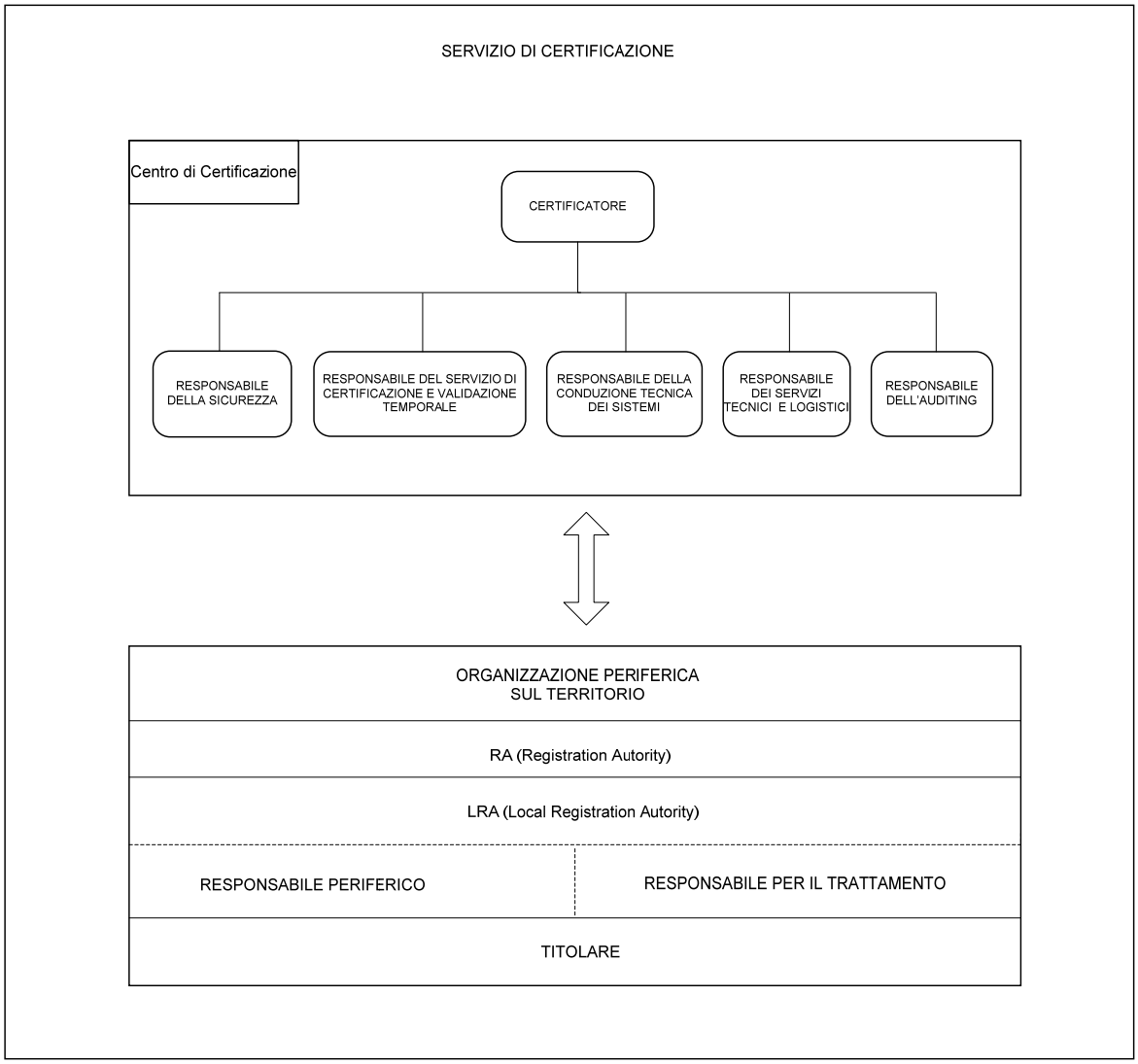
Per le funzionalità organizzative del servizio di certificazione, il Responsabile delle verifiche e delle ispezioni (auditing) è anche **"Capo del Centro di Certificazione"** e risponde al Certificatore,

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:

- Responsabile Periferico (figura professionale presso l'Ente che richiede l'emissione del certificato di firma qualificata per il Titolare).
- Responsabile per il Trattamento (figura professionale presso l'Ente che coadiuva il futuro titolare del certificato nella fase di presentazione dei dati necessari al rilascio del certificato stesso ed è responsabile della corretta identificazione del futuro titolare).
- Titolare (soggetto al quale è rilasciato il certificato di firma qualificata da parte del Certificatore)
- Utilizzatore (una qualsiasi entità, figurata o reale, che fa uso di un certificato di firma qualificata per verificare la validità della firma digitale)

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



4.2 Definizione degli obblighi del Certificatore, dei Responsabili Periferici, dei Responsabili per il Trattamento, dei Titolari e degli Utilizzatori

4.2.1 Obblighi del Certificatore

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

1. adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri (art. 32, comma 2, DL 82/2005 e successive modificazioni);

2. identificare la persona che fa richiesta della registrazione ai fini della certificazione (art. 32, comma 3, lett. A, DL 82/2005);
3. comunicare ad AgID 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, DL 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, DL 82/2005 e successive modificazioni;
5. accertare l'autenticità delle richieste di certificazione (art. 18, comma 1, lett. a), DPCM 22-02-2013);
6. attenersi 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 [(DLGS 196/2003), (art. 32, comma 5, DL 82/2005)];
7. 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, DL 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, lett. f, DPR 82/2005 e successive modificazioni);
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, DPR 82/2005 e successive modificazioni;
7. comunicare per iscritto ad AgID ogni variazione significativa delle soluzioni tecnico-organizzative da adottare (Circolare CNIPA/CR/48, 6 settembre 2005);
8. comunicare tempestivamente ad AgID 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 Responsabile

Periferico 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).

4.2.2 Obblighi del Responsabile Periferico

Il Responsabile Periferico che abbia tra i suoi dipendenti dei Titolari di certificati deve:

1. valutare l'opportunità o la necessità, sulla base delle normative vigenti in ambito A.D., 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 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.

4.2.3 Obblighi del Responsabile per il Trattamento

Il Responsabile per il Trattamento 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 Responsabile Periferico.

4.2.4 Obblighi del Titolare del certificato

Il Titolare del Certificato deve:

1. fornire tutte le informazioni necessarie al Responsabile per il Trattamento/Responsabile Periferico garantendone, sotto la propria responsabilità, l'attendibilità ai sensi della legge n. 15 del 1968 e successive modifiche ed integrazioni;
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);

4.2.5 Obblighi dell' Utilizzatore del certificato

L'utilizzatore del Certificato per accertare in modo inconfutabile la *"non repudiabilità"* 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 applicativi le cui case produttrici ne dichiarano espressamente la conformità alla normativa vigente in materia di firma elettronica qualificata/firma digitale .

4.3 Definizione delle responsabilità del Certificatore, dei Responsabili Periferici, dei Responsabili per il Trattamento, dei Titolari e degli Utilizzatori.

Nell'espletamento dei servizi di certificazione e nell'utilizzo operativo della firma qualificata, il Certificatore, il Responsabile Periferico, il Responsabile per il Trattamento, i Titolari e gli Utilizzatori hanno le responsabilità di seguito esplicitate.

4.3.1 Responsabilità del Certificatore

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

- della certa identificazione del personale destinatario di 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 fino all'atto della spedizione, in busta chiusa, ai competenti Responsabili Periferici per la consegna ai Titolari destinatari;
- 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.

4.3.2 Responsabilità del Responsabile Periferico

Il Responsabile Periferico 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 o elettronico, pervenute dal Centro di Certificazione;
- dell'immediata comunicazione al Centro di Certificazione 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.

4.3.3 Responsabilità del Responsabile per il Trattamento

Il Responsabile per il Trattamento, nominato dal Responsabile Periferico, è responsabile:

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

4.3.4 Responsabilità del Titolare del certificato

Il Titolare di un certificato per firma digitale è responsabile:

- della corretta comunicazione dei propri dati personali al Responsabile Periferico;
- della corretta custodia del dispositivo di firma e dei relativi codici di attivazione (PINCarta, PUK Carta, PIN Firma, PUK Firma). Per nessun motivo è consentito la ristampa dei codici di attivazione PIN Firma, PUK Firma;
- del corretto utilizzo del dispositivo di firma;
- della corretta applicazione delle norme e procedure di lavoro che prevedano l'impiego di firma qualificata;
- della pronta comunicazione al Responsabile Periferico di possibili malfunzionamenti riscontrati sul dispositivo di firma;
- della pronta comunicazione al Responsabile Periferico o, qualora non sia immediatamente contattabile (es. fuori orario di servizio), direttamente al servizio di certificazione 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.

4.3.5 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.

4.4 Aspetti normativi e legislativi

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

4.5 Normativa in vigore

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

Le relative norme attuative in ambito Difesa sono riportate nella direttiva SMD - I - 001 "Norme sull'impiego della firma digitale in ambito A.D." edizione 2005 e nella direttiva SMD - I - 009 "Carta Multiservizi della Difesa - Norme di gestione e di impiego" edizione 2005.

4.6 Avvisi

Il Certificatore si riserva di pubblicare sul proprio sito, all'indirizzo http://www.pkiff.difesa.it 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 AgID.

5 ASPETTI OPERATIVI

5.1 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.

5.1.1 Acquisizione dei Dati

La procedura acquisizione dei dati, il c.d. *enrollment*, avviene presso i Locali Centri di Registrazione (LRA), dislocati, ove possibile, in prossimità del Reparto/Ente del richiedente.

Il Responsabile del Trattamento (nominato dal Responsabile Periferico), effettuata l' identificazione del richiedente con un valido documento di riconoscimento, procede all'acquisizione dei dati personali, delle impronte e della foto attraverso specifiche procedure, convalida i dati con la propria firma digitale. Tale processo si conclude mediante la sottoscrizione, da parte del richiedente, di una copia cartacea dei dati raccolti e della controfirma da parte del Responsabile del Trattamento.

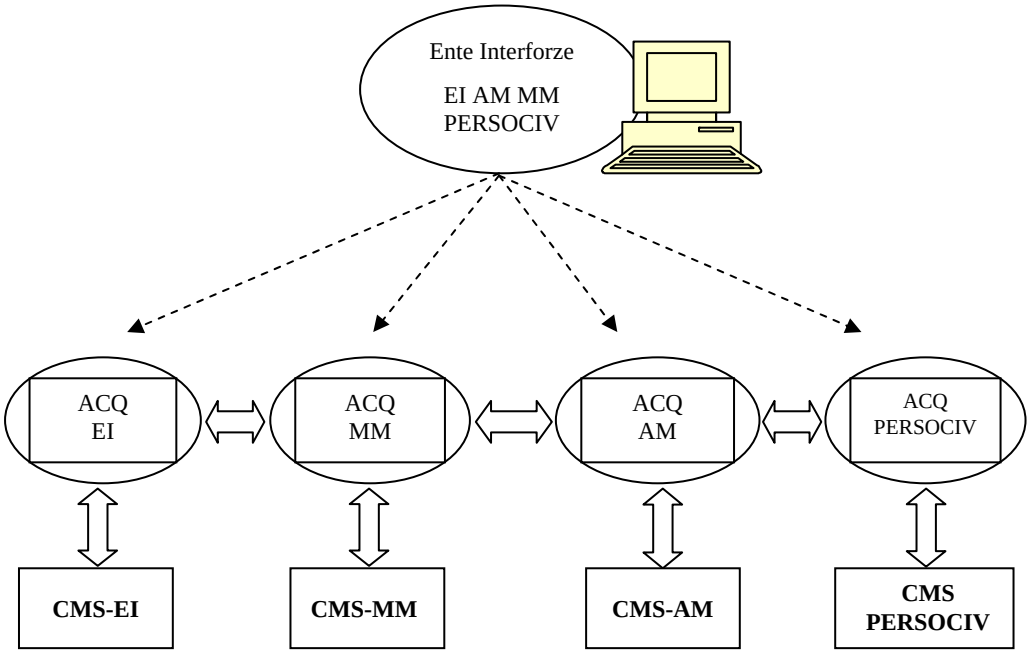
Il Responsabile Periferico (o suo delegato) convalida i dati attraverso un'apposita procedura di approvazione apponendo la propria firma digitale sul documento informatico e la propria firma autografa sulla copia cartacea.

I dati pervengono quindi al Card Management System (CMS) dove vengono verificate le firme digitali apposte dal Responsabile del Trattamento e dal Responsabile Periferico. Come ulteriore verifica dei dati ricevuti viene verificato sul Data Base del CMS che il Responsabile Periferico abbia ricevuto apposita delega per le operazioni di firma.

5.1.2 Acquisizione dei Dati in ambito Interforze

L'acquisizione dei dati al livello interforze è garantita dall'interoperabilità tra i CMS delle F.A. e PERSOCIV realizzata tramite moduli specifici di interscambio.

Di seguito viene mostrato uno schema esemplificativo:



Tale capacità di interscambio è strumentale al rilascio della CMD in tutte quelle occasioni in cui il richiedente lavori in un dominio differente dal proprio (altre F.A. o strutture interforze della Difesa) e inoltre consente una migliore razionalizzazione delle risorse in ambito Difesa. In tale contesto il Responsabile Periferico può convalidare la procedura perché il circuito di acquisizione con cui è normalmente in collegamento trasferirà automaticamente la richiesta alla corretta struttura di emissione.

5.1.3 Acquisizione dei Dati presso altro Ente

Considerata la varietà e la frammentazione sul territorio di alcuni Enti/Uffici, non in tutti sarà ritenuto conveniente costituire una LRA. Pertanto il personale di questi Enti sarà indirizzato presso specifici Centri viciniori che, in base al "concetto di ospitalità" già in altre occasioni applicato, si faranno carico dell'acquisizione e certificazione dei dati, indipendentemente dalla categoria e /o dalla F.A. del richiedente.

Potrà essere prerogativa del Centro quella di esigere che il personale proveniente da altro Ente giunga provvisto di una scheda anagrafico - amministrativa vidimata dal proprio Comando.

5.2 Tipologia, generazione e gestione delle coppie di chiavi

5.2.1 Tipologia

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

- Chiavi di certificazione;
- Chiavi di firma qualificata;
- Chiavi per applicazioni a supporto della PKI di Firma;
- Chiavi di certificazione CA-TSA;
- Chiavi di firma temporale per la TSU.
- Chiavi di firma del OCSP Responder

5.2.2 Policy supportate

Il profilo del certificato è conforme alla [DLB45/09]. Attributi ed estensioni facoltativi possono variare in rapporto alle specifiche policy utilizzate. Le policy del Centro di Certificazione denominato PKI-FF-Difesa sono identificate dagli OID presenti nell'estensione *CertificatePolicie*s ed indicati di seguito:

Policy OID	Descrizione
1.3.6.1.4.1.14031	Stato Maggiore della Difesa Italiana Comando C4
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

5.2.3 Generazione delle chiavi di certificazione

La chiave privata della CA di Firma è generata nel modulo Hardware Security Module (HSM) durante la cerimonia di generazione delle chiavi (Key Ceremony).

Nel modulo HSM del Server della CA, il giorno della cerimonia, viene generata la coppia di chiavi (pubblica e privata). Per l'attivazione del modulo HSM sono necessari l'apparato Pin Entry Device (PED) per il cui utilizzo vengono impiegate apposite "chiavi" a microchip contraddistinte da colori diversi. La chiave privata della CA è conservata sul modulo HSM.

La procedura operativa di gestione dell'apparato HSM prevede l'utilizzo di codici contenuti nei microchip inglobati in supporti a forma di chiave; queste sono colorate a seconda delle diverse funzioni svolte.

5.2.4 Generazione delle chiavi di firma qualificata

Allo scopo di garantire la protezione delle chiavi asimmetriche il processo di generazione avviene all'interno della singola *smart-card* durante il processo di certificazione.

5.2.5 Chiavi per applicazioni a supporto della PKI di Firma

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

5.2.6 Chiavi di certificazione CA-TSA

La chiave privata della Certification Authority di Time Stamping Authority (CA-TSA) è generata nel modulo HSM durante la Key Ceremony.

Nel modulo HSM della CA-TSA, il giorno della cerimonia, viene generata la coppia di chiavi (pubblica e privata). Per l'attivazione del modulo HSM sono necessari l'apparato PED e le relative chiavi colorate. La chiave privata della CA-TSA è conservata sul modulo HSM.

La procedura operativa di gestione dell'apparato HSM prevede l'utilizzo delle chiavi colorate a microchip in dotazione, necessarie per l'utilizzo del PED.

5.2.7 Chiavi per firma temporale per la TSU

La chiave privata del certificato di Time Stamping Unit (TSU) è generata nei moduli HSM durante le normali operazioni di rinnovo del certificato.

La procedura operativa di gestione dell'apparato HSM prevede l'utilizzo di codici contenuti nei microchip inglobati in supporti a forma di chiave; queste sono colorate a seconda delle diverse funzioni svolte.

5.2.8 Chiavi di firma del OCSP Responder

La chiave privata del certificato di firma del OCSP Responder è generata nei moduli HSM durante le normali operazioni di rinnovo del certificato.

La procedura operativa di gestione dell'apparato HSM prevede l'utilizzo di codici contenuti nei microchip inglobati in supporti a forma di chiave; queste sono colorate a seconda delle diverse funzioni svolte.

5.2.9 Distribuzione delle chiavi pubbliche del certificatore ai titolari

Il Certificatore 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).

5.2.10 Hardware e software di generazione delle chiavi

Le chiavi di sottoscrizione delle CMD vengono generate all'interno della CMD stessa. Le chiavi della CA vengono generate sul modulo HSM, le chiavi a supporto della PKI di Firma vengono generate su dispositivi sicuri (HSM o smartcard).

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

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

La CMD, che contiene la chiave privata per la Firma Qualificata usa un chip con a bordo il sistema operativo Siemens CardOS (CMD API); tale *smart-card* 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 Firma sono gli HSM o *smart-card*.

5.2.12 Estrazione della chiave privata dai dispositivi di firma

I criteri di sicurezza adottati per gli HSM e la CMD sono tali per cui non è praticamente possibile - allo stato attuale della tecnologia - l'estrazione in tempi utili della chiave privata dai dispositivi di firma.

5.2.13 Deposito e conservazione della chiave privata

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

La chiave privata del Certificato di Firma è generata e memorizzata solo sulla CMD, 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.

5.2.14 Backup della chiave privata

Il Backup della chiave privata della CA e della CA-TSA è effettuato su una scheda hardware del modulo HSM.

Il Backup della chiave privata, relativo al Certificato di Firma della CMD, non esiste in quanto la chiave privata viene generata internamente alla CMD e non è possibile estrarla.

Il Backup della chiave privata, relativo al server TSU, al server OCSP e delle applicazioni a supporto della PKI di Firma, non esiste in quanto la chiave privata viene generata internamente al modulo crittografico specifico (HSM) e non è possibile estrarla.

5.2.15 Modalità di attivazione della chiave privata

La chiave privata della CA, CA-TSA, TSU e OCSP può essere attivata tramite il modulo HSM specifico in cui viene inserita dapprima una chiave contenente il codice di attivazione (codice PIN) e successivamente vengono inserite altre due chiavi specifiche .

La chiave privata per la Firma qualificata è contenuta nella CMD e per la sua attivazione è necessario conoscere il PIN FIRMA (PIN specifico diverso da quello della carta). Il PIN FIRMA viene generato in modo casuale al momento della personalizzazione della CMD e viene distribuito insieme al PUK FIRMA in busta cieca consegnata disgiuntamente alla CMD.

La chiave privata delle macchine e applicazioni a supporto della PKI Firma, viene attivata con un codice di attivazione specifico.

5.2.16 Modalità di disattivazione della chiave privata

La chiave privata della CA e della CA-TSA viene disattivata se il Certificatore decide di interrompere l'emissione dei certificati (attraverso procedure specifiche di disattivazione).

La chiave privata relativa al Certificato di Firma delle CMD viene disattivata dopo tre tentativi errati di introduzione del PIN di Firma. In questo caso è necessario introdurre il codice PUK di Firma che viene generato assieme al PIN al momento della personalizzazione della CMD. Se viene inserito in modo sbagliato il codice PUK di Firma per dieci volte di seguito, la CMD, e in particolare la chiave privata relativa al Certificato di Firma, viene bloccata.

5.2.17 Modalità di distruzione della chiave privata

Alla scadenza di validità del certificato inserito nella CMD, la smartcard deve essere distrutta a mezzo rottura del microchip. Copia del verbale di distruzione deve essere inviato, dal CMS che ha emesso la smartcard, al Centro di Certificazione nel minor tempo possibile (al massimo 3 giorni lavorativi).

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

5.2.18 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 sul Directory LDAP raggiungibile all'indirizzo: ldap://ldappkiff.difesa.it.

5.3 Tipologie e modalità di emissione dei certificati

5.3.1 Tipologia

A partire dalle chiavi pubbliche generate secondo le procedure del paragrafo precedente, si giunge alla generazione dei differenti tipi di certificati digitali.

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

- Certificato di Certificazione;
- Certificato di Certificazione *CA*-TSA
- Certificato di firma temporale *Time Stamping Unit* (TSU);
- Certificati di Firma qualificata;
- Certificati di Firma del OCSP Responder:
- Certificati per applicazioni a supporto della PKI di Firma.

5.3.2 Modalità di emissione del certificato di Certificazione

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

5.3.3 Modalità di emissione del certificato di certificazione Time Stamp Authority (CA-TSA)

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

5.3.4 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)

5.3.5 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.

5.3.6 Modalità di emissione dei certificati di Firma qualificata

Un'apposita applicazione presente presso i CMS delle F.A., contestualmente alla generazione delle 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 RA, 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 RA che verifica la firma ed il mittente e sottopone il PKCS#10, contenuto nel PKCS#7, alla CA. La CA genera il certificato, lo invia alla RA che, all'atto della sua ricezione, lo firma producendo un nuovo PKCS#7. Il PKCS#7 viene inoltrato al CMS, esegue la verifica della firma eseguita dalla RA e del certificato CA e lo inserisce nella CMD.

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

Un'apposita applicazione presente presso i CMS delle F.A., 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.

5.4 Codici assegnati al titolare di un certificato di Firma qualificata

Il Titolare del certificato di Firma qualificata riceverà una busta cieca contenente i codici necessari per l'apposizione della firma. Nel complesso la busta cieca conterrà i seguenti codici:

- **PIN Carta**: da utilizzare per abilitare l'accesso alla CMD ai processi applicativi che richiedono l'esecuzione delle operazioni di autenticazione;
- **PUK Carta**: da utilizzare per lo sblocco del PIN Carta;
- **PIN di Firma**: da utilizzare per abilitare l'accesso alla CMD ai processi applicativi che richiedono l'esecuzione delle operazioni di Firma qualificata;
- **PUK di Firma**: da utilizzare per lo sblocco del PIN di Firma.

Il Titolare riceverà inoltre un codice di sospensione (o "*passphrase*") da utilizzare in caso di richiesta telefonica di sospensione. Per nessun motivo è consentito la ristampa della busta cieca contenente i suddetti codici. A tal proposito l'applicativo deputato al rilascio dei PIN inibisce la produzione di ulteriori stampe della distinta di consegna.

5.5 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 decennale, mentre i relativi certificati hanno una validità temporale di **15 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 qualificata sono sostituite contestualmente al rinnovo dei relativi certificati e relative CMD che hanno un periodo di validità di **5 anni**;
- Le chiavi delle **applicazioni** a supporto della CA sono sostituite contestualmente al rinnovo dei relativi certificati che hanno un periodo di validità di **5 anni**.

Per effetto dell'art.4 della Deliberazione CNIPA N.45 del 21 maggio 2009 che ha stabilito il passaggio dall'algoritmo SHA-128 all'algoritmo SHA-256, sarà possibile che alcune chiavi di firma qualificata e i relativi certificati potranno avere un periodo di validità inferiore ai **5 anni** in quanto la data di inizio coinciderà con la data del loro rinnovo mentre la data di scadenza sarà la stessa data di scadenza delle precedenti chiavi di firma qualificata e certificati prodotti con l'utilizzo dell'algoritmo SHA-128.

5.6 Procedura di emissione e personalizzazione dei dispositivi di Firma qualificata (CMD)

Poiché il processo di emissione del certificato di Firma qualificata è strettamente connesso al contestuale processo di emissione della CMD, quest'ultimo viene descritto nella sua interezza.

La CMD viene pre-stampata presso l'Istituto Poligrafico e Zecca dello Stato e contiene, oltre il layout, anche elementi che la rendono non replicabile; in particolare viene impresso con una tecnologia di *laser engraving* l'identificativo progressivo della carta. Il *file system* viene caricato a bordo del chip con l'identificativo della carta stessa impresso nel layout. Presso i CMS avviene la seconda fase di personalizzazione.

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

Il personale del CMS preposto all'emissione, dopo aver verificato il corretto funzionamento della carta, avvia il processo di emissione per il certificato di firma, di autenticazione e di cifra, come di seguito illustrato:

Certificato di Autenticazione

- si genera all'interno della carta la prima coppia di chiavi e viene inoltrata all'apposita Sub CA una richiesta di certificato di autenticazione firmata dalla carta stessa;
- la Sub CA rilascia il certificato di autenticazione e lo pubblica sul proprio sito;
- il certificato viene installato a bordo della CMD, vengono inseriti i dati personali nel chip e personalizzata la carta graficamente;

1. Certificato di Firma
   - si genera all'interno della carta la seconda coppia di chiavi e viene inoltrata alla PKI di Firma una richiesta di certificato di Firma qualificata firmata dalla carta stessa;
   - la PKI di Firma rilascia il certificato di Firma qualificata e lo pubblica sul proprio sito;
   - il certificato di Firma qualificata viene installato a bordo della CMD;
2. Certificato di Cifra
   - viene generata dal CMS la terza coppia di chiavi e viene fatta firmare la richiesta di un certificato di cifra alla carta stessa;
   - il CMS inoltra la richiesta alla propria Sub CA che rilascia il certificato di cifra;
   - il CMS installa a bordo della CMD il certificato di cifra, e memorizza in un proprio database la chiave privata corrispondente (procedura di *escrow*);
   - il CMS stampa sulla busta apposita (busta cieca) i relativi PIN, PUK e "codice di sospensione" insieme eventualmente all'indirizzo di posta elettronica del titolare;
   - il CMS ad operazione avvenuta con successo pone la carta in stato attivo;

Le CMD così personalizzate possono essere ritirate da personale delegato dal Responsabile Periferico o inviate tramite posta assicurata.

Le buste contenenti i codici di attivazione, possono essere inviate per posta (ma non contestualmente alle CMD) o ritirate da altro personale delegato dal Responsabile Periferico (comunque diverso rispetto a chi riceve le CMD).

Il Responsabile Periferico riceve in consegna in tempi diversi la CMD e la busta dei codici che deve consegnare al Titolare previa autenticazione.

Il Titolare ritira la carta ed i codici dopo aver verificato che la busta dei codici sia intatta e che i dati riportati sulla CMD corrispondano ai propri.

5.7 Modalità di sospensione e revoca dei certificati

5.7.1 Generalità

La CMD, 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 qualificata", uno di "autenticazione" 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 annulla l'efficacia della carta che dovrà essere riemessa con nuovi certificati. Pertanto le procedure di sospensione/revoca della CMD sono da riferirsi alla validità dei certificati ivi contenuti e sono di stretta competenza dei CMS che si attivano, generalmente, su segnalazione delle LRA di FA o PERSOCIV.

5.7.2 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.

5.7.3 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 telefono comunicando il proprio "codice di sospensione" e presentando successivamente una motivata richiesta scritta. La LRA nella figura del Responsabile Periferico, provvederà a far pervenire la richiesta al competente CMS.
La LRA e il CMS possono, ove ne ricorrano giustificati motivi, procedere autonomamente alla procedura di sospensione dandone notizia e spiegazione al Titolare.
La sospensione di un certificato ha una durata limitata nel tempo (al massimo per 15 giorni), dopodiché, ove non siano cessate le condizioni di sospensione, si procede alla sua revoca. Il CMS provvederà a tenere aggiornata una lista pubblica dei certificati sospesi (CRL).

5.7.4 Riattivazione di un certificato sospeso

Il Responsabile Periferico, appurata la scomparsa delle motivazioni che hanno determinato la sospensione, invia una e-mail, firmata digitalmente con la propria CMD, al CMS della FA del Titolare, indicando gli estremi della carta (numero seriale, cognome, nome). Successivamente riceverà una e-mail firmata digitalmente della avvenuta riattivazione dal Responsabile del CMS.

5.7.5 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 (CMD).

5.7.6 Procedure per la revoca di un certificato

Il Responsabile Periferico, appurata la validità delle motivazioni di cui al paragrafo precedente, invia una e-mail, firmata digitalmente con la propria CMD, al CMS della FA del Titolare, indicando gli estremi della carta (numero seriale, cognome, nome). Successivamente riceverà una e-mail firmata digitalmente della avvenuta revoca dal Responsabile del CMS.
La LRA e il CMS possono, ove ne ricorrano giustificati motivi, procedere autonomamente alla procedura di revoca dandone notizia e spiegazione al Titolare.

5.7.7 Aggiornamento delle CRL (Certificate Revocation List)

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

5.8 Modalità di sostituzione delle chiavi e rinnovo dei certificati

Per la sostituzione delle coppie di chiavi e per il conseguente rinnovo dei certificati il Certificatore 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.

5.8.1 Sostituzione delle chiavi di certificazione e rinnovo dei relativi certificati

Con almeno novanta giorni di anticipo sulla scadenza del certificato relativo ad una chiave di certificazione, il Certificatore 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 uno relativo alla vecchia chiave pubblica sottoscritto con la nuova chiave privata.

5.8.2 Rinnovo dei certificati di firma temporale

La procedura prevede la :

- Generazione di una nuova coppia di chiavi di firma 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.

5.8.3 Rinnovo dei certificati di firma del OCSP Responder

La procedura prevede la :

- Generazione di una nuova coppia di chiavi di firma 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.

5.8.4 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 che ha rilasciato la CMD contenente il certificato qualificato in scadenza) provvede ad inviare una mail al Titolare del Certificato all'approssimarsi della scadenza dei certificati.

Contestualmente deve essere effettuata richiesta di emissione della nuova CMD con le metodologie già evidenziate nei capitoli precedenti.

Viene emessa la CMD e spedita al Titolare secondo le metodologie indicate precedentemente.

Alla ricezione della nuova CMD presso l'Ente di appartenenza del titolare, il Responsabile Periferico deve:

- Convocare il Titolare interessato;
- Ritirare la vecchia *smart-card*, distruggendola con taglio, a mezzo forbice, sul microprocessore;
- Consegnare al Titolare la nuova *smart-card*;
- Redigere un verbale di distruzione della vecchia *smart-card*.

Inviare copia del predetto verbale al Centro di Certificazione del CMS della FF.AA. o PERSOCIV che ha emesso la CMD ed al centro di Certificazione della PKI di Firma.

5.9 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, dalla CA di Firma qualificata.

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), sia dalla DIFENET (rete intranet della Difesa per l'erogazione di servizi al personale dipendente) sia da INTERNET. Ciò permette agli utilizzatori di verificare l'affidabilità e la validità dei certificati emessi dal servizio di certificazione che garantisce la sincronizzazione tra le due copie.

5.9.1 Informazioni contenute del registro dei certificati

Nel Registro dei Certificati vengono pubblicati:

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

5.9.2 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 DIFENET e di INTERNET.

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 dall'esterno, 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.

5.9.3 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 è disponibile H-24.

5.10 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.

5.10.1 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 dall'esterno, 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.

5.10.2 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 rimovibile in più copie;

- Custoditi sotto chiave;
- Sottoposti a periodici controlli dal 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.

5.10.3 Verifiche

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

5.11 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 concesso solo 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 le CMD dei Titolari sono custoditi in armadi sicuri 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.

5.12 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.

5.13 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 dei 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.

5.14 Servizio OCSP

Il servizio di certificazione rende disponibile un servizio OCSP autoritativo per la verifica dei certificati di firma qualificata emessi dalla sola infrastruttura PKI di Firma del Ministero della Difesa (PKI-FF).

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

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 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.

5.15 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)

5.15.1 Generazione della firma digitale

Il processo di firma può essere eseguito in modalità stand-alone tramite l'applicazione "PKI Desk". Di seguito vengono indicati i passi necessari (per ulteriori dettagli fare riferimento al "Tutorial per la firma"):

1. Avviata l'applicazione, l'utente può aprire il file sul quale deve apporre la firma. L'applicazione permette la selezione di qualsiasi tipo di file (Word, Excel, Power Point, PDF , p7m ….etc);
2. Viene data all'utente la possibilità di una "Preview" del documento e/o la trasformazione del documento nel formato "PDF" e, tramite appositi pulsanti, può eseguire la procedura di firma.
3. A questo punto il sistema esegue la procedura di firma, richiedendo al server di *Time-Stamping* la marcatura temporale (se tale richiesta è stata flaggata durante le operazioni di firma). Durante tale procedura viene richiesto l'inserimento del PIN per utilizzare la chiave di firma.

4. Terminata l'operazione viene prodotto il file "nome-originale.estensione". L'estensione dipenderà dal formato di firma scelto.

5.15.2 Verifica della Firma

Per verificare la firma digitale di un documento, viene utilizzata la stessa applicazione "PKI Desk" oppure un'analoga applicazione denominata "PKI Desk Verify" pubblicata sia su rete intranet che su rete internet ed è predisposta solo per le operazioni di verifica.
Entrambe le applicazioni citate sono conformi al [DPCM 22.02.2013] ed alla [DLB-45/09].

Per consentire il buon esito della procedura di verifica della firma, è necessario essere connessi alla rete per controllare lo stato di validità del certificato di firma tramite il controllo della CRL o tramite il servizio OCSP.

Il processo di verifica consiste nei seguenti passi:

1. Aprendo il file crittografato tramite l'apposito pulsante nella toolbar dell'applicazione, viene presentato all'utente il documento contenuto all'interno del file aperto;
2. L'applicativo esegue in background tutti i controlli sul documento aperto, in particolare la correttezza delle firme apposte e lo stato dei certificati contenuti nel documento attraverso il servizio OCSP (configurato per default all'atto dell'istallazione della suite PKIDesk) o attraverso la CRL (se diversamente configurato);
3. L'applicativo presenta quindi tutti i firmatari del documento e una serie di indicazioni visive sulla correttezza delle firme. Selezionando una delle firme visualizzate, si ha la possibilità di consultare nel dettaglio:
    a. Il certificato di chi ha firmato (data di scadenza, i punti di distribuzione della CRL, URL del OCSP Responder e la validità elettronica);
    b. La marca temporale apposta dove presente;
    c. Il certificato dell'Authority che ha rilasciato la marca temporale (data di scadenza e punti di pubblicazione della CRL).

Nel caso in cui una delle precedenti verifiche non vada a buon fine, la procedura visualizzerà il dettaglio del problema, ad esempio impossibilità di verificare la CRL, certificato revocato, alterazione del documento firmato, ecc..

5.16 Cessazione dell'attività del Certificatore

Il Certificatore se intende cessare l'attività deve, almeno sessanta giorni prima della data di cessazione, darne avviso a DigitPA 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 Certificatore comunica contestualmente la rilevazione della documentazione da parte di altro certificatore o l'annullamento della stessa (l'indicazione di un certificatore sostitutivo evita la

revoca dei certificati e della relativa documentazione). Il Certificatore indica altro depositario del registro dei certificati e della relativa documentazione [DLGS82].

6 ELENCO APPENDICI

- **Appendice SGD v.1.0 - Firma Remota con procedura Automatica - Servizio di Protocollo del Ministero della Difesa presso il Segretariato Generale della Difesa**