Ministero della Difesa

Public Key Infrastructure

Certificate Policy

CA Certificati di Firma

CP – Certificate Policy

Autore:	Ministero della Difesa
Versione:	1.9
Data del documento:	24 marzo 2025
No Doc.:	IT-CP–DS01

Certificate Policy
CA Certificati di Firma

Validato da	Serg. Marco D'AGOSTINO	Responsabile Conduzione Tecnica dei Sistemi	*Firmato Digitalmente da/Signed by:* MARCO D'AGOSTINO *In Data/On Date:* mercoledì 26 marzo 2025 15:39:31
	Lgt. Gennaro GIANNINO	Responsabile Auditing	*Firmato Digitalmente da/Signed by:* GENNARO GIANNINO Lgt. *In Data/On Date:* giovedì 27 marzo 2025 08:30:19
	S.T.V. Ernesto PETRONI	Responsabile Sicurezza	*Firmato Digitalmente da/Signed by:* ERNESTO PETRONI *In Data/On Date:* mercoledì 26 marzo 2025 15:57:57
	Ten.Col. Andrea PERNA	Responsabile Servizi Tecnici e Logistici	*Firmato Digitalmente da/Signed by:* ANDREA PERNA *In Data/On Date:* venerdì 28 marzo 2025 14:24:15
Approvato da	Gen. Div. AAran Sandro SANASI	Prestatore di Servizi Fiduciari Qualificati (QTSP)	*Firmato Digitalmente da/Signed by:* SANDRO SANASI *In Data/On Date:* venerdì 28 marzo 2025 16:22:06

Indice

Versione	Sezione	Descrizione	Data
1.9	Tutte	Cambio componenti Gruppo di Certificazione. Cambio Certificatore	24 Marzo 2025
1.8	Tutte	Sostituito Responsabile Sicurezza	13 Ottobre 2022
1.7	Tutte	Aggiunte Specifiche ETSI profilo Sigillo Elettronico	15 Giugno 2022
1.6	Tutte	Aggiunta modalità operattive rilascio Firma Automatica e Sigillo Digitale Sostituito Responsabile Sicurezza	22 Novembre 2021
1.5	Sezione 1.2 Sezione 3.1 Sezione 7.1	Aggiunta O.I.D. Sigillo Digitale Sostituito Responsabile Sicurezza Sostituito Responsabile Servizi Tecnici e Logistici	06 Aprile 2021
	Sezione 1.2 Sezione 1.6 Sezione 7.1	Aggiunte informazioni riguardo l'OID per la Policy dei Certificati AgID (agIDcert).	
	Sezione 4.10 Sezione 6.3.2	Aggiunte informazioni riguardo lo stato dei certificate oltre la data di scadenza degli stessi.	
1.4	Tutte	Modificata l'indicazione del repository del certificatore Aggiunta NOTA nel paragrafo 2.1 inerente il reindirizzamento in https del URL www.pki.difesa.it Aggiunte NOTE descrittive nei paragrafo 1.3.1 e 3.1 relativi al cambio di denominazione dell'Ente e all'OU presente nel certificato di CA Aggiornati i punti di contatto del help desk di primo livello	05 Novembre 2020
1.3	Sezione 1.2	Aggiunta nota relativa agli OID	24 Giugno 2020
1.2	Tutte	Cambio Denominazione Ente da Comando C4 Difesa in Comando per le Operazioni in Rete	

		Sostituita la figura di Responsabile Periferico con Funzionario Autorizzato alla Validazione dei Dati e la relativa abbreviazione da RP a FA. Sostituita la figura di Incaricato al Trattamento dei Dati con Operatore Autorizzato all'inserimento dei dati e la relativa abbreviazione da ITD a OA.	09 Marzo 2020
1.1	Tutte	Correzione Ortografiche	10 Maggio 2018
	Sezione 4.2.1	Sostituite le figure del Responsabile del trattamento dei dati e (RDT) e del Responsabile Periferico (RP) con le figure di Incaricato al Trattamento dei dati (ITD) e con Responsabile al Trattamento (RT)	
1.0			01 Giugno 2017

1 INTRODUZIONE

Il presente documento descrive l'organizzazione implementata, dal Ministero della Difesa/Stato Maggiore della Difesa Comando per le Operazioni in Rete - nell'esercizio delle funzioni di Prestatore di Servizi Fiduciari Qualificati accreditato presso l'Agenzia per l'Italia Digitale (Ag.I.D.), per il rilascio dei certificati di firma.

Inoltre, il presente documento, descrive i processi necessari per la generazione, la pubblicazione, la sospensione e la revoca dei certificati di firma.

Il certificato di firma digitale viene installato su supporto fisico (smartcard) denominato Modello AT elettronico (ATe). Il Mod. ATe contiene i certificati digitali e le relative coppie di chiavi dei titolari.

Tale Modello, rilasciato ai sensi del DPR 851/1967, del DPCM 24 maggio 2010 e del DPCM 18 gennaio 2016, ha valore di tessera di riconoscimento elettronico.

Ai fini dell'acquisizione dei dati, necessari per l'emissione dei certificati di Firma digitale, la PKI-Difesa utilizza il circuito di emissione del modello ATe denominato Card Management System Unico (Registration Authority-R.A.) e delle relative organizzazioni periferiche di Forza Armata (Local Registration Authority - L.R.A.).

1.1 Scopo del documento

Il presente documento è il Certificate Policy (CP) del Ministero della Difesa relativo all'emissione e alla gestione dei certificati di firma qualificata, remota ed automatica.

La struttura e il contenuto di questo CP si basano sulla specifica pubblica [RFC 3647].

Nel presente documento sono illustrate le modalità ed i processi operativi della Certification Authority denominata "Ministero della Difesa – Firma Qualificata" mediante la quale il Ministero della Difesa emette e gestisce i certificati di firma qualificata utilizzati dal proprio personale e dal personale delle PA che hanno stipulato un accordo con il Ministero della Difesa.

1.2 Nome documento e identificazione

Il presente CP della CA di Firma eIDAS è referenziato, nei certificati di firma, con il seguente Object Identifier (OID): 1.3.6.1.4.1.14031.2.1.1.101.

L'OID assegnato al Ministero della Difesa è 1.3.6.1.4.1.14031.

L'OID della CA di Firma eIDAS del Ministero della Difesa Firma Qualificata è 1.3.6.1.4.1.14031.2.1.1.

Internamente alla CA sono definiti i seguenti OID relativi ai certificati da lei emessi.

Nella tabella seguente sono riportati sia gli OID dei certificati gestiti dalle CA di Firma Digitale del Ministero della Difesa accreditate in Italia prima del 1 Giugno 2016. Delle due CA, quella denominata *"Ministero della Difesa - PKI di Firma Qualificata"* non emette più certificati da luglio 2014 ed esegue solo la gestione del ciclo di vita dei certificati emessi (revoca/sospensione/riattivazione), mentre la CA attuale denominata *"Ministero della Difesa - CA di Firma Digitale"* esegue emissioni e gestione del ciclo di vita.
Gli OID delle policy dei certificati emessi per i Titolari, si basano sulle policy emanate da ETSI nell'ambito della normativa eIDAS, consultare la sezione 7.1 per i dettagli sui profili supportati.

Descrizione	OID
OID base del Ministero della Difesa	1.3.6.1.4.1.14031
Base della vecchia struttura PKI Difesa (CSP)	1.3.6.1.4.1.14031.**1**
Policy della vecchia struttura PKI Difesa definita in *www.pki.difesa.it/firmadigitale.pdf*	1.3.6.1.4.1.14031.1.**1**
Base della nuova struttura PKI Difesa (CSP)	1.3.6.1.4.1.14031.**2**
Policy della nuova struttura PKI Difesa definita in www.pki.difesa.it/ManualeOperativoDifesa.pdf	1.3.6.1.4.1.14031.2.**1**
OID del certificato della CA di Firma	1.3.6.1.4.1.14031.2.1.**1**
OID del certificato di OCSP per la CA di Firma	1.3.6.1.4.1.14031.2.1.1.**1**
OID del certificato di Firma Utente senza limitazioni d'uso	1.3.6.1.4.1.14031.2.1.1.**2**
OID del certificato di Firma con limitazione d'uso[1]	1.3.6.1.4.1.14031.2.1.1.**3**
OID del certificato di Firma Remota per Test	1.3.6.1.4.1.14031.2.1.1.**4**
OID del certificato di Firma Remota	1.3.6.1.4.1.14031.2.1.1.**5**
OID del certificato di Firma Utente per Test	1.3.6.1.4.1.14031.2.1.1.**6**
OID del certificato di Firma Automatica (Remota)	1.3.6.1.4.1.14031.2.1.1.**8**
Policy della nuova struttura PKI eIDAS definita in https://pki.difesa.it/tsp	1.3.6.1.4.1.14031.2.**1**
OID del CPS per il servizio di Firma eIDAS in lingua Italiana	1.3.6.1.4.1.14031.2.1.1.**100**
OID del CP per il servizio di Firma eIDAS in lingua Italiana	1.3.6.1.4.1.14031.2.1.1.**101**
OID del documento di Terms and Condition del servizio di Firma eIDAS in lingua Italiana	1.3.6.1.4.1.14031.2.1.1.**102**
OID del documento PKI Disclosure Statement del servizio di Firma eIDAS in lingua Italiana e Inglese	1.3.6.1.4.1.14031.2.1.1.**103**
OID del CPS per il servizio di Firma eIDAS in lingua Inglese	1.3.6.1.4.1.14031.2.1.1.**200**
OID del CP per il servizio di Firma eIDAS in lingua Inglese	1.3.6.1.4.1.14031.2.1.1.**201**
OID del documento di Terms and Condition del servizio di Firma eIDAS in lingua Inglese	1.3.6.1.4.1.14031.2.1.1.**202**
OID del certificato di Firma eIDAS Utente senza limitazioni d'uso	1.3.6.1.4.1.14031.2.1.1.**12**
OID del certificato di Firma eIDAS con limitazione d'uso[2]	1.3.6.1.4.1.14031.2.1.1.**13**
OID del certificato di Firma eIDAS Remota per Test	1.3.6.1.4.1.14031.2.1.1.**14**
OID del certificato di Firma eIDAS Remota	1.3.6.1.4.1.14031.2.1.1.**15**
OID del certificato di Firma eIDAS Utente per Test	1.3.6.1.4.1.14031.2.1.1.**16**
OID del certificato di Firma eIDAS Automatica (S.G.D.)	1.3.6.1.4.1.14031.2.1.1.**18**
OID del certificato di Firma eIDAS Automatica (S.M.D. COR)	1.3.6.1.4.1.14031.2.1.1.**19**
OID del certificato di Sigillo Digitale eIDAS	1.3.6.1.4.1.14031.2.1.1.**23**
OID del certificato di Sigillo Digitale eIDAS Automatico (AUTOREMOTE)	1.3.6.1.4.1.14031.2.1.1.**28**

In ottemperanza alle raccomandazioni contenute in [AGID_LG11] sezione 4, ovvero "Linee guida contenente le Regole Tecniche e Raccomandazioni...", a partire da Dicembre 2019, il QTSP ha provveduto a inserire nell'attributo CertificatePolicies (OID 2.5.29.32) un ulteriore elemento PolicyIdentifier con valore **agIDcert** (OID **1.3.76.16.6**), il quale specifica "*When included into a Rec. ITU-T X.509 electronic certificate, it means that all the recommendations issued by the Agency for Digital Italy are fulfilled*" ("*Quando incluso in un certificate elettronico di tipo Rec. ITU-T X.509, indica che tutte le raccomandazioni emesse dall'Agenzia per l'Italia Digitale vengono soddisfatte*").

[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 Partecipanti alla PKI

Questa sezione fornisce un'introduzione sulla Certification Authorities, Registration Authorities, e le parti interessate della PKI Difesa.

1.3.1 Certification Authority

La Certification Authority (CA) è il soggetto terzo e fidato che emette i certificati, firmandoli con la propria chiave privata (chiave di CA). La CA dedicata ad emettere i certificati di Firma ed a gestire lo stato dei certificati stessi viene detta CA di Firma.

Nell'ambito del servizio qui descritto, il ruolo di CA di Firma è svolto dal Ministero della Difesa/Stato Maggiore della Difesa - Comando per le Operazioni in Rete identificato come segue:

Soggetto Giuridico	STATO MAGGIORE DELLA DIFESA - Comando per le Operazione in Rete
Indirizzo	Via Stresa 31b 00135 Roma
Legale Rappresentante	Comandante del COR
Codice Fiscale	97355240587
ISO Object Identifier	1.3.6.1.4.1.14031
Sito Web Generale	www.difesa.it
Sito Web del Centro di Certificazione	https://pki.difesa.it/tsp
Indirizzo di posta elettronica:	info_pkiff@smd.difesa.it
Directory Server	ldap://ldappkiff.difesa.it

Il Comandante del Comando per le Operazioni in Rete svolge anche il compito di Prestatore di Servizi Fiduciari Qualificati (QTSP) della Difesa.

La Certification Authority è una Root-CA che emette direttamente i certificati per i Titolari, non emette certificati di SubCA e non è coinvolta in processi di Cross-Certification.

NOTA – In data 9 Marzo 2020 il comando ospitante il Centro di Certificazione del QTSP – S.M.D. Ministero della Difesa ha cambiato denominazione da S.M.D. Comando C4 Difesa a S.M.D. Comando per le Operazioni in rete (CORDIFESA) con atto costitutivo del 4 Marzo 2020 regolato dalla circolare SMD-N-137. Il legale rappresentante resta sempre il Comandante pro tempore dell'Ente.

1.3.2 Registration Authority

La Registration Authority (RA) è la persona, struttura od organizzazione che svolge le attività di:

- accoglimento e validazione delle richieste di emissione e gestione dei certificati;

- registrazione del soggetto richiedente e dell'organizzazione di appartenenza;
- autorizzazione all'emissione, da parte della CA, del certificato digitale richiesto;
- fornitura al personale del certificato digitale e delle informazioni necessarie al suo utilizzo.

Tale attività è svolta per i certificati di firma digitale rilasciati a bordo del modello ATe dalla Local Registration Authority (LRA) e dal Card Management System (CMS) del Ministero della Difesa.

Per i certificati di firma automatica SGD la funziona di RA è svolta dal referente unico del protocollo informatico per l'A.D..

Per i certificati di firma remota, firma automatica e sigillo della Difesa SMD/COR, la funzione di RA è svolta direttamente dal Centro di Certificazione PKI Difesa.

1.3.3 Utenti finali (titolari)

Tutto il personale della Difesa ed il personale degli Enti/P.A. che hanno firmato un accordo di collaborazione. La Difesa per le attività direttamente o indirettamente pertinenti al servizio di firma digitale, definito in questa documento, ha dotato i propri dipendenti di firma digitale in virtù del normale rapporto di lavoro espletato nell'ambito delle attività previste dal presente documento.

Gli utenti finali, ovvero i Sottoscrittori dei certificati, sono persone fisiche che richiedono un certificato e che detengono la corrispondente chiave privata.

1.3.4 Parti interessate

Le parti interessate sono tutti i soggetti che fanno affidamento sulle informazioni contenute nel certificato per le operazioni di verifica dei documenti firmati dai titolari.

1.3.5 Altri utenti

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 di Servizi Fiduciari Qualificati (QTSP) 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 (F.A. figura professionale presente presso l'Ente che richiede l'emissione dei certificati qualificati per il Titolare).

- Operatore autorizzato all'inserimento dei dati (O.A., figura professionale presente 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).

- Utilizzatore (una qualsiasi entità, figurata o reale, che fa uso di un certificato qualificato per verificare la validità della firma digitale o dell'autenticazione)

1.4 Uso dei certificati

La CA del Ministero della Difesa CA di Firma Digitale eIDAS usa la sua coppia di chiavi per:

- firmare i certificati digitali emessi;
- firmare le Certification Revocation List (CRL) emesse.

Il Titolare del certificato di firma con limitazioni d'uso presente sul modello ATe e sull'HSM di firma remota usa la propria coppia di chiavi per:

- firmare un documento informatico nei formati previsti dalla normativa vigente nel rispetto delle limitazioni d'uso indicate all'interno del certificato stesso.

Il Titolare del certificato di firma senza limitazioni d'uso presente sul modello ATe e sull'HSM di firma remota usa la sua coppia di chiavi per:

- firmare un documento informatico nei formati previsti dalla normativa vigente.

Il Titolare del certificato di firma automatica/sigillo presente sull'HSM di firma automatica/sigillo usa la sua coppia di chiavi per:

- firmare l'avvio di un processo informatico all'interno del proprio ambito lavorativo.

Il certificato dell'OCSP della CA di Firma Qualificata è usato per:

- firmare le risposte alle richieste di verifiche dello stato di validità di un certificato di firma.

Tutto ciò che non rientra negli usi previsti dal paragrafo 1.4 è considerato un uso non autorizzato del certificato.

Ogni uso improprio dei certificati emessi dal Ministero della Difesa sulla base di questo CP è proibito e comporta, la revoca immediata del certificato qualora se ne venga a conoscenza.

1.5 Amministrazione delle policy

Questo documento è custodito e mantenuto aggiornato dal personale del Centro di Certificazione ed è approvato dal Comandante del Comando per le Operazioni in Rete in qualità di legale rappresentante del Centro di Certificazione e di Prestatore di Servizi Fiduciari Qualificati della Difesa.

Questo CP è redatto, pubblicato ed aggiornato dal Centro di Certificazione del Ministero della Difesa/Stato Maggiore della Difesa - Comando per le Operazioni in Rete, sito in via Stresa 31b, 00135 Roma.

Il presente documento viene revisionato e aggiornato anche in occasione di modifiche interne all'organizzazione (ad esempio per il cambio di uno dei responsabili) o per variazioni nella normativa di riferimento.

Richieste d'informazioni o chiarimenti sul presente CP possono essere inoltrate:

- all'indirizzo di posta elettronica del Centro di Certificazione PKI Difesa **info_pkiff@smd.difesa.it**
- tramite il link: **https://servicedesk.difesa.it**
- all'indirizzo di posta elettronica **helpdesk@cor.difesa.it**
- al numero **+39-06-46914444** del Help Desk del Comando per le Operazioni in Rete che si occuperà di inoltrare la richiesta al Centro di Certificazione

Questo CP e le policy in esso contenute è valutato da un Organismo di Certificazione (CAB).

Questo CP e le policy in esso indicate sono conformi con le policy emanate dal Ministero della Difesa Italiana.

Questo CP è stato letto e validato per la relativa parte di competenza dal responsabile della conduzione tecnica dei sistemi, del responsabile dell'auditing, dal responsabile della sicurezza, dal responsabile dei sistemi tecnici logisitci ed è stato approvato dal Comandante del Comando per le Operazioni in Rete in qualità di Prestatore di Servizi Fiduciari Qualificati della Difesa.

1.6 Definizioni e Acronimi

Questo paragrafo contiene un elenco di definizioni dei termini utilizzati all'interno del documento, così come una lista di acronimi e il loro significato.

Termine/ Acronimo	Descrizione	Spiegazione
AgID	Agenzia per l'Italia Digitale (ex gestione DigitPA) CA Certification	Organismo di vigilanza Italiano
CA	Certification Authority	Entità che emette i certificati
CMD	Carta Multiservizi Difesa	Smartcard fornita al personale della Difesa valida come documento elettronico e contenente i certificati del Titolare
CMS	Card Management System	Entità adibita al rilascio dei modelli ATe/CMD per il personale della Difesa e per quello delle PA che hanno che hanno firmato un accordo di collaborazione con la Difesa.
CP	Certificate Policy	Un nominato set di regole che indicano l'applicabilità di un certificato su una particolare comunità e/o classe di applicazioni con specifici requisiti di sicurezza
CPS	Certification Practice Statement	Documento che illustra le modalità ed i processi operativi della C.A. mediante la quale il Ministero della Difesa emette e gestisce i certificati di firma qualificata.
CRL	Certificate Revocation List	La lista dei certificati revocati
CSR	Certificate Signing Request	Richiesta di certificato
DN	Distinguished Name	Identificativo univoco del soggetto internamente al certificato
DR	Disaster Recovery	Sito di back-up dell'infrastruttura
FIPS	Federal Information Processing Standard	Regole e misure comuni che devono osservare i vari dipartimenti del governo degli Stati Uniti.
HSM	Hardware Security Module	Modulo hardware per l'immagazzinamento sicuro delle chiavi per operazioni crittografiche.
LDAP	Lightweight Directory Access Protocol	Il Directory Server dove vengono pubblicati I certificati
LRA	Logal Registration Authority	Entità periferica responsabile delle procedure di enrolment, esegue l'identificazione e l'autenticazione del soggetto richiedente il rilascio del certificato
OCSP	On-line Certificate Status Protocol	Servizio di verifica dello stato dei certificati
OTP	One Time Password	è una password che è valida solo per una singola sessione di accesso o una transazione
P.A.	Pubblica Amministrazione	Amministrazioni pubbliche
P.D.S.	PKI Disclosure Statement	Documento che riassume i concetti principali del CP e del CPS
PKI	Public Key Infrastructure	Insieme delle attrezzature e del personale adibito al rilascio di certificati
Private key	Chiave Privata	L'elemento segreto della crittografia asimmetrica basata su coppie di chiavi
Public key	Chiave Pubblica	L'elemento distribuito della crittografia asimmetrica basata su coppie di chiavi
RA	Registration Authority	Entità responsabile delle procedure di enrolment, esegue l'identificazione e l'autenticazione del soggetto richiedente il rilascio del certificato
O.A.	Operatore Autorizzato all'inserimento dei dati	Figura professionale dell'Ente che coadiuva il futuro titolare dei certificati nella fase di presentazione dei dati necessari al

Termine/ Acronimo	Descrizione	Spiegazione
		rilascio dei certificati stessi. E' responsabile della corretta identificazione del futuro titolare
F.A.	Funzionario Autorizzato alla validazione dei dati	Figura professionale dell'Ente che richiede l'emissione dei certificati qualificati per il Titolare
Rete SPC	Servizio di Pubblica Connettività	Rete di interconnessione della PA.
TSA	Time Stamping Authority	La Certification Authority dedicata ad emettere esclusivamente certificati di marcatura temporale
QTSP	Qualified Trust Service Provider	Prestatore di Servizi Fiduciari Qualificati (ex Certificatore)
TSR	Time Stamp Response	Struttura contenente al suo interno un Time Stamp Token e la risposta ricevuta dalla corrispondente Time Stamp Unit
TST	Time Stamp Token	Marcatura Temporale: associa data e ora certe e legalmente valide ad un documento informatico.
TSU	Time Stamping Unit	Il servizio software che, dotato di certificato di marcatura temporale, emette marcature temporale firmandole digitalmente con detto certificato

RIFERIMENTI

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

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

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

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

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

[RFC2560] "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP"

[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 » Mar 2014

[ETSI 862] ETSI TS 101 862 v.1.3.3 – "Qualified Certificate profile", Jan 2006.

[ETSI 412] ETSI EN 319 412 v.1.1.3 – "Electronic Signatures and Infrastructures (ESI) ; Certificate Profiles ; Part 3 : Certificate Profile for certificates issued to legal persons" Apr. 2020.

[RFC2560] "Online Certificate Status Protocal - OCSP", (http://www.ietf.org/rfc/rfc2560.txt)

[RFC3647] "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", (http://www.ietf.org/rfc/rfc3647.txt)

[DLGS] CAD - Codice Amministrazione Digitale – DLgs 82/2005 e ss.mm.

[DPCM] 22 febbraio 2013 e ss.mm.

[AGID_LG11] «Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate v.1.1» allegato alla «Determinazione 147/2019» di AgID (https://www.agid.gov.it/sites/default/files/repository_files/regole_tecniche_e_raccomandazioni_v1.1_0.pdf)

2 RESPONSABILITÀ DELLE PUBBLICAZIONI E DEL REPOSITORY

Questo capitolo contiene le disposizioni sull'identificazione del soggetto o dell'entità che gestisce il repository all'interno della PKI Difesa e la responsabilità nella pubblicazione delle informazioni e la frequenza con la quale esse vengono pubblicate.

Per "repository" si intende un insieme di archivi o registri on-line contenenti informazioni di interesse pubblico relativi ai certificati e al servizio di emissione e gestione degli stessi descritto in questo CP.

2.1 Gestione del repository

Il Centro di Certificazione del Comando per le Operazioni in Rete mette a disposizione degli utenti finali i seguenti repository:

- sito web https://pki.difesa.it/tsp – repository dove sono pubblicate le CRL e i documenti relativi alla PKI (CP, CPS, PDS, ecc…).

- Directory Server ldap://ldappkiff.difesa.it – repository dove sono pubblicati i certificati emessi e la CRL in vigore. Tale repository è raggiungibile solo internamente alla rete Difesa e dalle P.A. che hanno stipulato un accordo con il Ministero della Difesa.

Il Centro di Certificazione è responsabile della gestione di entrambe i repository.

La Certification Authority mantiene e gestisce un proprio repository ubicato all'interno dell'infrastruttura PKI Difesa, protetto da accessi esterni mediante firewall e dispositivi anti intrusione.

NOTA – Il repository consultabile al URL www.pki.difesa.it su protocollo http è stato inibito alla visualizzazione in http reindirizzando tale URL al repository https://pki.difesa.it/tsp.
Il repository www.pki.difesa.it è stato mantenuto disponibile su protocollo http solo ed esclusivamente per il download delle CRL

2.2 Informazioni pubblicate

Il Centro di Certificazione pubblica sul proprio sito web https://pki.difesa.it/tsp la seguente documentazione e software:

- Certification Practice Statement (CPS);
- Certificate Policy (CP);
- Terms and Conditions (T&C);
- PKI Disclosure Statement (PDS);
- Software per l'utilizzo del modello ATe (CMD API);
- Software per l'impiego della Firma Digitale (Kit di Firma);
- L'elenco delle liste di revoca (CRL);
- Certificati della CA.

I suddetti siti web sono disponibili 24 ore su 24, 7 giorni su 7.

Inoltre la CA pubblica sul Directory Server i certificati emessi e la CRL in vigore.

2.3 Tempi e frequenza delle pubblicazioni

Tutta la documentazione e i software presenti sul sito web vengono pubblicati ad ogni aggiornamento. La documentazione è pubblicata in formato PDF.

I certificati vengono pubblicati sul directory server al momento della loro emissione.

Le CRL vengono emesse e pubblicate almeno con frequenza giornaliera. Per maggiori dettagli si rimanda alla sezione 4.8**.**

2.4 Controllo degli accessi

Tutto il materiale pubblicato sul sito web del Centro di Certificazione https://pki.difesa.it/tsp è consultabile e/o scaricabile liberamente.

L'accesso al registro dei certificati avviene mediante Lightweight Directory Access Protocol (LDAP) ed è consultabile in sola lettura sul ramo di firma solo dall'interno della rete Difesa e dall'interno degli Enti/P.A. che hanno firmato un accordo di collaborazione con il Ministero della Difesa.

Gli utenti non autorizzati possono consultare LDAP in sola lettura per il solo recupero della CRL.

La modifica del contenuto del registro dei certificati digitali è possibile solo al personale del Centro di Certificazione e alla CA stessa.

Il servizio di Online Certificate Status Protocol (OCSP) è consultabile liberamente all'indirizzo http://ocsppkiff.difesa.it

3 IDENTIFICAZIONE ED AUTENTICAZIONE (I&A)

Questo capitolo descrive le procedure utilizzate per autenticare l'identità e/o altri attributi per il certificato dell'utente da parte della CA di Firma o della Registration Authority (RA) prima del rilascio dello stesso.

3.1 Regole di nomenclatura

I certificati emessi dalla PKI Difesa seguono lo standard X.509v3.

Nel campo Alternative Subject Name dei certificati è riportato, come "Nome RFC822", l'indirizzo e-mail del Titolare del certificato.

Il dettaglio dei contenuti è riportato nella seguente tabella:

CA Firma	
Common Name (CN)	Ministero della Difesa - CA di Firma Digitale
SERIALNUMBER	97355240587
Organizational Unit (OU)	S.M.D. – Comando per le Operazioni in Rete
Organizzation (O)	Ministero della Difesa
Country Code (C)	IT

Certificato di Firma - Firma Remota/Automatica	
dnQualifier	ID Carta - ID Ente + Nr progressivo
Common Name (CN)	NOME COGNOME
serialNumber	TINIT-CODICEFISCALE
GN	NOME
SN	COGNOME
Organizational Unit (OU)	NomeUnitàOrganizzativa
Organization (O)	NomeOrganizzazione/CodiceFiscaleOrganizzazione
Country Code (C)	IT

Certificato di Firma Automatica S.M.D./COR	
dnQualifier	ID + Nr progressivo
Common Name (CN)	NOME COGNOME
serialNumber	TINIT-CODICEFISCALE
GN	NOME
SN	COGNOME
Organizational Unit (OU)	IPAIT-AOO_*CODICEAOO* (Codice della AOO secondo IPA)
Organization (O)	NomeOrganizzazione
Country Code (C)	IT

Certificato di Firma con Sigillo Digitale	
dnQualifier	ID Ente + Nr unvico Ente
Common Name (CN)	Comando/Ente (AOO)
2.5.4.97 (Organization Identifier)	Codice IPA Ente

Certificato di Firma con Sigillo Digitale	
Organization (O)	NomeOrganizzazione
Country Code (C)	IT

I certificati dei titolari e della CA di firma contengono i nomi con una semantica comprensibile, per consentire la determinazione dell'identità del Titolare e della CA di Firma[3].

I nomi del Titolare dei certificati e dell'ente emittente sono registrati come Distinguished Name nei campi subject e issuer del certificato.

I certificati dei titolari sono rilasciati a persone fisiche. All'interno del certificato sono riportati i dati della persona privi di pseudonimi.

All'interno dei certificati di firma contenuti nel modello ATe è definito come valore del campo Nome Alternativo del Soggetto RFC822 la mail del Titolare del certificato.

I campi del Distinguished Name e i relativi contenuti, seguono le specifiche della firma digitale in italia, in particolare la Determinazione AgID nr. 121/2019 (che ha sostituito la Deliberazione CNIPA 45/2009).

La combinazione dei campi Distinguished Name elencati rende il nome di un Titolare unico per via del componente dnQualifier, che varia a ogni emissione per lo stesso Titolare.

Per i certificati di firma contenuti internamente al modello ATe l'univocità è fornita dal dnQualfier che corrisponde al ID della carta (ad es. MMDA12345).

Per i certificati di firma remota il dnQualifier è un codice progressivo della forma C4DRxxxxxxxx che cambia a ogni emissione.

Per i certificati di firma automatica il certificato è univocamente associato dal valore del dnQualiier che è della forma XXXnnnnnn (identificativo Ente + numero progressivo). Essendo il dnQualifier unico per ciascun Titolare di certificato di firma automatica, questi non può avere più di un certificato di firma automatica attivo.

Per i certificati di sigillo digitale il certificato è univocamente associato dal valore del dnQualiier che è della forma XXXnnnnnn (identificativo Ente + numero univoco Ente). Essendo il dnQualifier unico per ciascun Titolare di certificato di sigillo digitale, questi non può avere più di un certificato.

Il certificato del OCSP è reso univoco dal Common Name che al suo interno contiene la data di emissione del certificato stesso.

3.2 Validazione iniziale dell'identità

In questo paragrafo sono descritte le procedure di identificazione e autenticazione per l'iniziale registrazione di ciascun tipo di soggetto.

Il processo di registrazione dei titolari avviene attraverso una procedura informatica.

[3] Il campo OU contenuto all'interno del certificato di CA riporta il nome che aveva il Comando ospitante il Centro di Certificazione all'atto dell'emissione del certificato.

FIRMA SU MODELLO ATE

Di seguito sono evidenziate le modalità di acquisizione per il personale appartenente alla Difesa e alle P.A. che hanno stipulato un accordo di collaborazione con la Difesa per il rilascio del modello ATe e dei certificati inseriti nella carta.

L' Operatore autorizzato all'inserimento dei dati (O.A.) procede all'acquisizione dati ai fini dell'emissione del modello ATe previa presentazione da parte dell'interessato della seguente documentazione:

- documento d'identità in corso di validità;
- modulo di richiesta emissione modello ATe e relativa informativa, debitamente compilati e firmati.

L' Operatore autorizzato all'inserimento dei dati (O.A.) effettua le seguenti operazioni:

- acquisisce i dati attraverso specifiche procedure;
- convalida i dati raccolti, e sottoscritti dall'interessato mediante firma grafometrica, con la propria firma qualificata.

La procedura d'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, informativa compresa, e firmata dal Comandante/Dirigente responsabile.

Terminata la procedura di raccolta dei dati, il richiedente sottoscrive i dati con firma grafometrica e l'Operaore Autorizzato al trattamento dei dati valida l'acquisizione apponendo la propria firma qualificata con il certificato di firma presente sul proprio modello ATe.

Terminata la procedura d'acquisizione, il Funzionario Autorizzato alla validazione dei dati della LRA convalida i dati attraverso un'apposita procedura informatica apponendo la propria firma qualificata e provvede all'invio dei dati al CMS.

L'operatore CMS (OPCMS), prima di avviare il processo di stampa esegue un'ulteriore verifica di qualità visiva dei dati acquisiti.

Il CMS esegue una verifica dei dati pervenuti e richiede l'emissione dei certificati alla C.A. di Firma durante la personalizzazione del modello ATe.

Gli operatori FA, OA e OPCMS vengono nominati con un atto formale da parte dei Comandanti/ Dirigenti responsabili e possono operare esclusivamente dopo aver eseguito un'autenticazione forte mediante il proprio modello ATe.

FIRMA AUTOMATICA DI SGD

Per il rilascio dei certificati di firma automatica di SGD utilizzati nei sistemi di protocollazione la procedura di identificazione è la seguente:

Il richiedente, nominato con apposito Atto, compila il modulo di richiesta, lo firma con il certificato di firma presente all'interno del proprio Mod. ATe e lo invia al referente unico del protocollo informatico per l'A.D. che convalida la richiesta controfirmandola con il certificato di firma presente all'interno del proprio Mod. ATe.

Tutti i moduli di richiesta certificato contengono almeno le seguenti voci:

- Nome e Cognome;
- Codice Fiscale;
- Mail istituzionale del dominio difesa;
- AOO di appartenenza

FIRMA AUTOMATICA/ SIGILLO DIGITALE DELLA DIFESA SMD/COR

Per il rilascio del certificato di firma automatica/sigillo digitale della Difesa il Titolare compila un modulo PDF preformattato con all'interno i dati relativi alla richiesta e le informazioni che saranno incluse nel certificato (ad es. Cognome, Nome, Codice Fiscale per la Firma Automatica mentre per il Sigillo nome descrittivo, organizzazione, AOO, ECC...) Il titolare firma digitalmente il modulo PDF con il proprio modello ATE (il certficato di firma è rilasciato dal medesimo TSP) in formato PadES e lo invia al TSP.
L'operatore del TSP, ricevuto il modulo, con l'ausilio di strumenti informatici verfica il modulo ricevuto in termini di Validità della firma, presenza dei dati obbligatori, correttezza dei dati interni.
Terminato tale controllo in maniera automatica il sistema crea l'utenza sull'appliance di firma (HSM) generando i segreti in modo randomico, avvia la generazione della chiava privata sull'appliance, ottiene la richiesta di certificato (CSR), la sottopone alla Certification Authority ottenendo il certifcato che andrà scritto sul HSM.
In caso di successo, quindi, il sistema crea una busta cieca digitale PDF contenente i segreti e cifra tale busta utilizzando come certificato destinatario quello corrispondente all'utente che ha firmato il modulo di richiesta (il certificato viene recuperato in automatico dalla directory LDAP del TSP).
Infine, il sistema invia una email al titolare con la comunicazione dell'emissione del servzio richiesto ed in allegato la busta cieca digitale cifrata. In questo modo solo il titolare può visualizzare i contenuti della busta dopo averli decifrati con il proprio modello Ate (certificato di cifra) tramite l'applicazione software Kit di Firma.

FIRMA REMOTA

L'utente richiedente il certificato di firma remota invia un modulo di richiesta certificato debitamente compilato e firmato con il certificato di firma presente sul proprio modello ATe al Centro di Certificazione.

Per il rilascio del certificato di firma remota, l'operatore del Centro di Certificazione riceve il modulo di richiesta di certificato firmato con il certificato di firma del richiedente presente all'interno del modello ATe e ne verifica la correttezza.

L'operatore usando un apposito processo informatico genera l'utente all'interno dell'HSM di Firma Remota ed informa l'utente dell'avvenuta operazione.

CONSIDERAZIONI COMUNI A TUTTI I TIPI DI CERTIFICATO

La dimostrazione del possesso, da parte del richiedente, della chiave privata corrispondente al certificato richiesto si basa sulla verifica crittografica della CSR (*Certificate Signing Request*) inviata alla CA di Firma.

Il CMS o il referente unico del protocollo informatico per l'A.D. o il richiedente per il tramite del portale di firma remota, a seconda del tipo di emissione di certificato, invia la chiave pubblica alla CA di Firma sotto forma di CSR in formato PKCS#10 [RFC2314].

Solo le entità registrate (CMS, portale di firma remota, referente unico del protocollo informatico per l'A.D.) possono richiedere l'emissione del certificato attraverso una consegna affidabile della richiesta di certificato stessa.

Ciascuna di queste entità è dotata di un particolare certificato di firma con il quale controfirma le richieste di certificato (CSR) che poi vengono sottomesse alla Registration Authority della CA di Firma. La RA dopo aver controllato l'integrità della richiesta, verifica l'autorizzazione del certificato usato e, se valida, sottopone la richiesta CSR originale alla CA di Firma.

Non sono accettate richieste di certificato proveniente direttamente da individui al di fuori del Ministero della Difesa e degli Enti/PA che hanno stipulato con la Difesa un accordo di collaborazione.

I certificati emessi non contengono informazioni che non possono essere verificate. Tutti i dati riportati nei certificati emessi sono verificati e sottoscritti dal Titolare durante la fase di acquisizione.

Il richiedente è responsabile penalmente della correttezza dei dati sottoscritti al momento della procedura di acquisizione, ai sensi del D.P.R. n.445/2000, art.76.

La CA di Firma non esegue alcuna validazione dei dati del richiedente, controlla esclusivamente che il DN sia unico per i certificati in corso di validità e che sia unica la chiave pubblica.

3.3 I&A per le richieste di rinnovo

Non applicabile in quanto la durata dei certificati di Firma contenuti all'interno del modello ATe è pari alla durata di vita del modello ATe stesso. Alla scadenza del modello ATe verrà emessa una nuova carta con nuovi certificati rieseguendo il medesimo processo della sezione 3.2.

3.4 I&A per le richieste di sospensione o revoca

La modalità di identificazione ed autenticazione delle richieste di sospensione o revoca dipende dal tipo di certificato.

FIRMA SU MODELLO ATE

Certificato di firma qualificata presente su modello ATe:

- sospensione: l'identificazione e autorizzazione del Titolare avviene mediante verifica del relativo Codice di Emergenza se l'operazione viene eseguita in modalità autonoma o assistita, oppure tramite verifica del documento di identità se l'operazione viene eseguita presso una LRA.

- revoca: l'identificazione e autorizzazione del Titolare avviene sempre presso una LRA mediante verifica del documento di identità del Titolare e, in caso di furto/smarrimento, verifica della denuncia presso le autorità.

Tutti gli operatori abilitati alla sospensione e/o revoca dei certificati, sono identificati mediante autenticazione forte con modello ATe.

Per i certificati presenti sul modello ATe deve essere fornito anche l'identificativo del modello ATe. In caso di revoca e di sospensione a lungo termine, la stessa deve essere restituita. In caso di furto o smarrimento deve essere presentata la denuncia alle competenti autorità.

FIRMA REMOTA

Per i certificati di firma remota il Titolare invia il modulo di richiesta di revoca debitamente compilato e firmato con il certificato presente sul modello ATe al Centro di Certificazione che esegue la revoca del certificato.

Per i certificati di firma remota il modulo deve contenere anche il seriale del OTP Token RSA.

FIRMA AUTOMATICA DI SGD

Per il certificato di firma automatica il Titolare del certificato invia il modulo di richiesta revoca/sospensione debitamente compilato e firmato con il certificato di firma presente sul modello AT al referente unico del protocollo informatico per l'A.D. che controfirma la richiesta e la invia al Centro di Certificazione che provvede ad eseguire la revoca del certificato.

La revoca del certificato di firma automatica e sigillo digitale può essere richiesta direttamente dal referente unico del protocollo informatico per l'A.D. nei casi previsti e riportati sul modulo, firmata solo dal referente.

La richiesta di sospensione/revoca del certificato include almeno le seguenti informazioni:

- Cognome e Nome;
- Codice Fiscale;
- Motivazione.

FIRMA AUTOMATICA/SIGILLO DELLA DIFESA SMD/COR

Per i certificati di firma automatica e sigillo della Difesa, il Titolare del certificato invia il modulo di richiesta revoca/sospensione debitamente compilato e firmato con il certificato di firma presente sul modello ATe al Centro di Certificazione che provvede ad eseguire la revoca del certificato.

La richiesta di sospensione/revoca del certificato include almeno le seguenti informazioni:

- Cognome e Nome;
- Codice Fiscale;
- Motivazione.

SIGILLO DELLA DIFESA SMD/COR SU SMART CARD

Il certficato di sigillo elettronico su Smart Card può essere richiesto dalle P.A. che hanno sottoscritto un accordo di collaborazione con il Ministero della Difesa, tale certificato viene richiesto solo ed esclusivamente per comprovante esigenze organizzative delle P.A. e viene rilasciato direttamente dal Centro di Certificazione al Titolare richiedente.

4 REQUISITI OPERATIVI DI GESTIONE DEI CERTIFICATI

4.1 Richiesta del certificato

Una richiesta di certificato di firma può essere sottoposta alla CA di Firma:

- dal CMS previa autorizzazione del FA, per i certificati di firma presenti all'interno del modello ATe.
- dall'operatore presente al Centro di Certificazione previa approvazione del referente unico del protocollo informatico per l'A.D., per i certificati di firma automatica di SGD;
- dall'operatore presente al Centro di Certificazione previa approvazione della corretta compilazione della richiesta efefttuata da parte dell'utente, per i certificati di firma automatica e sigillo digitale della Difesa SMD/COR;
- dall'utente richiedente, previa approvazione del Centro di Certificazione, per i certificati di firma remota.

Per richiedere l'emissione di un certificato debbono essere seguite le procedure descritte al paragrafo 3.2.

Durante la fase di identificazione e autenticazione il richiedente è responsabile penalmente delle dichiarazioni da lui rese ai sensi del D.P.R. n.445/2000, art.76, mentre i vari operatori sono responsabili della verifica della corrispondenza e completezza dei dati dichiarati dall'utente.

4.2 Processo di approvazione della richiesta

FIRMA SU MODELLO ATE

OA e FA approvano la richiesta di emissione Mod. Ate e certificato di firma solo se ha avuto successo l'identificazione e l'autenticazione di tutti i dati forniti dall'utente richiedente.

Il rifiuto e/o l'approvazione dell'emissione di un Mod ATe e quindi del relativo certificato di firma in esso contenuto può dipendere dal:

- Operatore autorizzato all'inserimento dei dati verifica la correttezza e la completezza dei dati presentati dall'utente.

- Funzionario Autorizzato alla validazione dei dati della LRA che, sulla base della verifica dei dati acquisiti dall' Incaricato del Trattamento dei Dati, può decidere se approvare o rifiutare la richiesta di emissione della carta.

- Operatore CMS che, prima dell'emissione del modello ATe, esegue un'ulteriore controllo per verificare che la foto del richiedente acquisita dall'OA e validata dal FA rispetti gli standard previsti.

FIRMA AUTOMATICA DI SGD

Per l'emissione dei certificati di firma automatica di SGD, il referente unico del protocollo informatico per l'A.D. approva la richiesta di emissione solo se ha avuto successo l'identificazione e l'autenticazione di tutti i dati forniti dall'utente richiedente.

Per i certificati di firma automatica l'approvazione o il rifiuto dipende dalla verifica dei dati del richiedente eseguita prima dal referente unico del protocollo informatico per l'A.D. e successivamente dall'Operatore del Centro di Certificazione.

FIRMA AUTOMATICA/SIGILLO DIGITALE DELLA DIFESA SMD/COR

Per i certificati di firma automatica/sigillo digitale della Difesa il Capo Centro Certificazione approva la richiesta per l'emissione del certificato di firma automatica/sigillo digitale se ha avuto successo l'identificazione e l'autenticazione di tutti i dati forniti dall'utente richiedente.

FIRMA REMOTA

Per i certificati di firma remota il Capo Centro Certificazione approva la richiesta per l'emissione del certificato di firma remota se ha avuto successo l'identificazione e l'autenticazione di tutti i dati forniti dall'utente richiedente.

Per i certificati di firma remota l'approvazione o il rifiuto della richiesta di emissione del certificato dipende direttamente dal Capo Centro di Certificazione che, eseguita la verifica della correttezza dei dati presentati dal richiedente, può decidere se approvare o meno la richiesta.

CONSIDERAZIONI COMUNI A TUTTI I TIPI DI CERTIFICATO

La CA di Firma accetta le richieste di certificati (CSR) in formato PKCS#10 in conformità alle specifiche RFC 2986. Una richiesta nel dato formato dimostra il possesso della chiave privata corrispondente.

Per esigenze di servizio particolari, richieste di emissioni possono essere approvate con procedura di urgenza. Tali procedure comunque non variano i processi elencati in questo documento, bensì solo la priorità della gestione delle code.

4.3 Emissione del Certificato

Non appena viene sottoposta una richiesta di certificato alla CA di Firma, questa emette il certificato, lo memorizza sul proprio database e ne dà evidenza pubblicandolo sul Directory Server.

Un certificato di firma contenuto internamente al Mod. ATe viene generato ed emesso non appena il CMS sottopone la richiesta CSR nel formato PKCS#10 alla CA di Firma.

I certificati di firma remota vengono generati ed emessi dalla CA di Firma non appena il richiedente porta a termine la procedura di emissione certificato dal portale di firma remota.

I certificati di firma automatica e sigillo digitale vengono emessi non appena l'Operatore del Centro di Certificazione ha ultimato le procedure preliminari per sottoporre la richiesta e ha sottoposto la richiesta di certificato CSR nel formato PKCS#10 alla CA di Firma.

Il CMS notifica al richiedente del modello ATe l'emissione della propria carta e dei certificati in essa contenuti, inviando alla mail istituzionale dell'interessato, un apposito codice di visualizzazione, utilizzabile una sola volta e necessario per la distribuzione della carta, il recupero dei codici PIN e PUK per l'utilizzo della carta e dei certificati.

Per i certificati di firma remota la notifica dell'emissione del certificato all'utente avviene attraverso il portale di firma remota stesso appena è stata ultimata la procedura di generazione.

Per i certificati di firma automatica di SGD il Centro di Certificazione comunica l'avvenuta generazione del certificato al referente unico del protocollo informatico per l'A.D. che è responsabile della notifica al Titolare, della generazione del certificato.

Per i certificati di firma automatica/sigillo digitale della Difesa SMD/COR il Centro di Certificazione comunica l'avvenuta generazione del certificato e l'attivazione del servizio richiesto al titolare a mezzo mail cifrata.
La suddetta mail è generata in automatico dal sistema.

4.4 Accettazione del certificato

Durante la fase di distribuzione della carta Titolare presso la LRA, il Titolare accetta il certificato e ne dà evidenza tramite firma grafometrica.

Per i certificati di firma automatica SGD il certificato è considerato accettato dal Titolare qualora non vengano evidenziati dal referente unico del protocollo informatico per l'A.D. o/e dal Titolare stesso degli errori nei dati del certificato in tempi ragionevoli.

La CA di Firma pubblica i certificati emessi sul Directory Server all'indirizzo ldap://ldappkiff.difesa.it

L'emissione del certificato di firma, contenuto all'interno del modello ATe e del certificato di firma remota, viene notificata solo al Titolare del certificato. Per il primo la notifica avviene via mail istituzionale, mentre per il secondo attraverso il portale di firma remota.

L'emissione del certificato di firma automatica di SGD è comunicato via mail al referente unico del protocollo informatico per l'A.D. che a sua volta, espletate le procedure informatiche di caricamento del certificato all'interno dell'HSM, inoltra la comunicazione al Titolare del certificato.

Per i certificati di firma automatica/sigillo digitale della Difesa SMD/COR il certificato è considerato accettato dal Titolare qualora non vengano evidenziati dal Titolare stesso degli errori nei dati del certificato in tempi ragionevoli.

4.5 Uso della coppia di chiavi e del certificato

L'uso della chiave privata corrispondente alla chiave pubblica è consentita solo dopo che il Titolare ha accettato il Certificate Policy ed il certificato.

Il certificato deve essere usato in accordo con le leggi e con i termini indicati nel CP e nel CPS. Il sottoscrittore usa la coppia di chiavi ed il certificato per firmare i documenti digitali.

Le parti interessate devono valutare indipendentemente:

- l'appropriatezza dell'uso del certificato per uno specifico scopo che non sia vietato da questo CP. Il Prestatore di Servizi Fiduciari Qualificati non è responsabile di questa valutazione.
- L'utilizzo del certificato in accordo con l'estensione KeyUsage del certificato stesso (ad esempio: se il valore dell'estensione è diverso da "Non Ripudio", il certificato non può essere usato per la firma).
- Lo stato del certificato mediante CRL/OCSP e lo stato della CA di Firma emettitrice mediante la Trusted List europea e/o nazionale.

Supponendo che l'uso del certificato sia appropriato, le parti interessate devono utilizzare software e/o hadware appropriato per la verifica delle firme apposte tramite certificati emessi da questa CA di Firma.

4.6 Rinnovo del certificato

Non è previsto al momento un rinnovo per alcun tipo di certificato di firma.

Il certificato di firma contenuto all'interno del modello ATe ha una durata di vita pari alla durata del modello ATe stesso. Alla sua scadenza il Titolare dovrà richiedere l'emissione di una nuova carta e di un nuovo certificato.

Per i certificati di firma remota, automatica e sigillo alla loro regolare scadenza verranno emessi nuovi certificati inibendo l'uso dei precedenti.

4.7 Rinnovo della chiave

Non previsto per quanto indicato al punto 4.6 e 3.3.

Nel caso in cui l'utente finale (Titolare) decida di utilizzare una nuova chiave, egli deve necessariamente fare richiesta di un nuovo certificato e di un nuovo modello ATe, in sostituzione di quello in uso.

Per ogni nuovo certificato di firma viene generata una nuova coppia di chiavi effettuando il medesimo processo di generazione chiavi e certificato eseguito la prima volta e descritto al 4.1 e al 4.2 ed il 4.4.

4.8 Modifica del Certificato

Un certificato, essendo firmato dalla CA emittente, non può essere "modificato". Per rimediare ad eventuali errori nella generazione del certificato, dunque, è necessario, per evidenti ragioni di sicurezza, revocare quello errato ed emetterne uno nuovo. Le procedure seguite sono le stesse descritte in precedenza nel documento.

4.9 Revoca e sospensione del certificato

4.9.1 Circostanze per la revoca

E' possibile richiedere la revoca di un certificato:

- per sospetta compromissione;
- per furto o smarrimento;
- per inefficienza del chip o danneggiamento del modello ATe;
- per dati errati contenuti nel certificato;
- per terminazione del rapporto di lavoro (licenziamento, collocamento in congedo assoluto, pensionamento, decesso, ecc);
- per perdita delle credenziali di utilizzo del certificato in caso di certificato firma automatica e remota.

4.9.2 Chi può richiedere la revoca

La revoca può essere richiesta:

- dal Titolare del certificato;
- dal FA o dal CMS nei casi di sospetto uso improprio del certificato;
- dal Centro di Certificazione;
- dal referente unico del protocollo informatico per l'A.D..

4.9.3 Procedure per richiedere la revoca

FIRMA SU MODELLO ATE

In caso di furto o smarrimento, il Titolare del certificato richiede come prima cosa la sospensione di emergenza, attraverso il portale fornendo il Codice Fiscale ed il Codice di Emergenza.

In caso sia impossibilitato all'accesso al portale, il Titolare contatta il call center e chiede la sospensione dopo essere stato identificato mediante alcune domande sui propri dati e una porzione del Codice di Emergenza.

Se anche ciò non è possibile, contatta la propria LRA e richiede la sospensione del certificato all' OA il quale dà seguito alla richiesta.

La sospensione viene tramutata in richiesta di revoca a seguito della presentazione della denuncia di furto e/o smarrimento all' OA, il quale identifica l'utente richiedente attraverso un documento di identità in corso di validità e raccoglie i dati necessari.

Il Funzionario autorizzato alla validazione dei dati valida la richiesta di revoca inviando i dati al CMS, dove l'operatore esegue la revoca.

In caso di deterioramento della carta o del chip, si procede direttamente con la richiesta di revoca presso la LRA. L' OA inserisce i dati richiesti, li sottoscrive e li invia al FA, che li valida per il successivo invio al CMS, dove l'operatore abilitato esegue la revoca.

Una sospensione si tramuta in ogni caso in una revoca, passati 15 giorni dalla data di sospensione, entro i quali non è stata manifestata l'esigenza di riattivazione del certificato. Tale procedura non vale per i certificati sospesi a lungo termine.

La revoca d'ufficio viene eseguita direttamente dall'operatore del CMS o della PKI Difesa nei casi previsti dalla SMD-I-009.

FIRMA REMOTA, AUTOMATICA E SIGILLO DIGITALE

Per i certificati di firma remota e/o automatica il Titolare del certificato richiede la revoca del certificato compilando e firmando l'apposito modulo.

Il modulo di revoca dei certificati di firma remota e automatica/sigillo SMD/COR è inviato al Centro di Certificazione mentre quello per i certificati di firma automatica SGD viene inviato prima al referente unico del protocollo informatico per l'A.D. che lo controfirma e lo inoltra al Centro di Certificazione.

Il referente unico del protocollo informatico per l'A.D. può richiedere direttamente la revoca di un certificato di firma automatica di terze persone per cessazione dell'attività o per dati non corretti.

4.9.4 Periodo di tolleranza di una richiesta di revoca

Le richieste di revoca devono essere processate il più presto possibile.

Le richieste di revoca vengono processate non appena queste sono sottoposte alla CA.

4.9.5 Frequenza di emissione della CRL

La CRL viene emessa almeno con frequenza giornaliera ed hanno una durata di 7 giorni.

In caso di revoca per compromissione, furto/smarrimento o in caso di sospensione o di riattivazione, la CRL viene emessa contestualmente all'operazione eseguita.

La CRL viene pubblicata immediatamente, e comunque in un tempo ragionevolmente breve, dopo la sua emissione, sui repository indicati nelle sezioni precedenti.

4.9.6 Disponibilità del controllo on-line dello stato di revoca

Il controllo della stato di revoca può avvenire mediante interrogazione del servizio OCSP sempre disponibile (24 ore su 24) salvo attività di manutenzione o guasti.

Il servizio di OCSP è consultabile liberamente all'indirizzo http://ocsppkiff.difesa.it

4.9.7 Requisiti per il controllo on-line della revoca

Il servizio è disponibile agli utenti che dispongono di un'applicazione che esegua la verifica conformemente al RFC 2560.

4.9.8 Altre forme di avvisi di revoca disponibili

All'atto della revoca viene data comunicazione al Titolare mediante l'invio automatico di una mail.

4.9.9 Circostanze per la sospensione

Un certificato di firma viene sospeso cautelativamente in caso di sospetto furto o smarrimento.

Può inoltre essere sospeso per particolari esigenze d'ufficio, quale:

- personale sottoposto a fermo giudiziario;
- personale allontanato dall'attività lavorativa per un determinato periodo di tempo.
- ogni altro motivo che possa dare adito ad un uso improprio della carta.

Nel caso di una sospensione che si traduce in revoca definitiva, la data di decorrenza di quest'ultima coincide con la data della sospensione.

4.9.10 Chi può richiedere la sospensione

La richiesta di sospensione di un certificato di firma è presentata dal Titolare:

- per il certificato di firma a bordo del modello ATe, presso una qualunque Local Registration Authority (LRA) o, in alternativa, via WEB o telefonicamente;
- per i certificati di firma automatica, al referente unico del protocollo informatico per l'A.D.;
- per i certificati di firma remota, direttamente al Centro di Certificazione
- per i certificati di firma automatica e sigillo digitale della Difesa SMD/COR direttamente al Centro di Certificazione.

Il responsabile della LRA o il referente unico del protocollo informatico per l'A.D. ed anche il CMS ed il Centro di Certificazione, ove ne ricorrano giustificati motivi, possono procedere autonomamente alla procedura di sospensione. L'operazione viene comunicata immediatamente tramite email al Titolare, nella quale viene anche riportata la motivazione.

4.9.11 Procedure per le richieste di sospensione

Le procedure per richiedere la sospensione standard sono le medesime seguite per la richiesta di revoca indicate nel paragrafo 4.9.3.

Per particoli esigenze di servizio il CMS può eseguire una richiesta di sospensione a lungo termine per i titolari di Mod.ATe.

Passati 15 giorni, una sospensione viene tramutata in revoca, con decorrenza dalla data di sospensione.

La sospensione a lungo termine, invece, non ha limiti di tempo fissati ed è in funzione delle esigenze dell'Organizzazione.

4.10 Servizio di stato del certificato

La PKI Difesa mette a disposizione servizi di controllo dello stato del certificato, come CRL e OCSP.

Lo stato dei certificati (attivo, sospeso, revocato) è reso disponibile a tutti gli interessati mediante pubblicazione della Certificate Revocation List (CRL) nel formato definito dalla specifica [RFC5280].

La CA di Firma rende, inoltre, disponibile anche un servizio OCSP (On-line Certificate Status Provider) conforme alla specifica [RFC2560].

Il servizio di stato del certificato, mantiene lo stato dei certificati anche dopo la loro scadenza naturale. In particolare per la CRL, tale condizione viene indicata mediante un'estensione della CRL come specificato nella sezione 7.2.

Il servizio di stato del certificato, mantiene lo stato dei certificati anche dopo la loro scadenza naturale. In particolare per la CRL, tale condizione viene indicata mediante un'estensione della CRL come specificato nella sezione 7.2.2.

L'informazione dello stato di revoca nelle CRL viene rinnovata con cadenza almeno giornaliera mentre sull'OCSP avviene in tempo reale.

In caso di compromissione della CA, il QTSP pubblicherà sul proprio sito l'ultima CRL emessa prima della accertata compromissione, comprensiva della relativa dati di emissione. Contestualmente verrà emessa una nuova CRL con data di scadenza prolungata alla data di scadenza delle CA. Le due CRL saranno rese disponibili per un periodo pari a 20 dalla data di scadenza della CA.

In caso di terminazione del servizio di QTSP il servizio di OCSP non sarà mantenuto in vita mentre verrà emessa un'unica CRL prolungata con data di scadenza pari a quella della CA stessa. Questa CRL sarà pubblicata sul sito del certificatore e fornita ad AgiD per la conservazione a norma di legge.

La CRL è accessibile in due diverse modalità:

- con protocollo LDAP [RFC2251] sul server ldappkiff.difesa.it raggiungibile solo da rete Difenet e da rete SPC per le P.A. che hanno stipulato un accordo di collaborazione con il Ministero della Difesa;
- con protocollo HTTP [RFC2616] sul server www.pki.difesa.it.

Gli indirizzi completi LDAP ed HTTP della CRL sono inseriti nell'estensione CRLDistributionPoints del certificato.

La CRL viene rigenerata e ripubblicata:

- almeno ogni 24 ore, anche in assenza di nuove sospensioni o revoche;
- a seguito di una nuova sospensione, riattivazione o revoca con grave motivazione.

L'indirizzo del server OCSP è inserito nell'estensione AuthorityInformationAccess del certificato.

Il servizio OCSP è liberamente consultabile da chiunque.

Il servizio OCSP segue lo standard RFC 2560 ed è raggiungibile all'URL http://ocsppkiff.difesa.it.

L'accesso alla CRL e all'eventuale servizio OCSP è sempre disponibile (24 ore su 24), tranne in caso di fermi per manutenzione o di guasto. Nel caso di indisponibilità prolungata per cause non dipendenti dal TSP, quest'ultimo si impegna a ripristinare almeno il servizio di stato dei certificati tramite CRL entro 24 ore.

4.11 Fine della sottoscrizione

Il certificato di firma viene rilasciato ai soli dipendenti della Difesa e degli Enti/P.A. che hanno stipulato un accordo di collaborazione con il Ministero della Difesa ed è contenuto all'interno del modello ATe che è utilizzato anche come tessera di riconoscimento del pubblico dipendente ai sensi della normativa vigente.

L'accordo di servizio con il dipendente può definirsi quindi cessato, allo scadere dello status di pubblico dipendente.

I certificati di firma remota, automatica e sigillo sono rilasciati ai soli dipendenti della Difesa e degli Enti/P.A. che hanno sottoscritto un accordo di collaborazione che necessitano di queste tipologie di certificato.

In analogia ai certificati presenti sul modello ATe, anche per loro l'accordo di servizio è da intendersi cessato allo scadere dello status di dipendente in servizio attivo.

4.12 Key escrow e key recovery

Non è previsto il Key Escrow e il Key Recovery dei certificati di firma.

Il ripristino della chiave (key recovery) di certificazione è previsto, in caso di cancellazione involontaria o guasto o sostituzione del dispositivo HSM. Al fine di consentire il key recovery, la CA di Firma conserva una copia di backup della chiave secondo i meccanismi certificati da parte del produttore del dispositivo HSM.

5 MISURE DI SICUREZZA FISICA ED OPERATIVA

5.1 Sicurezza fisica

L'infrastruttura di sicurezza è costituita da strutture di difesa passiva (muri di cinta o perimetrali cancelli d'accesso controllati da remoto, porte blindate), da elementi di difesa attiva (servizio di vigilanza armata) e da componenti applicativi come ad esempio sistemi basati su token crittografici e codici personali o conoscenza di username e password di accesso.

L'integrità delle apparecchiature e degli impianti è mantenuta e verificata costantemente, in conformità con le attuali disposizioni normative al fine di evitare guasti che possano causare interruzione al funzionamento continuo dei servizi.

La struttura dove è ubicato il sito primario dell'infrastruttura PKI Difesa è sito il Comando per le Operazioni in Rete in via Stresa n. 31b, 00135 Roma.

Il sito di Disaster Recovery dell'infrastruttura PKI Difesa è situato presso il CED della caserma Ciarpaglini – Comando C4 Esercito ubicato in via Guido Reni n. 22, 00196 Roma.

L'accesso fisico all'edificio e ai locali interni è consentito solo al personale autorizzato. Gli ospiti devono esserepreventivamente autorizzati e registati prima di accedere agli stessi e devono essere accompagnati da personale abilitato.

L'accesso al CED del sito primario è consentito solo al personale autorizzato previa autenticazione mediante modello ATe.

L'infrastruttura di PKI Difesa è custodita all'interno di Rack ubicati nel Data Center del Comando. L'accesso al Data Center è consentito, unicamente al personale autorizzato a mezzo identificazione elettronica con Mod. ATe. L'accesso ai rack dell'Infrastruttura PKI è consentito unicamente al solo personale del Centro di Certificazione a mezzo chiavi elettroniche esclusive.

L'accesso alla struttura di DR della PKI Difesa è protetto da porte antiscasso, accessibili solo previa autorizzazione del personale preposto alla sorveglianza.

I locali sono muniti di impianto di condizionamento e l'impianto elettrico è protetto da cadute di tensione tramite un sistema UPS ed un gruppo elettrogeno.

Il sito primario sorge in un luogo sovra elevato della città e distante dal mare. Per entrambi i siti il Ministero della Difesa ha preso le ragionevoli precauzioni per minimizzare l'impatto dell'esposizione all'acqua.

Tutti i siti sono dotati di sofisticati sistemi per il rilevamento e soppressione degli incendi. Il personale viene inoltre adeguatamente formato affinché apprenda le procedure di evacuazione dell'edificio e di raduno presso il punto di raccolta designato.

Tutti i media contenenti software, dati, audit, informazioni di archiviazione e backup vengono registrati all'interno di sistemi di archiviazione ridondati e protetti con adeguati controlli fisici e logici per limitare l'accesso al personale autorizzato e proteggere tali supporti da danni accidentali (esempio acqua, fuoco, elettromagnetismo, ecc.).

Tutti i documenti e i materiali sensibili sono triturati prima dello smaltimento. Supporti utilizzati per raccogliere o trasmettere informazioni sensibili sono resi illeggibili prima dello smaltimento.

I dispositivi crittografici sono fisicamente distrutti o cancellati secondo la guida dei costruttori prima dello smaltimento.

La PKI Difesa esegue un backup di routine dei dati critici del sistema, dei dati del registro di controllo e delle altre informazioni sensibili.

I supporti di backup vengono memorizzati in modo sicuro all'interno di unità di storage.

5.2 Sicurezza delle procedure

Il Ministero della Difesa definisce e mantiene un Piano della Sicurezza che analizza gli asset e descrive le misure tecniche ed organizzative atte a garantire un adeguato livello di sicurezza delle operazioni.

Sono considerate persone di fiducia tutti i dipendenti, collaboratori e consulenti che hanno accesso ai sistemi di autenticazione e controllo o alle operazioni di crittografia che possono materialmente influenzare:

- il funzionamento e la validazione delle operazioni della PKI Difesa;
- i processi di accettazione, il rifiuto, o altro delle richieste di emissione certificato, di revoca, di rinnovo, o le informazioni di enrollment;
- il processo di acquisizione dei dati del Titolare.

Sono considerati di fiducia:

- gli Operatori autorizzati all'inserimento dei Dati;
- i Funzionari autorizzati alla validazione dei Dati;
- gli Operatori del CMS;
- il referente unico del protocollo informatico per l'A.D.;
- gli Operatori del Centro di Certificazione;
- il Prestatore di Servizi Fiduciari Qualificati;
- il Personale esterno preventivamente identificato ed autorizzato.

La PKI Difesa ha stabilito, mantiene e rafforza le procedure di controllo per garantire la separazione dei compiti basandosi sulla responsabilità lavorativa in modo da garantire che più persone è in grado di svolgere compiti delicati.

I compiti più delicati, come l'attivazione della CA di Firma e l'attivazione dei moduli crittografici richiedono la presenza di più persone di fiducia.

Queste procedure di controllo interno sono previste per assicurare che almeno due persone fidate abbiano sia l'accesso fisico sia logico al dispositivo.

Per tutto il personale di fiducia l'identità viene verificata utilizzando prioritariamente il modello ATe ovvero un documento d'identità in corso di validità.

I ruoli che richiedono la separazione dei compiti sono:

- le operazioni di acquisizione e validazione delle richieste di carte e/o certificati;
- le operazioni sui dispositivi hardware e/o software su cui sono immagazzinate le chiavi della CA di Firma;
- le operazioni per la richiesta di revoca.

5.3 Sicurezza del personale

Il personale addetto al servizio ha una esperienza pluriennale nel campo della definizione, sviluppo e gestione di servizi di PKI Difesa ed ha ricevuto un'adeguata formazione sulle procedure e sugli strumenti da utilizzare nelle varie fasi operative.

Il personale abilitato ad operare presso la PKI Difesa ha un'esperienza pluriennale ed è munito di particolari autorizzazioni di sicurezza (Nulla Osta di Segretezza – NOS) .

Prima di ritenere un dipendente idoneo per un ruolo presso il Centro di Certificazione, vengono eseguiti una serie di controlli sui requisiti posseduti:

- conferma dei precedenti incarichi;
- controllo delle referenze professionali;
- controllo del possesso del Nulla Osta di Segretezza - NOS
- conferma delle certificazioni professionali o equipollenti acquisite in ambito accademico;
- ricerca di eventuali precedenti giudiziari/penali.

Il Ministero della Difesa fornisce al proprio personale la formazione al momento dell'assegnazione dell'incarico presso il Centro di Certificazione, nonché la necessaria formazione on-the-job necessaria per svolgere le mansioni con competenza e in modo soddisfacente.

I programmi di formazione del Ministero della Difesa sono adeguati alle responsabilità dell'individuo e trattano i seguenti argomenti:

- concetti di base sulle PKI Difesa;
- responsabilità del lavoro quotidiano;
- sicurezza e policy operative e procedurali;
- utilizzo e funzionamento di hardware e software utilizzato e distribuito;
- procedure di gestione e comunicazione degli incidenti di sicurezza;
- Disaster Recovery e Business Continuity.

Il Ministero della Difesa predispone corsi formativi e di aggiornamento al proprio personale nella misura e nella frequenza necessarie per garantire che tale personale mantenga il necessario livello di competenza per eseguire le mansioni in sicurezza senza soluzioni di continuità ed interruzione dei servizi.

All'interno della PKI Difesa, la rotazione dei compiti è eseguita in modo che ci sia sempre un periodo di affiancamento per consentire il passaggio di conoscenze tra il personale che lascia l'incarico e quello subentrante.

La frequenza della rotazione dei compiti è dettata dalle policy di impiego del personale vigenti presso il Ministero della Difesa.

In caso di azioni non autorizzate le sanzioni previste sono quelle indicate dal Codice dell'Ordinamento Militare.

Tutte le azioni sono soggette alla Normativa Italiana.

In circostanze limitate, consulenti esterni possono essere autorizzati a ricoprire posizioni di fiducia. Qualsiasi consulente è tenuto agli stessi criteri funzionali e di sicurezza che si applicano al personale della PKI Difesa impiegato in una posizione analoga. In caso di azioni non autorizzate il consulente viene denunciato alle autorità di polizia.

Ai consulenti esterni che non hanno completato le procedure di controllo indicate al punto 5.3 è consentito l'accesso alle strutture sicure della PKI Difesa solo se se vengono accompagnati e controllati dalle persone di fiducia del Centro di Certificazione.

Il Centro di Certificazione fornisce ai propri dipendenti la formazione necessaria e la documentazione per svolgere i propri compiti lavorativi in modo efficace.

5.4 Registrazione degli eventi

I principali eventi relativi alla gestione del ciclo di vita dei certificati, incluse le richieste di certificazione, sospensione o revoca, vengono registrati in forma elettronica.

Sono inoltre registrati anche altri eventi quali: gli accessi fisici all'infrastruttura, gli accessi logici al sistema di gestione dei certificato, l'entrata e l'uscita dai locali in cui si svolge l'attività di certificazione ed ogni movimento ritenuto utile a monitorare gli eventi.

Di ogni evento viene registrata la tipologia, la data e l'ora di occorrenza e, se disponibili, altre informazioni utili ad individuare il personale coinvolto nell'evento e l'esito delle operazioni.

L'insieme delle registrazioni costituisce il "giornale di controllo" (audit log). I file che lo compongono vengono trasferiti tutti i giorni su supporto permanente.

La PKI Difesa, in modalità manuale o automatica, registra i seguenti eventi significativi:

- Eventi di gestione del ciclo di vita delle chiavi della CA di Firma, tra cui:
  - generazione chiave, backup, archiviazione, recovery, conservazione e distruzione;
  - eventi legati al ciclo di vita dei device Crittografici (HSM).
- Eventi di gestione del ciclo di vita dei certificati CA e dei sottoscrittori:
  - richieste di certificato, revoche, sospensioni, riattivazioni;
  - richieste processate con o senza successo;
  - generazione ed emissioni di certificati.
- Eventi di sicurezza:
  - accessi fisici ai rack attraverso le chiavi elettroniche del Data Center:
  - accesso ai sistemi;
  - Log dei firewall;
  - azioni sulla sicurezza eseguiti dal personale;
  - crash dei sistemi o guasti hardware e altre anomalie.
- Le voci di registro includono i seguenti elementi:
  - data e ora del record;
  - numero di serie o di sequenza del record, per le voci del giornale dei controlli;
  - identità dell'entità che firma la voce del registro di controll;
  - tipo di entry;
  - messaggio descrittivo.

I registri di controllo sono prodotti in tempo reale e vengono estratti ed esaminati con frequenza giornaliera.

I log di sistema e dei firewall sono generati in tempo reale ed archiviati con frequenza giornaliera.

Inoltre il Centro di Certificazione produce i verbali indicati nella tabella sottostante:

Nome Verbale	Frequenza
Verbale funzionalità del Disaster Recovery	Annuale
Verbale Conformità Prassi	Semestrale
Verbale Conformità dell'hardware	
Verbale Verifica Attivazione chiavi HSM	
Censimento Asset	
Verifica del contenuto del giornale di controllo	Bimestrale
Verifica integrità del giornale di controllo	Mensile
Verbale di verifica di integrità dei log di Auditing	

I log riguardanti il ciclo di vita di un certificato sono conservati per 20 anni.
I log dei server vengono conservati per un periodo pari a 3 mesi.
I log degli accessi alla gabbia sono conservati per un periodo di almeno 1 anno.
I log dei firewall sono conservati per un tempo non superiore ad 1 anno.
I log dei device crittografici hanno una periodo di retention di 4 mesi.

I log dei giornali di controllo sono conservati all'interno del database di storage e sono replicati sul sito del Disaster Recovery.

I log di audit della CA estratti giornalmente sono firmati dal responsabile dei servizi tecnici.

Una copia dei log di audit viene estratta giornalmente con procedura automatica dal database e viene copiata su un sistema di storage esterno dove vengono firmati digitalmente e conservati.

I log dei server sono estratti giornalmente.

I log di sistema vengono archiviati localmente e salvati su un sistema di storage esterno e sono conservati per 3 mesi.

L'infrastruttura è munita di un sistema di supervisione dei log di audit usato per monitorare gli eventi in tempo reale.

Sui server sono attivi dei processi di monitoraggio interni che in caso di errore inviano una notifica agli operatori del Centro di Certificazione.

Tranne che per l'emissione e il cambio di stato del suo certificato, non vengono inviate altre notifiche al Titolare del certificato.

Durante il normale esercizio delle funzioni della CA di Firma, tutti i sistemi software e l'hardware vengono sottoposti manualmente e/o automaticamente a una verifica di eventuali vulnerabilità.

5.5 Archiviazione dei dati

La CA di Firma conserva tutte le informazioni relative ai processi di emissione e gestione dei certificati, tra cui:

- le richieste di emissione;
- la documentazione fornita dai richiedenti;
- le CSR (Certificate Signing Request) fornite dai richiedenti;
- i dati anagrafici dei richiedenti e degli utilizzatori finali (ove siano soggetti diversi);
- i risultati delle verifiche svolte dalla CA di Firma;
- le richieste di revoca o sospensione;
- tutti i certificati emessi;
- gli audit log, per un periodo non inferiore a 20 anni.

Una copia di sicurezza (backup) dei dati, delle applicazioni, del giornale di controllo e di ogni altro file necessario al completo ripristino del servizio viene effettuata giornalmentee replicata in tempo reale sul sito del Disaster Recovery.

L'infrastruttura della PKI Difesa raccoglie e gestisce:

- tutti i log di audit indicati al punto 5.4;
- le Informazioni sulle richieste di certificati;
- la documentazione di supporto;
- le informazioni sul ciclo di vita dei certificati.

Per quanto riguarda gli eventi di log consultare la sezione 5.4.

Tutti i certificati e le corrispondenti richieste, vengono conservati per 20 anni dopo la loro scadenza.

La PKI Difesa protegge l'archivio in modo tale che solo il personale autorizzato e di fiducia siano in grado di accedervi.

L'archivio è protetto contro accessi non autorizzati, modifica, cancellazione o altra manomissione da parte personale non abilitato.

La PKI Difesa esegue la copia degli archivi elettronici e delle informazioni immagazzinate in base alle politicy interne al Comando Comando per le Operazioni in Rete e sono mantenute in un dispositivo di storage esterno.

Copie dei documenti cartacei sono conservati in un apposito armadio.

Le entry del database e i certificati contengono informazioni sulla data e sull'ora ottenuta da una fonte oraria certa.

Solo il personale autorizzato e di fiducia è in grado di ottenere l'accesso all'archivio. L'integrità delle informazioni viene verificata sia in fase di backup sia in fase di ripristino.

5.6 Rinnovo della chiave della CA

Entro i due terzi della durata di vita del certificato della CA di Firma, il Ministero della Difesa rinnova la coppia di chiavi ed il certificato della CA. Da quel momento in poi i nuovi certificati e le nuove CRL vengono firmate con la nuova chiave.

5.7 Compromissione e Disaster Recovery

Per "key compromise" s'intende la violazione di una o più condizioni vincolanti per l'erogazione del servizio di CA; per "disastro" s'intende un evento dannoso le cui conseguenze determinano l'indisponibilità del servizio in condizioni ordinarie.

A seguito di situazioni di compromissione della chiave privata della CA di Firma è prevista un'apposita procedura finalizzata al ripristino (recovery) dei servizi di certificazione. La procedura è indicata all'interno del Piano della Sicurezza del Comando per le Operazioni in Rete.

Il ripristino da compromissione o disastro avviene in ogni caso nelle seguenti situazioni:

- guasti di una o più delle apparecchiature usate per erogare i servizi di certificazione;

- compromissione (es. rivelazione a terzi non autorizzati, perdita) di una o più chiavi private di certificazione.

I backup dei dati immagazzinati nei database primari e di replica vengono eseguiti in momenti differenti della giornata e conservati su device di storage presenti nei rispettivi siti in modo da garantire un maggior livello di affidabilità.

I backup possono essere utilizzati per ripristinare il database in caso di compromissione o di fault.

In caso di fault è possibile anche attivare i servizi sul sito di Disaster Recovery per limitare i disagi.

I backup delle chiavi di CA di Firma sono conservate in un apposito armadio corazzato, la cui apertura è consentita solo al personale autorizzato. Questo armadio è ubicato all'interno di un'area il cui accesso è consentito solo al personale autorizzato.

In caso di danni alle risorse o al software, o ai dati il responsabile del Centro di Certificazione informerà il Community Emergency Response Team (CERT) della Difesa ed il Comandante del Comando per le Operazioni in Rete in qualità di Prestatore di Servizi Fiduciari Qualificati della Difesa per attivare le dovute procedure di gestione degli incidenti e di investigazione.

Se necessario saranno attivate le procedure di compromissione o di Disaster Recovery.

In caso di sospetta compromissione della CA o dell'infrastruttura, il CERT Difesa e il Centro di Certificazione attivano le procedure di compromissione chiave.

Il CERT Difesa, che comprende personale preposto alla sicurezza, e il Centro di Certificazione e altri rappresentanti che sono incaricati della conduzione operativa della PKI Difesa, valutano la situazione, sviluppano un piano d'azione, e attuano il piano d'azione con l'approvazione del Comandante del Comando per le Operazioni in Rete in qualità di Prestatore di Servizi Fiduciari Qualificati.

Qualora sia richiesta la revoca del certificato della CA di Firma:

- viene data comunicazione a tutti i titolari di certificato e alle parti interessate;
- viene data comunicazione a tutti i Dicasteri/Organismi pubblici con cui sono stipulati Accordi di collaborazione;
- viene informata l'autorità di vigilanza Italiana;
- viene generata una nuova chiave privata per la CA di Firma a meno che non si decida per la cessazione del servizio.

In caso di compromissione della chiave privata viene data indicazione che i certificati e le informazioni sullo stato di revoca emesse usando tale chiave privata non possono più essere considerati validi. In caso di compromissione di un algoritmo utilizzato, viene data indicazione sul piano di revoca dei certificati interessati.

Il Centro di Certificazione ha implementato un sito di Disaster Recovery similare alla struttura del sito primario in modo da mitigare i disservizi in caso di danneggiamenti al sito primario.

Ha inoltre implementato, testato e mantiene aggiornato un piano per l'attivazione del sito di Disaster Recovery per mitigare gli effetti di ogni tipo, per calamità naturale o provocata dall'uomo.

5.8 Cessazione della CA o della RA

Il Prestatore di Servizi Fiduciari Qualificati qualora intenda cessare l'attività si impegna, almeno sessanta giorni prima della data di cessazione, a darne avviso all'autorità di vigilanza nazionale (Ag.ID) e ad informare senza indugio i titolari dei certificati da lui emessi mediante comunicazioni

interne all'organizzazione ed invio di mail, specificando che tutti i certificati non scaduti al momento della cessazione saranno revocati.

Il Prestatore di Servizi Fiduciari Qualificati provvederà inoltre a distruggere le chiavi private, incluse le copie di backup, in modo che queste non possano essere recuperate.

Il Prestatore di Servizi Fiduciari Qualificati comunica contestualmente alla cessazione l'eventuale rilevazione di tutte le informazioni necessarie da parte di altro Prestatore di Servizi Fiduciari Qualificati o l'annullamento della stessa (l'indicazione di un Certificatore sostitutivo evita la revoca dei certificati e della relativa documentazione).

Il Prestatore di Servizi Fiduciari Qualificati indica anche il nominativo del depositario del registro dei certificati e della relativa documentazione [DLGS82], oltre alle informazioni di registrazione, le informazioni sullo stato di revoca, gli archivi dei log degli eventi.

Le motivazioni per la cessazione del servizio potrebbero essere di natura volontaria:"Servizio non considerato di pubblica utilità"; "Costi elevati del servizio non convenienti all'A.D."; "Radicale modifica della tecnologia del Mod. Ate"; involontaria:"Compromissione dell'intera Infrastruttura".

6 MISURE DI SICUREZZA TECNICA

6.1 Generazione ed installazione della coppia di chiavi

La coppia di chiavi usata dalla CA di Firma per firmare i certificati e le CRL è generata all'interno di un dispositivo crittografico (HSM) certificato FIPS 140-2 Level 3 o superiore e Common Criteria EAL4+, in un ambiente fisicamente sicuro.

Il CMS durante l'atto dell'emissione del modello ATe genera la coppia di chiavi internamente alla carta anch'essa certificata Common Criteria EAL4+.

Il referente unico del protocollo informatico per l'A.D. genera la coppia di chiavi internamente all'HSM di firma automatica, per i certificati di firma automatica SGD.

Il Titolare con apposita procedura informatica genera la propria coppia di chiavi internamente all'HSM di firma remota, per i certificati di firma remota.

L'operatore del Centro di Certificazione con apposita procedura informatica genera la coppia di chiavi internamente all'HSM di firma automatica/sigillo, per i certificati di firma automatica/sigillo della Difesa SMD/COR.

Il CMS richiedente riceve dalla CA di Firma il certificato emesso, e quindi la chiave pubblica, e inserisce il certificato all'interno del modello ATe del Titolare in modo automatico. Nel momento in cui il Titolare ritira il modello ATe, riceverà quindi la chiave pubblica collegata al certificato.

Il Titolare riceve il certificato di firma remota, e quindi la chiave pubblica, all'interno del sistema stesso di firma remota in modo automatico.

L'operatore del Centro di Certificazione invia il certificato di firma automatica di SGD emesso, e quindi la chiave pubblica, al referente unico del protocollo informatico per l'A.D. tramite email.

L'operatore del Centro di Certificazione invia una mail con allegato una busta cifrata contenente i segreti del certificato di firma automatica e/o Sigillo Digitale della Difesa SMD/COR e la comunicazione dell'erogazione del servzio richiesto direttamente al titolare.

Il Centro di Certificazione rende pubblico il certificato della CA di Firma sul sito https://pki.difesa.it/tsp.

La chiave della CA di Firma ha lunghezza 4096 bit.

Un certificato di firma ha una chiave di lunghezza pari a 2048 bit.

Un certificato OCSP ha una chiave di lunghezza pari a 2048 bit.

6.2 Protezione della chiave privata e dei moduli crittografici

La coppia di chiavi usata dalla CA di Firma per firmare i certificati e le CRL è conservata all'interno di un HSM (Hardware Security Module) di alta qualità, dotato di certificazione di sicurezza FIPS PUB 140-2 a livello 3 e Common Criteria EAL 4+.

La coppia di chiavi del Titolare del certificato di firma è conservata all'interno del modello ATe che è un dispositivo certificato Common Criteria EAL 4+.

La coppia di chiavi del Titolare del certificato di firma remota, automatica e sigillo digitale è conservata all'interno di un HSM di alta qualità, dotato di certificazione di sicurezza secondo la norma FIPS PUB 140-2 a livello 3, Common Criteria EAL 4+ e conforme allo standard Italiano.

La PKI Difesa, per proteggere la chiave privata della CA di Firma, usa Hardware Security Modules (HSM) certificati FIPS 140-2 Level 3 e Common Criteria EAL 4+.

Per l'esecuzione di compiti sensibili, come operazioni crittografiche legate all'attivazione della CA di Firma, la PKI Difesa ha implementato una procedura che richiede la partecipazione di più operatori ognuno dotato di una parte del "segreto" necessario ad eseguire l'operazione.

La chiave privata della CA di Firma non è esportabile fuori dell'HSM.

Allo scopo di garantire la continuità del servizio, la CA di Firma conserva la coppia di chiavi su più dispositivi HSM in alta affidabilità sul sito primario e sul sito secondario.

La CA di Firma inoltre effettua una copia di backup della coppia di chiavi su supporto removibile protetto secondo le procedure certificate dell'HSM stesso.

La copia di backup viene conservata in luogo sicuro e distinto da quello in cui si trova la copia operativa (all'interno dello HSM).

La chiave privata dei certificati di firma viene generata internamente al modello ATe e non è possibile eseguirne il backup o il processo di key recovery.

La chiave privata dei certificati di firma remota e automatica è generata all'interno degli HSM di firma remota.

La coppia di chiavi associata al certificato della CA di Firma viene conservata in modo sicuro esclusivamente utilizzando metodi di backup certificati dal produttore del dispositivo HSM e che hanno gli stessi livelli di sicurezza dell'HSM stesso.

La CA di Firma genera la propria coppia di chiavi internamente al primo HSM che trasferisce in modo sicuro la chiave anche sui dispositivi in alta affidabilità usando il meccanismo certificato dell'HSM stesso.

Sull'HSM di DR la chiave viene trasferita attraverso la procedura certificata di backup e recovery.

La chiave privata della CA di Firma è custodita all'interno del HSM secondo i meccanismi di protezione e cifra certificati dell'HSM.

La chiave privata della CA di Firma viene abilitata al momento dell'attivazione dell'HSM e del servizio CA di Firma.

La chiave privata della CA di Firma viene disattivata al momento della disattivazione dell'HSM e del servizio CA di Firma.

Ove richiesto il Centro di Certificazione distruggere la chiave privata della CA di Firma in modo da garantire che non vi siano residui che potrebbero portare alla ricostruzione della chiave stessa.

Il Centro di Certificazione utilizza la funzione *"zeroization"* degli HSM e altri mezzi adeguati per garantire la completa distruzione delle chiavi private della CA di Firma.

6.3 Altri aspetti della gestione della coppia di chiavi

Il certificato della CA di Firma è archiviato su un apposito database sul quale vengono eseguite opportune policy di backup e conservazione.

Inoltre il certificato della CA di Firma insieme con tutti i certificati emessi sono conservati durante il loro periodo di validità all'interno del Directory Server.

La durata operativa di un certificato finisce al raggiungimento della sua data di scadenza o alla sua revoca.

La durata operativa di una coppia di chiavi è la stessa del corrispondente certificato.

Nel seguito il riepilogo delle durate massime dei singoli certificati:

Entità	Durata certificato	Durata chiave
Certificato di CA di Firma	Fino a 30 anni	Fino a 20 anni
Certificato utente firma su Mod.ATe	Fino a 10 anni	Fino a 10 anni
Certificato utente firma remota/automatica/sigillo	Fino a 10 anni	Fino a 10 anni
Certificato OCSP	Fino a 5 anni	Fino a 5 anni

Ii QTSP non emette certificati la cui data di scadenza sia superiore alla data di scadenza del certificato di CA e provvederà in tempo utile al rinnovo o all'emissione di nuove chiavi di CA e del relativo certificato.

6.4 Dati di attivazione della chiave

L'attivazione dell'HSM della CA di Firma necessita dell'ausilio di un certo numero di chiavi e PIN in possesso del personale addetto alla gestione operativa del servizio, alle dirette dipendenze del Responsabile della Certificazione.

L'utilizzo della chiave da parte del Titolare del certificato di firma necessita dell'inserimento di un PIN per il login al modello ATe e di un PIN per l'utlizzo della firma conosciuti solo ed esclusivamente dal Titolare della smartcard. Prima di poter utilizzare la chiave di firma per la prima volta, il Titolare verifica che la propria firma non sia stata utilizzata in precedenza, attraverso una procedura che prevede l'inserimento del PIN FIRMA e che se completata con esito positivo, sblocca l'utilizzo della chiave.

L'utilizzo della chiave di firma automatica e della firma remota da parte del Titolare necessita della conoscenza di un PIN (PIN smartcard o PIN OTP) e/o di una password, noti soli al Titolare del certificato.

I dati necessari per proteggere i token e consentire l'attivazione della chiave privata sono generati durante la procedura di Key Cerimony secondo le specifiche di sicurezza della certificazione dell'HSM. Tutte le informazioni sulla distribuzione delle chiavi sono registrate.

I dati necessari all'attivazione dei token e della chiave sono conservati in apposito armadio corazzato.

6.5 Controlli di sicurezza sugli elaboratori

I sistemi operativi usati dalla CA di Firma per la gestione dei certificati sono dotati di controlli e di livello di sicurezza adeguati e sono sottoposti ad un hardening continuo.

I sistemi operativi sono configurati in modo tale da richiedere sempre l'identificazione dell'utente mediante username e password oppure, nel caso dei sistemi più critici, mediante smartcard/token e relativo PIN.

Gli eventi di accesso ai sistemi sono registrati, come descritto nella sezione 5.4.

La PKI Difesa assicura che i sistemi di gestione del software e dei file della CA di Firma sono affidabili e protetti da accessi non autorizzati. Inoltre, la PKI Difesa limita l'accesso ai server alle sole persone autorizzate.

Gli utenti generici non dispongono di account sui server.

La rete della PKI Difesa è logicamente separata dalle altre reti. Questa separazione consente l'accesso solo attraverso i processi definiti dalle applicazioni interne alla struttura. La PKI Difesa utilizza un sistema di firewall per proteggere la rete da intrusioni interne ed esterne e limita la natura delle fonti che possono accedere ai sistemi di produzione.

I server della PKI Difesa richiedono l'uso di password che hanno una lunghezza minima di caratteri e una combinazione di caratteri alfanumerici e speciali.

L'accesso diretto alle banche dati a supporto delle operazioni della PKI è limitato alle solo persone di fiducia.

6.6 Controlli tecnici sul ciclo di vita

All'interno dell'infrastruttura PKI Difesa, le attività di sviluppo includono la sicurezza dell'ambiente di sviluppo, del personale di sviluppo, del sistema di gestione della configurazione durante la manutenzione del prodotto, pratiche di ingegneria del software, metodologie per lo sviluppo del software e dei locali utilizzati.

La PKI Difesa è dotata di strumenti per la gestione della sicurezza e di procedure che assicurano che i sistemi operativi e le reti aderiscano agli stardard ed alle policy di di sicurezza della configurazione.

Questi tool includono controlli sull'integrità del software, dell'hardware e dei flussi applicativi in modo da garantire il corretto funzionamento dell'infrastruttura.

6.7 Controlli di sicurezza sulla rete

L'infrastruttura della PKI Difesa è suddivisa in differenti livelli di sicurezza separati tra loro e dalla rete Difesa da un sistema di firewall di alta qualità che garantiscono un adeguato filtraggio delle connessioni.

I server CA di Firma sono collocati nei segmenti di rete più interni dell'infrastruttura a garanzia di un maggior livello di sicurezza.

Sui server tutte le porte di comunicazione non necessarie sono disattivate. Sono attivi esclusivamente quei servizi che supportano i protocolli e le funzioni necessarie per il funzionamento dell'applicazione.

6.8 Riferimento temporale

Tutti i sistemi di elaborazione usati dalla CA di Firma sono allineati con un time-server sincronizzato col segnale orario fornito dalla rete satellitare GPS.

7 PROFILO DEI CERTIFICATI, DELLE CRL E DEL OCSP

7.1 Profilo dei certificati

I certificati sono conformi allo standard internazionale ISO/IEC 9594-8:2005 [X.509] e alla specifica pubblica [RFC 5280].

La base dei profili dei certificati emessi è la policy ETSI chiamata **QCP-n-qscd** *"policy per i certificati qualificati UE emessi a persone naturali con la chiave privata e il relativo certificato installato a bordo di un dispositivo per la creazione di firme/sigilli elettronici qualificati"* e identificata dal seguente OID: `Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2).`

Per le persone legali, la policy ETSI chiamata **QCP-l-qscd** "" è identificata dal seguente OID: `itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3)`

PROFILO DEL CERTIFICATO DELLA CA DI FIRMA

Si riporta di seguito il profilo definito per i certificati della CA di Firma.

CAMPO	VALORE
Version	3
Serial Number	Variabile come da RFC 5280
Signature	Firma RSA apposta dalla CA come da RFC 5280
Issuer	Identico al Subject
Validity	Variabile, come indicato nella sezione 6.3
Subject	Come indicato nella sezione 3.1
Subject Public Key Info	Chiave pubblica RSA (modulo ed esponente pubblico) come da RFC 5280
ESTENSIONE	**VALORE**
Basic Constraints [Critical]	Subject Type=CA Path Length Constraint=0
Subject Key Identifier (SKI)	Variabile e calcolato come da RFC 5280
Key Usage [Critical]	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Certificate Policies	• Certificate Policy: Policy Identifier=1.3.6.1.4.1.14031.2.1.1 - Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.pki.difesa.it/ManualeOperativoDifesa.pdf
Authority Information Access (AIA)	• Authority Info Access - Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsppkiff.difesa.it/
CRL Distribution Points (CDP)	• CRL Distribution Point URL=http://www.pki.difesa.it/cafirmadigitale.crl • CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa - CA di

CAMPO	VALORE
	Firma Digitale,OU=S.M.D. - C.do C4 Difesa,O=Ministero della Difesa,C=IT

PROFILO DEL CERTIFICATO DI FIRMA

Si riporta di seguito il profilo di default definito per i certificati di firma di titolari del modello ATe.

L'utente può richiedere in fase di acquisizione dati che venga inserito il profilo di firma senza limitazioni d'uso di OID 1.3.6.1.4.1.14031.2.1.1.12

CAMPO	VALORE
Version	3
Serial Number	Variabile come da RFC 5280
Signature	Firma RSA apposta dalla CA come da RFC 5280
Issuer	Corrispondente al Subject della CA, come indicato nella sezione 3.1
Validity	Variabile, come indicato nella sezione 6.3
Subject	Come indicato nella sezione 3.1
Subject Public Key Info	Chiave pubblica RSA (modulo ed esponente pubblico) come da RFC 5280
ESTENSIONE	**VALORE**
Basic Constraints [Critical]	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier (AKI)	Corrispondente al SKI della CA
Subject Key Identifier (SKI)	Variabile e calcolato come da RFC 5280
Key Usage	Non Repudiation (40)
Certificate Policies	• Certificate Policy: - Policy Identifier=1.3.6.1.4.1.14031.2.1.1.13 User Notice: Il Titolare fa uso del certificato solo per le finalita' di lavoro per le quali esso e' rilasciato. The certificate holder must use the certificate only for the purposes for which it is issued. Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://pki.difesa.it/tsp • Certificate Policy: - Policy Identifier=1.3.76.16.6
Subject Alternative Name (SAN)	RFC822 Name corrispondente all'email istituzionale
Authority Information Access (AIA)	• Authority Info Access - Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.pki.difesa.it/cafirmadigitale.crt - Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsppkiff.difesa.it/
CRL DistributionPoints (CDP)	• CRL Distribution Point URL=http://www.pki.difesa.it/cafirmadigitale.crl • CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa - CA di

	Firma Digitale,OU=S.M.D. - C.do C4 Difesa,O=Ministero della Difesa,C=IT
Qualified Certificate Statements	• NESSUNA informazione sul limite di negoziazioni (QcLimitValue) • Periodo di Conservazione (QcRetentionPeriod) di anni 20 • Chiave protetta da un dispositivo sicuro di creazione della firma (QcSSCD) • Certificato Qualificato (QcCompliance) • Certificato per la Firma Elettronica come da Regolamento eIDAS (Regolamento UE N. 910/2014) (QcType=id-etsi-qct-esign) • Indirizzi di pubblicazione dei PKI Disclosure Statements (QcEuPDS): - https://pki.difesa.it/tsp/ (lingua EN) - https://pki.difesa.it/tsp/ (lingua IT)

PROFILO DEL CERTIFICATO DI FIRMA REMOTA

Si riporta di seguito il profilo definito per i certificati di firma di titolari di firma remota.

CAMPO	VALORE
Version	3
Serial Number	Variabile come da RFC 5280
Signature	Firma RSA apposta dalla CA come da RFC 5280
Issuer	Corrispondente al Subject della CA, come indicato nella sezione 3.1
Validity	Variabile, come indicato nella sezione 6.3
Subject	Come indicato nella sezione 3.1
Subject Public Key Info	Chiave pubblica RSA (modulo ed esponente pubblico) come da RFC 5280
ESTENSIONE	**VALORE**
Basic Constraints [Critical]	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier (AKI)	Corrispondente al SKI della CA
Subject Key Identifier (SKI)	Variabile e calcolato come da RFC 5280
Key Usage	Non Repudiation (40)
Certificate Policies	• Certificate Policy: - Policy Identifier=1.3.6.1.4.1.14031.2.1.1.15 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://pki.difesa.it/tsp • Certificate Policy: - Policy Identifier=1.3.76.16.3 User Notice: Il Certificatore garantisce che le firme basate su questo certificato qualificato sono valide in quanto il certificato ad esse associato era valido al momento della generazione delle firme User Notice: The qualified certification service provider that issued this certificate ensures that the signatures based on this certificate have been generated during the period of validity of the certificate • Certificate Policy: - Policy Identifier=1.3.76.16.6
Subject Alternative Name (SAN)	RFC822 Name corrispondente all'email istituzionale

Authority Information Access (AIA)	• Authority Info Access - Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.pki.difesa.it/cafirmadigitale.crt - Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsppkiff.difesa.it/
CRL DistributionPoints (CDP)	• CRL Distribution Point URL=http://www.pki.difesa.it/cafirmadigitale.crl • CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa - CA di Firma Digitale, OU=S.M.D. - C.do C4 Difesa,O=Ministero della Difesa,C=IT
Qualified Certificate Statements	• NESSUNA informazione sul limite di negoziazioni (QcLimitValue) • Periodo di Conservazione (QcRetentionPeriod) di anni 20 • Chiave protetta da un dispositivo sicuro di creazione della firma (QcSSCD) • Certificato Qualificato (QcCompliance) • Certificato per la Firma Elettronica come da Regolamento eIDAS (Regolamento UE N. 910/2014) (QcType=id-etsi-qct-esign) • Indirizzi di pubblicazione dei PKI Disclosure Statements (QcEuPDS): - https://pki.difesa.it/tsp/ (lingua EN) - https://pki.difesa.it/tsp/ (lingua IT)

PROFILO DEL CERTIFICATO DI FIRMA AUTOMATICA SGD

Si riporta di seguito il profilo definito per i certificati di firma di titolari di firma automatica.

CAMPO	VALORE
Version	3
Serial Number	Variabile come da RFC 5280
Signature	Firma RSA apposta dalla CA come da RFC 5280
Issuer	Corrispondente al Subject della CA, come indicato nella sezione 3.1
Validity	Variabile, come indicato nella sezione 6.3
Subject	Come indicato nella sezione 3.1
Subject Public Key Info	Chiave pubblica RSA (modulo ed esponente pubblico) come da RFC 5280
ESTENSIONE	**VALORE**
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier (AKI)	Corrispondente al SKI della CA
Subject Key Identifier (SKI)	Variabile e calcolato come da RFC 5280
Key Usage [Critical]	Non Repudiation (40)
Certificate Policies	• Certificate Policy: - Policy Identifier=1.3.6.1.4.1.14031.2.1.1.18 User Notice: Il presente certificato è valido solo per firme apposte con procedura automatica./This certificate may only be used for unattended/automated digital signatures. Policy Qualifier Info:

	Policy Qualifier Id=CPS Qualifier: https://pki.difesa.it/tsp • Certificate Policy: - Policy Identifier=1.3.76.16.6
Subject Alternative Name (SAN)	RFC822 Name corrispondente all'email istituzionale
Authority Information Access (AIA)	• Authority Info Access - Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.pki.difesa.it/cafirmadigitale.crt - Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsppkiff.difesa.it/
CRL DistributionPoints (CDP)	• CRL Distribution Point URL=http://www.pki.difesa.it/cafirmadigitale.crl • CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa - CA di Firma Digitale, OU=S.M.D. - C.do C4 Difesa,O=Ministero della Difesa,C=IT
Qualified Certificate Statements	• NESSUNA informazione sul limite di negoziazioni (QcLimitValue) • Periodo di Conservazione (QcRetentionPeriod) di anni 20 • Chiave protetta da un dispositivo sicuro di creazione della firma (QcSSCD) • Certificato Qualificato (QcCompliance) • Certificato per la Firma Elettronica come da Regolamento eIDAS (Regolamento UE N. 910/2014) (QcType=id-etsi-qct-esign) • Indirizzi di pubblicazione dei PKI Disclosure Statements (QcEuPDS): - https://pki.difesa.it/tsp/ (lingua EN) - https://pki.difesa.it/tsp/ (lingua IT)

PROFILO DEL CERTIFICATO DI FIRMA AUTOMATICA SMD COR

Si riporta di seguito il profilo definito per i certificati di firma di titolari di firma automatica.

CAMPO	VALORE
Version	3
Serial Number	Variabile come da RFC 5280
Signature	Firma RSA apposta dalla CA come da RFC 5280
Issuer	Corrispondente al Subject della CA, come indicato nella sezione 3.1.1
Validity	Variabile, come indicato nella sezione 6.3.2
Subject	Come indicato nella sezione 3.1
Subject Public Key Info	Chiave pubblica RSA (modulo ed esponente pubblico) come da RFC 5280
ESTENSIONE	**VALORE**
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier (AKI)	Corrispondente al SKI della CA
Subject Key Identifier (SKI)	Variabile e calcolato come da RFC 5280
Key Usage [Critical]	Non Repudiation (40)

Certificate Policies	• Certificate Policy: - Policy Identifier=1.3.6.1.4.1.14031.2.1.1.19 User Notice: Il presente certificato è valido solo per firme apposte con procedura automatica./This certificate may only be used for unattended/automated digital signatures. Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://pki.difesa.it/tsp • Certificate Policy: - Policy Identifier=1.3.76.16.3 User Notice: Il Certificatore garantisce che le firme basate su questo certificato qualificato sono valide in quanto il certificato ad esse associato era valido al momento della generazione delle firme User Notice: The qualified certification service provider that issued this certificate ensures that the signatures based on this certificate have been generated during the period of validity of the certificate • Certificate Policy: - Policy Identifier=1.3.76.16.6
Subject Alternative Name (SAN)	RFC822 Name corrispondente all'email istituzionale
Authority Information Access (AIA)	• Authority Info Access - Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.pki.difesa.it/cafirmadigitale.crt - Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsppkiff.difesa.it/
CRL DistributionPoints (CDP)	• CRL Distribution Point URL=http://www.pki.difesa.it/cafirmadigitale.crl • CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa - CA di Firma Digitale,OU=S.M.D. - C.do C4 Difesa,O=Ministero della Difesa,C=IT
Qualified Certificate Statements	• NESSUNA informazione sul limite di negoziazioni (QcLimitValue) • Periodo di Conservazione (QcRetentionPeriod) di anni 20 • Chiave protetta da un dispositivo sicuro di creazione della firma (QcSSCD) • Certificato Qualificato (QcCompliance) • Certificato per la Firma Elettronica come da Regolamento eIDAS (Regolamento UE N. 910/2014) (QcType=id-etsi-qct-esign) • Indirizzi di pubblicazione dei PKI Disclosure Statements (QcEuPDS): - https://pki.difesa.it/tsp/ (lingua EN) - https://pki.difesa.it/tsp/ (lingua IT)

PROFILO DEL CERTIFICATO DI SIGILLO DIGITALE EIDAS

Si riporta di seguito il profilo definito per i certificati di firma di titolari di firma automatica.

CAMPO	VALORE

Version	3
Serial Number	Variabile come da RFC 5280
Signature	Firma RSA apposta dalla CA come da RFC 5280
Issuer	Corrispondente al Subject della CA, come indicato nella sezione 3.1
Validity	Variabile, come indicato nella sezione 6.3
Subject	Come indicato nella sezione 3.1
Subject Public Key Info	Chiave pubblica RSA (modulo ed esponente pubblico) come da RFC 5280
ESTENSIONE	**VALORE**
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier (AKI)	Corrispondente al SKI della CA
Subject Key Identifier (SKI)	Variabile e calcolato come da RFC 5280
Key Usage [Critical]	Non Repudiation (40)
Certificate Policies	• Certificate Policy: - Policy Identifier=1.3.6.1.4.1.14031.2.1.1.23 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://pki.difesa.it/tsp • Certificate Policy: - Policy Identifier=1.3.76.16.6
Subject Alternative Name (SAN)	RFC822 Name corrispondente all'email istituzionale
Authority Information Access (AIA)	• Authority Info Access - Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.pki.difesa.it/cafirmadigitale.crt - Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsppkiff.difesa.it/
CRL DistributionPoints (CDP)	• CRL Distribution Point URL=http://www.pki.difesa.it/cafirmadigitale.crl • CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa - CA di Firma Digitale, OU=S.M.D. - C.do C4 Difesa,O=Ministero della Difesa,C=IT
Qualified Certificate Statements	• NESSUNA informazione sul limite di negoziazioni (QcLimitValue) • Periodo di Conservazione (QcRetentionPeriod) di anni 20 • Chiave protetta da un dispositivo sicuro di creazione della firma (QcSSCD) • Certificato Qualificato (QcCompliance) • Certificato per la Firma Elettronica come da Regolamento eIDAS (Regolamento UE N. 910/2014) (QcType=id-etsi-qct-esign) • Indirizzi di pubblicazione dei PKI Disclosure Statements (QcEuPDS): - https://pki.difesa.it/tsp/ (lingua EN) - https://pki.difesa.it/tsp/ (lingua IT)

PROFILO DEL CERTIFICATO DI SIGILLO DIGITALE AUTOREMOTE EIDAS

Si riporta di seguito il profilo definito per i certificati di firma di titolari di firma automatica.

CAMPO	VALORE
Version	3
Serial Number	Variabile come da RFC 5280
Signature	Firma RSA apposta dalla CA come da RFC 5280
Issuer	Corrispondente al Subject della CA, come indicato nella sezione 3.1
Validity	Variabile, come indicato nella sezione 6.3
Subject	Come indicato nella sezione 3.1
Subject Public Key Info	Chiave pubblica RSA (modulo ed esponente pubblico) come da RFC 5280
ESTENSIONE	**VALORE**
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier (AKI)	Corrispondente al SKI della CA
Subject Key Identifier (SKI)	Variabile e calcolato come da RFC 5280
Key Usage [Critical]	Non Repudiation (40)
Certificate Policies	• Certificate Policy: - Policy Identifier=1.3.6.1.4.1.14031.2.1.1.28 User Notice: Il presente certificato è valido solo per firme apposte con procedura automatica./This certificate may only be used for unattended/automated digital signatures. Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://pki.difesa.it/tsp • Certificate Policy: - Policy Identifier=1.3.76.16.6
Subject Alternative Name (SAN)	RFC822 Name corrispondente all'email istituzionale
Authority Information Access (AIA)	• Authority Info Access - Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.pki.difesa.it/cafirmadigitale.crt - Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsppkiff.difesa.it/
CRL DistributionPoints (CDP)	• CRL Distribution Point URL=http://www.pki.difesa.it/cafirmadigitale.crl • CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa - CA di Firma Digitale, OU=S.M.D. - C.do C4 Difesa,O=Ministero della Difesa,C=IT

Qualified Certificate Statements	• NESSUNA informazione sul limite di negoziazioni (QcLimitValue) • Periodo di Conservazione (QcRetentionPeriod) di anni 20 • Chiave protetta da un dispositivo sicuro di creazione della firma (QcSSCD) • Certificato Qualificato (QcCompliance) • Certificato per la Firma Elettronica come da Regolamento eIDAS (Regolamento UE N. 910/2014) (QcType=id-etsi-qct-esign) • Indirizzi di pubblicazione dei PKI Disclosure Statements (QcEuPDS): - https://pki.difesa.it/tsp/ (lingua EN) - https://pki.difesa.it/tsp/ (lingua IT)

I certificati sono firmati con il seguente algoritmo:

sha256withRSAEncryption - OBJECT IDENTIFIER ::= {iso(**1**) member-body(**2**) us(**840**) rsadsi(**113549**) pkcs(**1**) pkcs-1(**1**) **11**}

Ogni tipologia di certificato ha un suo OID definito internamente alla PKI Difesa per differenziarne l'utilizzo. Tale OID è riportato nell'estensione X.509v3 Certificate Policies. I vari valori sono indicati nella sezione 2.1.

All'interno dei certificati viene riportato nell'estensione Certificate Policies:

- l'identificativo OID della policy di riferimento;
- l'URL per consultare il documento CPS/Manuale Operativo;
- in alcuni casi un testo User Notice che specifica ulteriori dettagli (ad esempio per i certificati di test).

7.2 Profilo della CRL

Le CRL sono conformi allo standard internazionale ISO/IEC 9594-8:2005 [X.509 versione 2] e alla specifica pubblica RFC 5280.

In corrispondenza di ogni voce della CRL è presente l'estensione reasonCode a indicare la motivazione della sospensione o revoca.

CRL	
Version	2
Issuer DN	Corrispondente al Subject della CA, come indicato nella sezione 3.1
Effective Date	Data di emissione
Next Update	Data entro la quale verrà emessa una nuova CRL
Revoked Certificates	Elenco dei certificati revocati. Per ogni voce viene indicato: • Il numero di serie del certificato revocato, • La data e ora di revoca • L'eventuale codice della motivazione
CRL Extensions	Estensioni come da tabella seguente
CRL Signature Algorithm	Algoritmo sha256WithRSAEncryption (1.2.840.113549.1.1.11)
CRL Signature	Firma RSA apposta dalla CA di Firma come da RFC 5280
ESTENSIONE	**Valore**
Authority Key Identifier	Valore corrispondente al SKI dalla CA
CRL Number	Numero progressivo della CRL emessa

CRL	
Estensione id-ce-expiredCertsOnCRL (2.5.29.60)	Indica la data a partire dalla quale la CRL contiene anche i certificati revocati scaduti

7.3 Profilo dei Certificati OCSP

L'OCSP è conforme alla specifica pubblica RFC 2560.

Di seguito sono riportate le caratteristiche del profilodi tale certificato.

CAMPO	VALORE
Version	3
Serial Number	Variabile come da RFC 5280
Signature	Firma RSA apposta dalla CA come da RFC 5280
Issuer	Corrispondente al Subject della CA, come indicato nella sezione 3.1
Validity	Variabile, come indicato nella sezione 6.3
Subject	Come indicato nella sezione 3.1
Subject Public Key Info	Chiave pubblica RSA (modulo ed esponente pubblico) come da RFC 5280
ESTENSIONE	**VALORE**
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier (AKI)	Corrispondente al SKI della CA
Subject Key Identifier (SKI)	Variabile e calcolato come da RFC 5280
Key Usage	Digital Signature (80)
Enhanced Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)
Certificate Policies	• Certificate Policy: Policy Identifier=1.3.6.1.4.1.14031.2.1.1.1 - Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://pki.difesa.it/tsp
CRL DistributionPoints (CDP)	• CRL Distribution Point URL=http://www.pki.difesa.it/cafirmadigitaleeidas.crl • CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa - CA di Firma Digitale eIDAS, OU=S.M.D. - C.do C4 Difesa, O=Ministero della Difesa, C=IT

8 VERIFICHE DI CONFORMITÀ

Il Ministero della Difesa per ottenere (e mantenere) la qualifica di Prestatore di Servizi Fiduciari Qualificati secondo il Regolamento UE N. 910/2014 del Parlamento Europeo e del Consiglio, chiederà ogni 24 mesi una relazione di valutazione della conformità ai requisiti del Regolamento da parte di un Organismo di Certificazione (CAB - Conformity Assessment Body) accreditato secondo il Regolamento (CE) 765/2008.

Il Ministero della Difesa inoltre è tenuto a svolgere periodiche ispezioni interne.

8.1 Frequenza e circostanze dalle verifiche

Le ispezioni esterne, da parte del CAB, sono svolte con periodicità biennale (24 mesi).

Le ispezioni interne sono svolte nel rispetto di un piano che prevede frequenze diverse (da mensile ad annuale) per i diversi aspetti tecnico-operativi del servizio di CA di Firma.

8.2 Identità e qualificazione degli ispettori

Le verifiche esterne sono condotte da terze parti indipendenti e che offrono adeguate garanzie dal punto di vista organizzativo e tecnologico e in possesso delle adeguate competenze in materia.

Le verifiche interne sono svolte da personale della struttura delegata al governo dei servizi di CA in possesso delle adeguate qualifiche in materia.

8.3 Relazioni tra la CA e gli ispettori

Non esiste alcuna relazione tra l'organismo che esegue l'audit esterno e il Centro di Certificazione che possa in alcun modo influenzare l'esito delle ispezioni a favore del Ministero della Difesa.

Il responsabile Audit del Ministero della Difesa è un dipendente della Difesa che opera internamente al Centro di Certificazione ed è pertanto dipendente dalla struttura organizzativa preposta all'erogazione del servizio di CA di Firma.

8.4 Argomenti coperti dalle verifiche

Gli audit svolti dagli enti esterni sono finalizzati a verificare la conformità dei servizi di CA con gli standard internazionali di riferimento in materia dal punto di vista tecnico ed organizzativo.

L'ispezione del CAB segue delle Linee Guida basate sulla norma europea ETSI EN 319 401 – "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

L'ispezione interna è principalmente rivolta a verificare l'integrità del "giornale di controllo" (audit log), ed il rispetto delle procedure operative della CA di Firma.

8.5 Azioni conseguenti alle non-conformità

Nel caso di non-conformità, Ag.ID richiede alla CA di Firma di adottare le necessarie misure correttive entro un certo arco di tempo, pena la sospensione o revoca dell'accreditamento.

8.6 Comunicazione dei risultati delle verifiche

Il risultato dell'ispezione è una relazione che viene utilizzato per chiedere o mantenere la qualificazione all'Organismo di vigilanza competente in ambito nazionale (per l'Italia Ag.ID), allegando la relazione di cui sopra.

Il risultato dell'ispezione interna viene comunicato al Centro di Certificazione redigendo un'apposito verbale.

9 ALTRI ASPETTI COMMERCIALI E LEGALI

9.1 Tariffe del servizio

A fronte di un investimento complessivo centralizzato per realizzare l'infratruttura PKI Difesa, il servizio è offerto a titolo gratuito per le attività istituzionali ai dipendenti del Ministero della Difesa. Inoltre, in fase di stipula degli Accordi di collaborazione è stata chiesta ai Dicasteri/Organismi pubblici una compartecipazione, proporzionale al numero di modelli ATe emessi, ai costi che la Difesa comunque sostiene per le esigenze di funzionamento del Card Management System (CMS) e della Public Infrastructure Key (PKI), pertanto il servizio a titolo gratuito è offerto anche ai dipendenti delle altre P.A. che hanno stipulato un accordo di collaborazione il Ministero della Difesa, limitatamente alle attività istituzionali.

Il Ministero della Difesa è un ente governativo che fornisce il servizio di rilascio, gestione ed eventuale rinnovo dei certificati a titolo gratuito ai propri dipendenti e ai dipendenti delle altre P.A. che hanno stipulato un accordo di collaborazione con il Ministero della Difesa.

Per questo motivo non sono previsti costi per le seguenti voci:

- Accesso ai certificati
- Accesso alle informazioni di revoca o di stato del certificato
- Altri servizi della PKI

Quindi, non sono previste politiche di rimborso.

9.2 Responsabilità finanziaria

Trattandosi di Pubblica Amministrazione, non è prevista alcuna copertura assicurativa.

9.3 Tutela della riservatezza dei dati aziendali

Il Ministero della Difesa è titolare dei dati personali raccolti in fase di identificazione e registrazione dei soggetti che richiedono i certificati e si obbliga quindi a trattare tali dati con la massima riservatezza e nel rispetto di quanto previsto dal Reg. (UE) 2016/679 (GDPR), anche detto "Codice in materia di protezione dei dati personali".

Nel caso in cui l'attività di identificazione e registrazione degli utenti avvenga presso una struttura delegata (LRA), quest'ultima è qualificata come "incaricato del trattamento".

Sono considerate confidenziali per l'organizzazione le seguente informazioni:

- il piano di attivazione del sito di Disaster Recovery;
- il piano di indirizzamento dell'infrastruttura e la struttura di rete;
- le procedure di attivazione delle chiavi e i segreti (password, PIN, ecc…);
- i log di Audit e delle transazioni.

Non sono considerate riservate le informazioni contenute all'interno del certificato, né gli indirizzamenti ai servizi di verifica dello stato del certificato o per lo scarico della CRL.

Tutte le informazioni non indicate in questa sezione sono considerate non confidenziali.

Questa sezione è soggetta alla disposizioni di legge in materia.

La PKI Difesa garantisce la riservatezza delle informazioni considerate confidenziali.

9.4 Privacy dei dati personali

Il Ministero della Difesa è titolare del trattamento dei dati forniti dal richiedente la carta, informandolo del trattamento degli stessi, ai sensi e per gli effetti di cui al Reg. (UE) 2016/679 (GDPR), Tali dati personali saranno trattati da personale autorizzato, mediante archivi cartacei e strumenti informatici idonei a garantirne la sicurezza e la riservatezza nel rispetto delle modalità indicate nel succitato Decreto.

I dati forniti dal richiedente si distinguono in obbligatori e facoltativi. I dati obbligatori sono necessari allo svolgimento del servizio; il loro mancato conferimento da parte del richiedente comporta l'impossibilità di concludere il contratto. Si noti che la pubblicazione del certificato comporta la diffusione a terzi, delle informazioni contenute nel certificato stesso. I dati facoltativi agevolano semplicemente il servizio; il loro mancato conferimento non ostacola la conclusione del processo di acquisizione.

I dati forniti dal richiedente sono trattati esclusivamente per le finalità di rilascio o rinnovo dei certificati.

La PKI Difesa è conforme al Reg. (UE) 2016/679 (GDPR), in materia di gestione della privacy e protezione dei dati personali.

Qualunque informazione sul sottoscrittore non disponibile sul directory server pubblico è trattata come privata.

In base alla legge locale tutte le informazioni rese pubbliche nel certificato non sono considerate private.

I partecipanti alla PKI Difesa che vengono a conoscenza di informazioni private debbono proteggerle da compromissione e divulgazione verso soggetti terzi e sono tenuti al rispetto di tutte le leggi locali in materia di riservatezza della privacy.

Tranne dove diversamente indicato all'interno di questo CP, o della legge sulla privacy o in accordi intercorsi tra le parti, le informazioni private non debbono essere usate senza il consenso scritto dell'interessato.

La PKI Difesa ha il diritto di rivelare informazioni riservate/confidenziali se, in buona fede, ritiene che la divulgazione sia necessaria in risposta a procedimenti giudiziari, amministrativi o altro durante un processo di rilevanza civile o amministrativa, quali citazioni, interrogatori, richieste di ammissione e richieste di produzione di documenti.

In particolare:

- La PKI Difesa produce i dati, informazioni, documenti all'Autorità giudiziaria richiedente, ad esclusione di quelli coperti dal Segreto di Stato.
- La PKI Difesa istruisce le varie richieste di accesso (in osservanza della procedura interna dello SMD) in relazione alla tipologia (*generalizzato* ai sensi del D.Lgs. n.33/13 e *documentale* ai sensi dell'Art.22 della L. n. 241/90), valutando le limitazioni assolute e qualificate nel primo caso (Art. 5-bis del citato D.Lgs. n.33/2013) e quelle di esclusione da documenti concernenti la sicurezza e la difesa nazionale, le relazioni internazionali, l'ordine pubblico, la prevenzione e repressione della criminalità, la salvaguardia della riservatezza dei terzi, persone, gruppi e imprese (di cui al D.P.R. n.352/92, Art.8 e correlati Artt. 1048, 1049 e 1050 del D.P.R. n.90/10 - TUOM).

9.5 Diritti di proprietà intellettuale

Il proprietario del presente documento è il Ministero della Difesa/Stato Maggiore della Difesa - Comando per le Operazioni in Rete, che si riserva tutti i diritti ad esso relativi.

Per la sua redazione ed aggiornamento si avvale del dipendente Centro di Certificazione e PKI Difesa.

Relativamente alla proprietà di altri dati ed informazioni si applicano le leggi in materia in vigore.

9.6 Obblighi e garanzie

9.6.1 Obblighi della CA e garanzie

La CA di Firma si impegna a:

- operare in conformità a questo CP e al CPS;
- identificare i richiedenti come descritto in questo CP e al CPS;
- emettere e gestire i certificati come descritto nel presente CP e al CPS;
- fornire un efficiente servizio di sospensione o revoca dei certificati;
- garantire che il Titolare possedeva, al momento dell'emissione del certificato, la corrispondente chiave privata;
- segnalare tempestivamente l'eventuale compromissione della propria chiave privata;
- fornire informazioni chiare e complete sulle procedure e requisiti del servizio;
- rendere disponibile una copia di questo CP a chiunque ne faccia richiesta;
- garantire un trattamento dei dati personali conforme alle norme vigenti;
- fornire un servizio informativo efficiente ed affidabile sullo stato dei certificati.

9.6.2 Obblighi e garanzie della RA

La RA e le LRA si impegnano ad:

- operare in conformità a questo CP e al CPS;
- identificare i richiedenti come descritto in questo CP e al CPS;
- segnalare tempestivamente l'eventuale compromissione della propria chiave privata;
- fornire informazioni chiare e complete sulle procedure e requisiti del servizio;
- garantire un trattamento dei dati personali conforme alle norme vigenti.

Nel caso in cui una LRA sia un soggetto esterno al Ministero della Difesa, gli obblighi della LRA sono definiti nell'apposito accordo di collaborazione e si basano sugli obblighi qui esposti come misura minima.

9.6.3 Obblighi del Titolare

Il soggetto richiedente o Titolare (Subscriber) ha l'obbligo di:

- leggere, comprendere ed accettare integralmente questo CP e al CPS;
- richiedere il certificato con le modalità previste da questo CP e al CPS;
- fornire alla CA di Firma, RA e LRA le informazioni esatte e veritiere in fase di registrazione;

- adottare misure tecniche ed organizzative idonee atte ad evitare la compromissione della propria chiave privata;
- richiedere immediatamente la sospensione del certificato nel caso di sospetta o accertata compromissione della propria chiave privata e poi procedere alla richiesta di revoca nel caso il sospetto fosse fondato;
- richiedere immediatamente la revoca del certificato nel caso in cui una o più delle informazioni contenute nel certificato (es. cognome, nome, codice fiscale, etc.) siano errate o perdano di validità;
- successivamente all'emissione e fino alla scadenza o revoca del certificato, avvisare prontamente la CA di Firma di ogni variazione alle informazioni fornite in fase di richiesta;
- al momento dell'eventuale revoca del certificato, restituire o cessare immediatamente l'uso del certificato.

9.6.4 Dichiarazioni e garanzie delle parti interessate

Le Parti interessate sono reciprocamente informate e, per quanto di competenza, espressamente confermano di avere informazioni sufficienti per prendere una decisione per quanto riguarda la misura in cui scelgono di affidarsi alle informazioni contenute in un certificato, e sono le sole responsabili per decidere se fare o meno affidamento su tali informazioni, addossandosi le conseguenze giuridiche della loro incapacità di eseguire gli obblighi di una parte interessata nei termini di questo documento.

9.6.5 Dichiarazioni e garanzie degli altri partecipanti

Tutti i fornitori di servizi che hanno impatto sull'erogazione dei servizi della PKI sono controllati dal Ministero della Difesa. I corrispondenti contratti sono depositati presso il Ministero della Difesa e riportano gli SLA di intervento (ad esempio per servizi connettività, fornitura elettrica, assistenza sistemistica, sistema condizionamento).

9.7 Esclusione di garanzie

La CA di Firma non ha ulteriori obblighi e non garantisce nulla più di quanto espressamente indicato in questo CP o previsto dalle norme vigenti.

9.8 Limitazioni di responsabilità

La CA di Firma declina ogni responsabilità per gli eventuali danni sofferti dal personale a causa della mancata ricezione delle comunicazioni della CA di Firma in conseguenza di un errato indirizzo di e-mail fornito in fase di richiesta.

9.9 Risarcimenti

L'Amministrazione della Difesa, a fronte di:

- false dichiarazioni nella richiesta di certificazione;
- omessa informazione su atti o fatti essenziali per negligenza o con l'obiettivo di raggirare il Ministero della Difesa;
- utilizzo di nomi in violazione dei diritti di proprietà individuale;
- utilizzo del Mod.ATe e relativi certificati per attività non previste dalla normativa in vigore;

dei titolari dei dati, avvia tutte le procedure previste per legge, per l'accertamento di eventuali responsabilità di natura penale (ai sensi dell'Art.76 del D.P.R. n.445/2000), civile (quando ne ricorrano i presupposti) e amministrativa (per eventuale danno erariale).

Il Ministero della Difesa non prevede alcun risarcimento in caso di disservizio.

9.10 Durata e cessazione

Questo CP entra in vigore al momento della sua pubblicazione (vedere il capitolo 2) e resta in vigore fino al momento della sua eventuale sostituzione con una nuova versione.

Questo CP resta in vigore fino alla pubblicazione di una nuova versione.

Alla risoluzione del presente CP alcune disposizioni dell'accordo possono rimane in vigore in riconoscimento dei diritti di proprietà intellettuale e delle disposizioni sulla riservatezza.

9.11 Comunicazioni individuali e comunicazioni ai partecipanti

La RA comunica all'indirizzo mail fornito dal Titolare al momento dell'acquisizione l'emissione o il cambio di stato del certificato.

Il Centro di Certificazione comunica al Titolare del certificato l'avvenuta pubblicazione di una nuova versione del software di firma utilizzando un processo informatico interno al software di firma stessa.

La CA accetta comunicazioni da parte dell'utente Titolare nelle modalità riportate al paragrafo 1.5.

9.12 Emendamenti

Il Ministero della Difesa si riserva la facoltà di modificare questo CP in qualsiasi momento. Per ogni cambiamento sarà prodotta e pubblicata una nuova versione di questo CP, dandone opportuno preavviso.

Un OID deve essere cambiato solo nel caso di una ristrutturazione del OID principale, non imputabile alla PKI Difesa.

9.13 Procedure per la risoluzione delle dispute

Per ogni eventuale controversia e disputa il Foro competente è quello di Roma.

9.14 Legge Applicabile

Questo CP è soggetto alla legge italiana e come tale sarà interpretato ed eseguito. Per quanto non espressamente previsto nel presente CP, valgono le norme vigenti.

9.15 Conformità con le norme applicabili

Questo CP è soggetto alle vigenti norme nazionali ed estere, tra cui, ma non limitatamente, le restrizioni di esportazione o l'importazione di software, hardware, o informazioni tecniche.

9.16 Disposizioni Varie

Essendo il certificato di firma fornito congiuntamente al modello ATe sono da ritenersi applicabili tutte le disposizioni vigenti relative all'impiego e all'uso del modello ATe in ambito Ministero della Difesa e Pubbliche Amministrazioni.

Per i dipendenti del Ministero della Difesa il certificato di firma viene rilasciato a bordo del modello ATe, tessera di riconoscimento del dipendente, ed è considerato uno strumento di lavoro.

Per i dipendenti di un Ente/P.A. il rilascio del modello ATe e dei relativi certificati è vincolato alla stesura di un accordo di collaborazione tra l'Ente/P.A. stessa ed il Ministero della Difesa.

Nel caso in cui una clausola o disposizione di questo CP è ritenuta inapplicabile da un organo giudiziario che ne ha l'autorità, il resto del CP resta valido.

La PKI Difesa può, per sopravvenuti motivi di interesse dell'Amministrazione della Difesa, recedere unilateralmente dell'accordo di collaborazione stipulato con altra Pubblica Amministrazione ai sensi dell'articolo 15 e dell'articolo 11, commi 2 e 3 della L.n.241/90.

Nella misura consentita dalla legge, la PKI Difesa non può garantire tutto ciò che è indicato nel presente CP quando uno o più eventi di forza maggiore si verificano.

Per eventi considerati di "forza maggiore" si intendono guerre, atti di terrorismo, disastri naturali, guasti alle apparecchiature per la fornitura di energia o guasti della rete Internet o ad altre infrastrutture.

9.17 Altre disposizioni

Pubblicazione SMD -I-009 "Norme di gestione e d'impiego per il rilascio in formato elettronico della in formato elettronico della tessera personale di riconoscimento Mod. ATe e dei certificati digitali emessi dalla Public Key Infrastructure (PKI) della DIFESA, in vigore.

La suddetta pubblicazione è di riferimento anche per le P.A. che hanno stipulato un accordo di collaborazione con il Ministero della Difesa.