Ministero della Difesa

Public Key Infrastructure

Certificate Policy

Certificati di Marcatura Temporale

CP – Certificate Policy

Autore:	Ministero della Difesa
Versione:	1.7
Data del documento:	24 Marzo 2025
No Doc.:	IT-CP–TSA01

Certificate Policy

Certificati di Marcatura Temporale

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 15:42:35
	Lgt. Gennaro GIANNINO	Responsabile Auditing	*Firmato Digitalmente da/Signed by:* GENNARO GIANNINO Lgt. *In Data/On Date:* giovedì 27 marzo 2025 08:32:00
	S.T.V. Ernesto PETRONI	Responsabile Sicurezza	*Firmato Digitalmente da/Signed by:* ERNESTO PETRONI *In Data/On Date:* mercoledì 26 marzo 2025 16:00:00
	Ten.Col. Andrea PERNA	Responsabile Servizi Tecnici e Logistici	*Firmato Digitalmente da/Signed by:* ANDREA PERNA *In Data/On Date:* venerdì 28 marzo 2025 14:16:41
Approvato da	Gen.Div. AAran Sandro SANASI	Prestatore Servizi Fiduciari Qualificati (QTSP)	*Firmato Digitalmente da/Signed by:* SANDRO SANASI *In Data/On Date:* venerdì 28 marzo 2025 16:35:29

Indice

Versione	Sezione	Descrizione	Data
1.7	Tutte	Cambio componenti Gruppo di Certificazione. Cambio Certificatore	24 marzo 2025
1.6	Tutte	Sostituito Responsabile alla Sicurezza	13 Ottobre 2022
1.5	Tutte	Sostituito Responsabile alla Sicurezza	22 Novembre 2021
1.4	Tutte	Cambio componenti gruppo Certificazione	06 Aprile 2021
1.3	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
1.2	Tutte	Cambio Denominazione Ente da Comando C4 Difesa in Comando per le Operazioni in Rete Sostituite le figure di Responsabile Periferico con Funzionario Autorizzato alla Validazione dei Datii, Incaricato al Trattamento dei Dati con Operatore Autorizzato all'inserimento dei dati	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 Qualidficato accreditato presso l'Agenzia per l'Italia Digitale (Ag.ID), per il rilascio dei certificati per la marcatura temporale (Time Stamping) secondo il Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014, anche detto eIDAS.

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

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 marcatura temporale.

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 (CA) denominata "Ministero della Difesa – Time Stamping Authority" mediante la quale la Difesa emette e gestisce i certificati di marcatura temporale utilizzati dal proprio personale e dal personale delle Pubbliche Amministrazioni (PA) che hanno stipulato un accordo con il Ministero della Difesa.

1.2 Nome documento e identificazione

Internamente alla TSA sono definiti i seguenti OID relativi ai certificati da essaemessi.

L'Object Identifier (OID) assegnato al Ministero della Difesa è: 1.3.6.1.4.1.14031.

L'OID della CA di Marcatura Temporale (TSA) del Ministero della Difesa è: 1.3.6.1.4.1.14031.2.1.7.

Il presente CP è referenziato, nei certificati di marcatura temporale, col seguente OID: 1.3.6.1.4.1.14031.2.1.7.101

La presente policy si basa a sua volta sulla seguente policy: **BSTP** *"a best practices policy for time-stamp"* emessa da ETSI e identificata dal seguente OID: `itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)`, ovvero `0.4.0.2023.1.1`.

Nella tabella seguente sono riportati gli OID dei certificati gestiti dalle CA-TSA del Ministero della Difesa accreditate in Italia prima del 1 Giugno 2016 e gli OID dei certificati gestiti dalla CA-TSA eIDAS:

Descrizione	OID
OID base del Ministero della Difesa	1.3.6.1.4.1.14031
Base della vecchia struttura PKI (CSP)	1.3.6.1.4.1.14031.**1**
Policy della vecchia struttura PKI definita in www.pki.difesa.it/firmadigitale.pdf	1.3.6.1.4.1.14031.1.**1**
Base della nuova struttura PKI (CSP)	1.3.6.1.4.1.14031.**2**

Descrizione	OID
Policy della nuova struttura PKI definita in www.pki.difesa.it/ManualeOperativoDifesa.pdf	1.3.6.1.4.1.14031.2.**1**
OID del certificato della CA TSA	1.3.6.1.4.1.14031.2.1.**3**
OID del certificato di OCSP per la CA TSA	1.3.6.1.4.1.14031.2.1.3.**1**
OID del certificato di TSU	1.3.6.1.4.1.14031.2.1.3.**2**
Base della nuova struttura PKI eIDAS (CSP)	1.3.6.1.4.1.14031.**2**
Policy della nuova struttura PKI definita in https://pki.difesa.it/tsp/	1.3.6.1.4.1.14031.2.**1**
OID del certificato della CA TSA eIDAS	1.3.6.1.4.1.14031.2.1.**7**
OID del certificato di OCSP per la CA TSA eIDAS	1.3.6.1.4.1.14031.2.1.7.**1**
OID del certificato di TSU eIDAS	1.3.6.1.4.1.14031.2.1.7.**2**
OID del CPS per il servizio di Marcatura Temporale eIDAS in lingua Italiana	1.3.6.1.4.1.14031.2.1.7.**100**
OID del CP per il servizio di Marcatura Temporale eIDAS in lingua Italiana	1.3.6.1.4.1.14031.2.1.7.**101**
OID del documento PKI Terms and Conditions del servizio di Marcatura Temporale eIDAS in lingua Italiana	1.3.6.1.4.1.14031.2.1.7.**102**
OID del documento PKI Disclosure Statement del servizio di Marcatura Temporale eIDAS in lingua Italiana e Inglese	1.3.6.1.4.1.14031.2.1.7.**103**
OID del CPS per il servizio di Marcatura Temporale eIDAS in lingua Inglese	1.3.6.1.4.1.14031.2.1.7.**200**
OID del CP per il servizio di Marcatura Temporale eIDAS in lingua Inglese	1.3.6.1.4.1.14031.2.1.7.**201**
OID del documento PKI Terms and Conditions del servizio di Marcatura Temporale eIDAS in lingua Inglese	1.3.6.1.4.1.14031.2.1.7.**202**

1.3 Partecipanti alla PKI

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

1.3.1 Certification Authority

La CA è il soggetto terzo e fidato che emette i certificati digitali, firmandoli con la propria chiave privata (chiave di CA). La CA dedicata ad emettere i certificati di marcatura temporale ed a gestire lo stato degli stessi viene detta Time Stamping Authority (TSA).

Nell'ambito del servizio qui descritto, il ruolo di TSA 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 OPERAZIONI IN RETE
Indirizzo	Via Stresa 31b 00135 Roma
Legale Rappresentante	Comandante del Comando per le Operazioni in Rete
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 per la Difesa il compito di Prestatore di Servizi Fiduciari Qualificati (QTSP).

La Certification Authority è una Root-CA che emette direttamente i certificati per le Time Stamping Unit, 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 del Comando.

1.3.2 Registration Authority

La Registration Authority (RA) è la persona, la struttura ovvero l'organizzazione che assolve alle seguenti:

- accoglimento e validazione delle richieste di emissione e gestione dei certificati digitali;
- registrazione del soggetto richiedente il certificato digitale e dell'organizzazione di appartenenza;
- autorizzazione all'emissione, da parte della TSA, del certificato digitale richiesto;
- fornitura al personale della Difesa ed al personale delle PA che hanno firmato un accordo di collaborazione del servizio di marcatura temporale e delle informazioni necessarie per il suo utilizzo.

Tale attività è svolta per i certificati di marcatura temporale direttamente dal Centro di Certificazione del Ministero della Difesa e non ha alcuna interazione con utenti esterni, in quanto i certificati digitali emessi sono usati esclusivamente all'interno della PKI Difesa.

1.3.3 Utenti finali (titolari)

Gli utenti finali, ovvero i servizi di Time Stamp Unit, sono i dispositivi hardware/software che richiedono un certificato digitale contenente la corrispondente chiave privata dei richiedenti al fine di produrre marche temporali a loro favore.

1.3.4 Parti interessate

Le parti interessate sono i soggetti che fanno affidamento sulle informazioni contenute nel certificato digitale per le operazioni di verifica dei documenti marcati temporalmente dagli utilizzatori del servizio.

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, ai medesimi soggetti, 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, quale suo delegato, dell'applicazione delle norme vigenti sul processo di certificazione, del corretto funzionamento dei servizi tecnologici e della corretta conduzione del servizio.

1.4 Uso dei certificati

Questo paragrafo elenca le tipologie di applicazioni per le quali vengono rilasciati i certificati digitali.

La CA del Ministero della Difesa Time Stamp Authority eIDAS usa la propria coppia di chiavi per:

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

Il titolare del certificato di marcatura temporale, la Time Stamping Unit (TSU), usa la propria coppia di chiavi per:

- firmare il digest di un documento producendo una marca temporale (Time Stamp Response) nei formati previsti dalla normativa vigente.

Le marcature temporali vengono emesse solo a fronte di richieste di marcatura eseguite con algoritmi di hashing SHA-256, SHA-384 e SHA-512. Il livello di accuratezza della data/ora inclusa nelle marche temporali emesse è +/- un (1) secondo rispetto all'ora UTC.
Le marche temporali emesse dai servizi di Time Stamping Unit sono conservate dal certificatore per una durata pari a 20 anni dalla data di emissione.

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

L'uso improprio dei certificati digitali emessi dal Ministero della Difesa sulla base di questo CP è vietato e qualora il Ministero della Difesa ne venga a conoscenza comporterà la revoca immediata degli stessi.

1.5 Amministrazione delle policy

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

Questo CP è redatto, pubblicato ed aggiornato dal Centro di Certificazione del Ministero della Difesa presso il 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 telefonico +39-06-46914444 del Help Desk del Comando per le Operazioni in Rete Difesa 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 disposizioni in esso contenuto sono conformi alle 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 logistici 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 e di termini utilizzati all'interno del documento, così come una lista di acronimi e il loro significato.

Termine/ Acronimo	Descrizione	Spiegazione
Ag.ID	Agenzia per l'Italia Digitale (ex gestione DigitPA) CA Certification	Organismo di vigilanza Italiano
CA	Certification Authority	Un'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
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	
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
OCSP	On-line Certificate Status Protocol	Servizio di verifica dello stato dei certificati
OTP	One Time Password	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
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

Termine/ Acronimo	Descrizione	Spiegazione
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

[ETSI 862] ETSI TS 101 862 v.1.3.2 – "Qualified Certificate profile", June 2004.

[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)

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 ha la responsabilità della pubblicazione delle informazioni e della frequenza con la quale esse vengono reso pubbliche.

Per "repository" si intende un insieme di archivi o registri on-line contenenti informazioni di interesse pubblico relativi ai certificati digitali 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 Operaioni in Rete mette a disposizione degli utenti finali i seguenti repository:

- siti web http://www.pki.difesa.it e https://pki.difesa.it – 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 delle P.A. che hanno stipulato un accordo di collaborazione con il Ministero della Difesa.

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

La Time Stamping 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 ed il seguente software:

- Certification Practice Statement (CPS);
- Certificate Policy (CP);
- Terms and Conditions (T&C);
- PKI Disclosure Statement (PDS);
- software per l'impiego della Firma Digitale (Kit di Firma);
- l'elenco delle liste di revoca dei certificati digitali (CRL);
- Certificati della TSA.

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

Inoltre la TSA 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 in occasione di 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 con frequenza giornaliera ovvero in caso di necessità. 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 dalla rete interna della Difesa e delle 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 Marcatura Temporale (TSU) è accessibile dall'indirizzo: http://tsapkiff.difesa.it/tsa

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 verificare l'identità e/o gli attributi del richiedente il certificato digitale da parte della TSA 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.

Il dettaglio dei contenuti è riportato nella seguente tabella:

CA Marcatura Temporale (TSA)	
Common Name (CN)	Ministero della Difesa - Time Stamping Authority eIDAS
SERIALNUMBER	97355240587
Organizational Unit (OU)	S.M.D. - C.do C4 Difesa
Organizzation (O)	Ministero della Difesa
Country Code (C)	IT

Certificato di Marcatura Temporale (TSU)	
Common Name (CN)	Ministero della Difesa – Time Stamp Unit *YYYYMMDDHHmm*
Organizational Unit (OU)	S.M.D. - C.do C4 Difesa
Organization (O)	Ministero della Difesa
Country Code (C)	IT

Nel certificato di marcatura temporale, la parte del CN indicata come *YYYYMMDDHHmm* varia a ogni emissione di certificato assumendo automaticamente la data e l'ora dell'emissione stessa (ad es. 201612140000 per il 14/12/2016 00:00).[1]

I certificati dei servizi di marcatura temporale (TSU) e della CA di marcatura temporale (TSA) contengono nomi che prevedono una semantica comprensibile per consentire la determinazione dell'identità della TSU e della TSA.

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

Il Ministero della Difesa non prevede l'emissione di certificati digitali con tale tipologia di attributi.

I campi del Distinguished Name e i relativi contenuti, seguono le specifiche della firma digitale in ambito nazionale, in particolare la determinazione n. 121/2019 di AGID.

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

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

Il Ministero della Difesa non prevede l'adozione di tale tipologia di servizio.

[1] 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.

3.2 Validazione iniziale dell'identità

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

Il processo di registrazione dei titolari, ovvero dei servizi di TSU, avviene attraverso una procedura informatica automatizzata.

La TSA riconosce esclusivamente i servizi di TSU interni alla PKI Difesa come uniche entità identificabili. La validazione iniziale dell'identità del servizio di TSU è eseguita internamente al Centro di Certificazione nel momento dell'istituzione del servizio di TSU.

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

Il servizio TSU, in automatico e internamente alla PKI Difesa, invia la chiave pubblica alla CA sotto forma di CSR ed in formato PKCS#10 [RFC2314].

Nessuna organizzazione esterna al Ministero della Difesa può richiedere certificati digitali di marcatura temporale.

Non sono accettate richieste di certificato proveniente da entità al di fuori del Ministero della Difesa e delle PA che hanno firmato un accordo di collaborazione con la Difesa.

Ogni servizio TSU interno alla PKI Difesa è dotato di certificato digitale attraverso il quale si autentica come servizio che può richiedere l'emissione/rinnovo delle chiavi/certificati.

Il censimento e la messa in funzione iniziale di ogni servizio TSU interno alla PKI Difesa è compito del personale del Centro di Certificazione.

I certificati digitali emessi non contengono informazioni che non possono essere verificate.

La TSA non esegue alcuna validazione dei dati del richiedente ma controlla 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

Per quanto riguarda le richieste di rinnovo della chiave e del corrispondente certificato digitale, si applica quanto dettagliato riguardo l'emissione del primo certificato nella sezione 3.2 e sue sottosezioni.

In caso di revoca di un certificato di marcatura temporale, viene rieseguito quanto dettagliato un rinnovo di chiave (sezione 4.7). Solo i servizi TSU interni alla PKI Difesa autorizzati possono eseguire l'operazione.

3.4 I&A per le richieste di sospensione o revoca

La richiesta di revoca di un certificato di marcatura temporale viene eseguita unicamente dal personale del Centro di Certificazione. Si applicano tutti i meccanismi di identificazione e autenticazione del personale come indicato nella sezione 5.2 e sottosezioni.

4 REQUISITI OPERATIVI DI GESTIONE DEI CERTIFICATI

4.1 Richiesta del certificato

Una richiesta di certificato di marcatura temporale può essere sottoposta alla TSA esclusivamente e automaticamente dal servizio di TSU interno alla PKI Difesa. Solo un servizio TSU autorizzato può sottomettere una richiesta di certificato digitale.

Nel momento in cui viene eseguito il processo automatico di richiesta di certificato digitale da parte della TSU, il servizio genera una nuova coppia di chiavi sull'Hardware Security Module (HSM), genera le informazioni da includere nel Distinguished Name del certificato, firma una richiesta di certificato (CSR) e la sottomette alla TSA.

4.2 Processo di approvazione della richiesta

La procedura di richiesta del certificato digitale è automatica e interna alla PKI Difesa, quindi si considera identificata e autenticata se il servizio TSU viene riconosciuto come tale mediante verifica del certificato di mutua autenticazione utilizzato per l'I&A.

La TSA accetta le richieste di certificati in formato PKCS#10 in conformità alle specifiche RFC 2986. Una richiesta nel presente formato dimostra il possesso della chiave privata corrispondente.

La procedura di richiesta di certificato certificato è automatica e interna alla PKI Difesa, quindi, a meno di inconvenienti tecnici, si considera sempre approvata.

Le richieste di emissione vengono processate in tempo reale e in modo sincrono.

4.3 Emissione del Certificato

Non appena viene sottoposta una richiesta di certificato alla TSA, questa emette il certificato, lo memorizza sul proprio database e ne dà evidenza pubblicandolo sul Directory Server. Il certificato viene restituito al servizio TSU.

4.4 Accettazione del certificato

Il certificato è considerato accettato dalla TSU nel momento in cui viene salvato sull'HSM e viene attivato il suo utilizzo.

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

L'emissione del certificato di marcatura temporale non necessita di alcuna notifica alle altre entità.

4.5 Uso della coppia di chiavi e del certificato

L'uso della chiave privata corrispondente alla chiave pubblica è consentita solo dai servizi di TSU interni alla PKI Difesa.

Il certificato è usato solo in accordo con le leggi e con i termini indicati nel Certificate Policy (CP) e nel CPS. Il servizio TSU usa la coppia di chiavi ed il certificato digitale esclusivamente per produrre marcature temporali secondo lo standard.

Le parti interessate devono valutare indipendentemente:

- l'appropriatezza dell'uso del certificato digitale per uno specifico scopo che non sia vietato dal presente CP. Il Prestatore di Servizi Fiduciari Qualificati non è responsabile di questa valutazione.
- l'utilizzo del certificato in accordo con l'estensione KeyUsage ed EnhancedKeyUsage del certificato stesso (ad esempio: se il valore dell'estensione KeyUsage è diverso da "Digital Signature - valore 80) e il valore dell'estensione EnhancedKeyUsage è diverso da "Time Stamping (OID 1.3.6.1.5.5.7.3.8), il certificato non può essere usato per la marcatura temporale;
- lo stato del certificato digitale mediante CRL/OCSP e lo stato della TSA emettitrice mediante la Trusted List europea e/o nazionale.

Ammesso che l'uso del certificato digitale sia appropriato, le parti interessate devono utilizzare il software e/o l'hadware appropriato per la verifica delle marche temporali tramite i certificati emessi da questa TSA.

Per agevolare le procedure di verifica, ogni marcatura temporale emessa, contiene sempre il certificato del servizio TSU usato per produrre la marcatura stessa.

4.6 Rinnovo del certificato

Non è previsto un rinnovo del certificato digitale conservando la chiave privata precedente. Per questo motivo ogni nuovo certificato di marcatura temporale per un servizio di TSU prevede un rinnovo della chiave con conseguente emissione del nuovo certificato corrispondente. Per gli aspetti di dettaglio si rimanda alla sezione 4.7.

4.7 Rinnovo della chiave

I servizi di marcatura temporale richiedono, da best-practices, che la durata operativa di una coppia di chiavi sia minore della durata effettiva del certificato associato. Per questo motivo, secondo le tempistiche indicate nella sezione 6.3, viene eseguito il rinnovo della chiave e del conseguente certificato associato.

Le procedure sono simili a quanto indicato nelle sezioni relative all'emissione di un nuovo certificato di marcatura temporale.

Il rinnovo è schedulato secondo le tempistiche indicate nella sezione 6.3.

Una richiesta di certificazione di una nuova chiave pubblica di marcatura temporale può essere sottoposta alla TSA esclusivamente e automaticamente dal servizio di TSU interno alla PKI Difesa.

Non appena viene sottoposta una richiesta di certificato alla TSA, questa emette il certificato digitale, lo memorizza sul proprio database e ne dà evidenza pubblicandolo sul Directory Server. Il certificato digitale viene restituito al servizio TSU.

Il certificato è considerato accettato dalla TSU nel momento in cui viene salvato su HSM e attivato il suo utilizzo.

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

L'emissione del nuovo certificato di marcatura temporale non necessita di alcuna notifica alle altre entità.

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 è necessario 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 del servizio di TSU nel periodo di validità della chiave privata;
- per terme del servizio di TSU.

Qualunque altra circostanza che implica una sostituzione della chiave privata (e quindi del certificato), ma che non coinvolge attività malevoli, viene considerata come un rinnovo di chiavi e non comporta la preventiva revoca del certificato emesso in precedenza.

4.9.2 Chi può richiedere la revoca

La revoca può essere richiesta:

- dal Centro di Certificazione.

4.9.3 Procedure per richiedere la revoca

La revoca può essere richiesta esclusivamente dal personale del Centro di Certificazione. Una volta manifestatasi l'esigenza di revocare un certificato, l'operatore abilitato esegue l'operazione di revoca tramite gli strumenti informatici previsti.

4.9.4 Periodo di tolleranza di una richiesta di revoca

Le richieste di revoca devono essere sottoposte tempestivamente e comunque, entro un tempo di 30 giorni.

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 con una frequenza minima giornaliera ed ha 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 subito dopo la sua emissione sui repository indicati nelle sezioni precedenti ed in un tempo ragionevolmente breve.

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 nel caso in cui siano previste attività di manutenzione o guasti imprevisti.

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 a tutti gli utenti che dispongono di un'applicazione in grado di eseguire la verifica conformemente al RFC 2560.

4.9.8 Altre forme di avvisi di revoca disponibili

Non applicabile.

4.9.9 Circostanze per la sospensione

La sospensione di un certificato di marcatura temporale non è prevista. In caso di necessità, viene revocato ed emesso un nuovo certificato.

4.9.10 Chi può richiedere la sospensione

Non applicabile per quanto indicato al punto 4.9.9.

4.9.11 Procedure per le richieste di sospensione

Non applicabile per quanto indicato al punto 4.9.9.

4.10 Servizio di stato del certificato

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

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

La TSA rende inoltre disponibile anche un servizio OCSP conforme alla specifica [RFC2560].

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 pubblicata:

- almeno ogni 24 ore, anche in assenza di nuove sospensioni o revoche;
- a seguito di una revoca (operazioni di sospensione e riattivazione non sono mai eseguite).

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'Uniform Resource Locator (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 guasti.

4.11 Fine della sottoscrizione

Il certificato di marcatura temporale viene rilasciato esclusivamente ai servizi di TSU interni alla PKI Difesa. La sottoscrizione si intende terminata nell'eventuale momento in cui cessa il servizio di TSU. 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.

4.12 Key escrow e key recovery

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

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 TSA mantiene una copia di backup della chiave di TSA 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.

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

Il sito di Disaster Recovery è ubicato presso il CED della Caserma Ciarpaglini – Comando C4 Esercito ubicato in via Guido Reni, 22 00196 Roma.

L'accesso fisico all'edificio e ai locali interni è consentito solo al personale autorizzato. Gli ospiti vengono preregistrati prima di accedere agli stessi e se non in possesso dei necessari requisiti di sicurezza ed abilitazione ad operare, devono essere accompagnati.

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

L'infrastruttura PKI Difesa è custodita all'interno di una gabbia di sicurezza la cui apertura è consentita al solo personale del Centro di Certificazione previa autenticazione con mod. ATe/CMD.

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

I locali sono muniti di impianto di condizionamento e l'impianto elettrico è protetto da cadute di tensione tramite un sistema UPS e 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 memorizzati all'interno di sistemi di archiviazione ridondati e protetti con adeguati controlli per l'accesso fisico e logico per limitarne l'accesso al personale autorizzato e proteggere tali supporti da accidentale danni (ad esempio, l'acqua, il fuoco, l'elettromagnetismo).

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

I dispositivi crittografici sono fisicamente distrutti ovvero 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 dei 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 e 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 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 sono tenute a svolgere compiti delicati.

I compiti più delicati, come l'attivazione della TSA 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 verifica utilizzando un documento d'identità lettronico rilasciato dall'Ammministrazione della Difesa (Modello ATe/CMD).

I ruoli che richiedono la separazione dei compiti sono:

- le operazioni sui dispositivi hardware e/o software su cui sono immagazzinate le chiavi della CA.

5.3 Sicurezza del personale

Il personale addetto al servizio ha una pluriennale esperienza nel campo della definizione, sviluppo e gestione di servizi di PKI 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 valutare un dipendente idoneo per un ruolo presso il Centro di Certificazione, vengono eseguiti una serie di controlli preventivi per:

- la conferma dei precedenti incarichi;

- il controllo delle referenze professionali;
- il controllo del possesso del Nulla Osta di Segretezza – NOS;
- la conferma delle certificazioni professionali ovvero accademiche equipollenti;
- la verifica di eventuali precedenti giudiziari.

Il Ministero della Difesa fornisce al proprio personale la formazione al momento/in previsione dell'assegnazione dell'incarico presso il Certificatore, nonché la 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 per le responsabilità dell'individuo e prevedono i seguenti argomenti:

- concetti di base sulle PKI;
- responsabilità del lavoro quotidiano;
- sicurezza e politiche 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 prevede corsi formitivi 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 con competenza e in modo soddisfacente.

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

La frequenza della rotazione dei compiti è dettata dalle politiche 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 legge Italiana.

In circostanze limitate, consulenti esterni possono essere utilizzati per ricoprire posizioni di fiducia. Qualsiasi consulente è tenuto agli stessi criteri funzionali e di sicurezza che si applicano al personale della Difesa impiegato in una posizione analoga.

Ai consulenti esterni che non hanno completato o superato le procedure di controllo indicate al punto 5.3.2 è consentito l'accesso alle strutture sicure di PKI solo se accompagnati e direttamente controllati dalle persone di fiducia.

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

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, ecc.

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 TSA, 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 TSA e dei sottoscrittori:
  - richieste di certificato, revoche, sospensioni, riattivazioni;
  - richieste processate con successo e non;
  - generazione ed emissioni di certificati.
- Eventi di sicurezza:
  - accessi alla gabbia di sicurezza;
  - 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 controllo;
  - 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 controlli sono conservati all'interno del database di storage e sono replicati sul sito del Disaster Recovery.

I log di audit della TSA sono estratti giornalmente e vengono 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 supervizione 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 TSA, tutti i sistemi software e hardware vengono sottoposti manualmente e/o automaticamente alla verifica di eventuali vulnerabilità.

5.5 Archiviazione dei dati

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

- le CSR (Certificate Signing Request) fornite dai servizi TSU;
- i dati dei servizi TSU;
- i risultati delle verifiche svolte dalla CA;
- 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 quotidianamente e replicata in tempo reale sul sito del Disaster Recovery.

L'infrastruttura 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 sia in grado di accedervi.

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

La PKI Difesa esegue la copia degli archivi elettronici e delle informazioni immagazzinate in base alle politiche di backup interne al Comando per le Operazioni in Rete e sono mantenuti 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.

I sistemi di archiviazione sono interni.

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 TSA, il Ministero della Difesa rinnova la coppia di chiavi ed il certificato della TSA. 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" si intende la violazione di una o più condizioni vincolanti per l'erogazione del servizio di Certification Authority; per "disastro" si 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 TSA è prevista una 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, ecc.) di una più chiavi private di certificazione.

I backup dei dati immagazzinati nei database primari e di replica sono 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 TSA 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, al software o ai dati il responsabile del Centro di Certificazione interesserà il Community Emergency Response Team (CERT) della Difesa ed il di 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 TSA o dell'infrastruttura, il CERT Difesa e il Centro di Certificazione attivano le procedure di compromissione della chiave.

Il CERT Difesa, che comprende personale preposto alla sicurezza, il Centro di Certificazione e altri rappresentanti incaricati della conduzione operativa della PKI, valutano la situazione, sviluppano un piano d'azione e lo attuano 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 TSA:

- viene informata l'autorità di vigilanza italiana;
- viene generata una nuova chiave privata per la TSA ovvero si decide per la cessazione del servizio.

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 di calamità naturale ovvero 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 a le informazioni di registrazione, le informazioni sullo stato di revoca, gli archivi dei log degli eventi.

6 MISURE DI SICUREZZA TECNICA

6.1 Generazione ed installazione della coppia di chiavi

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

La TSU durante l'atto dell'emissione del nuovo certificato di marcatura temporale genera la coppia di chiavi internamente al HSM anch'esso certificato FIPS 140-2 Level 3 o superiore e Common Criteria EAL4+.

Non viene eseguita nessuna operazione di consegna della chiave privata.

Il certificato, e quindi la chiave pubblica, viene automaticamente consegnato tramite procedura automatica al sistema software che realizza il servizio di marcatura temporale (TSU).

Il Centro di Certificazione rende disponibile il certificato della TSA sul proprio sito web.

La chiave della TSA ha lunghezza 4096 bit.

Un certificato di marcatura temporale 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 TSA 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 servizio utilizzatore del certificato di marcatura temporale 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 PKI Difesa usa HSM certificati FIPS 140-2 Level 3 e Common Criteria EAL 4+ per proteggere la chiave privata della TSA e della TSU.

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

La chiave privata della TSA non è esportabile fuori del HSM.

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

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 marcatura temporale viene generata internamente all'HSM dedicato e non è possibile eseguirne il backup o il processo di key recovery.

La coppia di chiavi associata al certificato della TSA 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 TSA 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.

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

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

La chiave privata della TSA viene attivata al momento dell'attivazione dell'HSM e del servizio TSA.

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

Ove richiesto il Centro di Certificazione distrugge la chiave privata della CA in modo da garantire che non vi siano residui che potrebbe 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 TSA.

6.3 Altri aspetti della gestione della coppia di chiavi

Il certificato della TSA è immagazzinato su un apposito database sul quale vengono eseguite opportune politiche di backup e conservazione.

Inoltre il certificato della TSA 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 termina al raggiungimento della sua data di scadenza o alla sua revoca.

La durata operativa di una coppia di chiavi non è la stessa del corrispondente certificato in quanto viene rigenerato massimo ogni 3 mesi per motivi di sicurezza.

Nel seguito il riepilogo delle durate massime dei singoli certificati:

Entità	Durata certificato	Durata chiave
Certificato di TSA	Fino a 30 anni	Fino a 20 anni
Certificato di TSU	Fino a 10 anni	Fino a 3 mesi
Certificato OCSP	Fino a 5 anni	Fino a 5 anni

6.4 Dati di attivazione della chiave

L'attivazione dell'HSM della TSA necessita dell'ausilio di un certo numero di chiavi e PIN conosciuti esclusivamente dal personale addetto alla gestione operativa del servizio, sotto la responsabilità del Responsabile della Certificazione.

L’attivazione dell’HSM della TSU necessita dell’ausilio di un certo numero di chiavi e PIN conosciuti esclusivamente dal personale addetto alla gestione operativa del servizio, sotto la responsabilità del Responsabile della Certificazione.

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 vengono registrate.

I dati necessari all’attivazione dei token e della chiave sono conservati in 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

6.5 Controlli di sicurezza sugli elaboratori

I sistemi operativi usati dalla TSA per la gestione dei certificati sono dotati di controlli e di livello di sicurezza adeguata 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 TSA siano 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 alla rete 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 tipologia 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 Difesa 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, la sicurezza del personale, la sicurezza del sistema di gestione della configurazione durante la manutenzione del prodotto, pratiche di ingegneria del software, metodologie per lo sviluppo del software in sicurezza, sicurezza dei locali in cui viene eseguito lo sviluppo.

La PKI Difesa è dotata di strumenti per la gestione della sicurezza e di procedure che assicurano che i sistemi operativi e le reti siano aderenti agli stardard di sicurezza configurati.

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 attraverso un sistema di firewall di alta qualità che garantiscono un adeguato filtraggio delle connessioni.

I server TSA 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 vengono 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 TSA 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].

PROFILO DEL CERTIFICATO DELLA TSA

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

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=1.3.6.1.4.1.14031.2.1.7 - Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://pki.difesa.it/tsp
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/timestampauthorityeidas.crl • CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa - Time Stamp Authority eIDAS,OU=S.M.D. - C.do C4 Difesa,O=Ministero della Difesa,C=IT

PROFILO DEL CERTIFICATO DI MARCATURA TEMPORALE (TSU)

Si riporta di seguito il profilo definito per i certificati di marcatura temporale (TSU).

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 TSA, 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 TSA
Subject Key Identifier (SKI)	Variabile e calcolato come da RFC 5280
Key Usage [Critical]	Digital Signature (80)
Enhanced Key Usage [Critical]	Time Stamping (1.3.6.1.5.5.7.3.8)
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.14031.2.1.7.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://pki.difesa.it/tsp
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 DistributionPoints (CDP)	• CRL Distribution Point URL=http://www.pki.difesa.it/timestampauthorityeidas.crl • CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa – Time Stamp Authority eIDAS,OU=S.M.D. - C.do C4 Difesa,O=Ministero della Difesa,C=IT

Come indicato nello standard X.509 il campo Version specifica il numero della versione. Quella utilizzata è la 3 (tre).

Le estensioni contenute nei certificati sono specificate nella sezione 7.1.

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 per indicare la motivazione della sospensione o revoca.

CRL	
Version	2
Issuer DN	Corrispondente al Subject della TSA, 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 come da RFC 5280

ESTENSIONE	**VALORE**
Authority Key Identifier	Valore corrispondente al SKI dalla CA
CRL Number	Numero progressivo della CRL emessa

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	**VARLORE**
Version	3
Serial Number	Variabile come da RFC 5280
Signature	Firma RSA apposta dalla TSA come da RFC 5280
Issuer	Corrispondente al Subject della TSA, 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 TSA
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=1.3.6.1.4.1.14031.2.1.7.1 - 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/timestampauthorityeidas.crl • CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa – Time Stamp Authority eIDAS,OU=S.M.D. - C.do C4 Difesa,O=Ministero della Difesa,C=IT

Viene supportata la versione 1 (uno) delle specifiche OCSP come da RFC 2567.

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, prevede 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 prevede 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 TSA.

8.2 Identità e qualificazione degli ispettori

Le verifiche esterne sono condotte da terze parti indipendenti che offrono adeguate garanzie dal punto di vista organizzativo e tecnologico e sono 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 influenzare l'esito delle ispezioni a carico 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 TSA.

8.4 Argomenti coperti dalle verifiche

Gli audit svolti dagli enti esterni sono finalizzati a verificare la conformità dei servizi di Certification Authority 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.

8.5 Azioni conseguenti alle non-conformità

Nel caso di non-conformità, Ag.ID richiede alla TSA 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 consiste in una relazione che viene utilizzato per chiedere/ mantenere la qualificazione all'Organismo di vigilanza competente sul proprio territorio (per l'Italia Ag.ID).

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 servizi 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.

9.1.1 Costo per l'emissione dei certificati e il rinnovo

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

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 (RA), quest'ultima è qualificata come "Incaricato del trattamento dati".

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 le chiamate ai servizi di verifica dello stato del certificato o per lo scarico della CRL.

Tutte le informazioni non indicate al punto attuale sono considerate non confidenziali.

Questa sezione è soggetta all'attuazione delle leggi in vigore.

La PKI Difesa garantisce la riservatezza delle informazioni considerate confidenziali.

9.4 Privacy dei dati personali

I dati del servizio di marcatura temporale non sono considerati dati personali.

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

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

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

Il personale preposto ad operare presso la PKI Difesa che venga a conoscenza di informazioni private deve proteggerle da compromissione e divulgazione verso soggetti terzi ed è tenuto al rispetto di tutte le leggi nazionali 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 legali 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, diramata con lett. n. M_DSSMD REG2017 0056082 del 12-04-2017) 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 PKI Difesa.

Relativamente alla proprietà di altri dati ed informazioni si applicano le leggi vigenti

9.6 Obblighi e garanzie

9.6.1 Obblighi della CA e garanzie

La CA si impegna a:

- operare in conformità a questo CP e nel CPS;
- identificare i richiedenti come descritto in questo CP e nel CPS;
- emettere e gestire i certificati come descritto nel presente CP e nel CPS;
- fornire un efficiente servizio di sospensione o revoca dei certificati;
- garantire che il titolare possegga, 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

Non applicabile in quanto la RA corrisponde al Centro di Certificazione stesso.

9.6.3 Obblighi del Titolare

Non applicabile in quanto il titolare corrisponde al Centro di Certificazione stesso.

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

9.9 Risarcimenti

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

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 in caso di riorganizzazione dell'OID generale che non sia imputabile alla PKI Difesa.

9.13 Procedure per la risoluzione delle dispute

Per ogni eventuale controversia e disputa è competente esclusivamente il giudice ordinario.

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 le restrizioni di esportazione o l'importazione di software, hardware, o informazioni tecniche.

9.16 Disposizioni Varie

Nel caso in cui una clausola o disposizione di questo CP è ritenuta inapplicabile da un tribunale avente 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 si verificano uno o più eventi di forza maggiore.

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.