Ministry of Defence

Public Key Infrastructure

Certificate Policy

Timestamping Certificates

CP – Certificate Policy

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

Certificate Policy

Timestamping Certificates

Validated by	Serg. Marco D'AGOSTINO	Systems Technical Operations Manager	*Firmato Digitalmente da/Signed by:* MARCO D'AGOSTINO *In Data/On Date:* mercoledì 26 marzo 2025 15:37:18
	Lgt. Gennaro GIANNINO	Auditing Manager	*Firmato Digitalmente da/Signed by:* GENNARO GIANNINO Lgt. *In Data/On Date:* giovedì 27 marzo 2025 08:28:56
	S.T.V. Ernesto PETRONI	Security Manager	*Firmato Digitalmente da/Signed by:* ERNESTO PETRONI *In Data/On Date:* mercoledì 26 marzo 2025 15:56:45
	Ten.Col Andrea PERNA	Logistic and Technical Systems Manager	*Firmato Digitalmente da/Signed by:* ANDREA PERNA *In Data/On Date:* venerdì 28 marzo 2025 14:22:29
Approved by	Gen.Div AAran Sandro SANASI	Qualified Trust Service Provider (QTSP)	*Firmato Digitalmente da/Signed by:* SANDRO SANASI *In Data/On Date:* venerdì 28 marzo 2025 16:16:40

List of contents

Versione	Sezione	Descrizione	Data
1.7	All	Change components of Certification Centre Change QTSP	24 March 2025
1.6	All	Replaced Security Manager	13 Octpber 2022
1.5	All	Replaced Security Manager	22 November 2021
1.4	All	Change components of Certification Centre	7 May 2021
1.3	All	Replaced the URL of web site of QTSP. Added notes to specify the change of name of Department and OU shows in the CA Certificate	5 November 2020
1.2	All	Change name department from"Comando C4" to "Comando COR" Change abbreviation RP with FA Change ITD with OA	9 Marzo 2020
1.1	All	Spelling correction	10 May 2018
	Section 4.2.1	Change the abbreviations RDT and RP with ITD and RT	
1.0			01 June 2017

No. Doc.: EN-CP–TSA01 - 1.3.6.1.4.1.14031.2.1.7.201

1 INTRODUCTION

This paper describes the organization set up by the Ministry of Defence – Stato Maggiore della Difesa Comando per le Operazioni in Rete in its capacity as trust services provider accredited to the Digital Italy Agency (AgID) for issuing timestamping certificates pursuant to EU Regulation 910/2014 of the European Parliament and of the European Council of 23 July 2014, also known as eIDAS.

Additionally, this document describes the processes required to generate, issue, suspend and revoke timestamping certificates.

1.1 Overview

This document is the Certificate Polict (CP) of the Ministry of Defence concerning the issuing and management of timestamping certificates.

The structure and content of this CP are based on RFC 3647 specification.

This document illustrates the workings and operational procedures of the certification authority called "Ministero della Difesa – Time Stamping Authority" whereby the Ministry of Defence issues and manages timestamping certificates that are used by its own personnel and by personnel of public administration bodies who have signed an agreement with the Ministry of Defense.

1.2 Document name and identification

Within the TSA, the following OIDs have been defined regarding issued certificates.

The Object Identifier (OID) assigned to the Ministry of Defence is: 1.3.6.1.4.1.14031.

The OID for the Timestamping Certification Authority of the Ministry of Defence is: 1.3.6.1.4.1.14031.2.1.7.

Reference to this CP in timestamping certificates is made through the following OID: 1.3.6.1.4.1.14031.2.1.7.201

This policy is based, in turn, on the following policy: **BSTP** *'a best practices policy for time-stamp'* issued by ETSI and identified by the following OID: `itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)`, or `0.4.0.2023.1.1`.

The following table shows the OIDs of certificates managed by the CA-TSA of the Ministry of Defence that were accredited in Italy before 1 June 2016. It also includes the OIDs of certificates managed by the eIDAS CA-TSA:

Description	OID
Basic OID for the Ministry of Defence	1.3.6.1.4.1.14031
Basis for former old PKI structure (CPS)	1.3.6.1.4.1.14031.**1**
Policy of the former PKI structure as defined in *www.pki.difesa.it/firmadigitale.pdf*	1.3.6.1.4.1.14031.1.**1**
Basis for the new PKI structure (CPS)	1.3.6.1.4.1.14031.**2**

Description	OID
Policy of the new PKI structure as defined in www.pki.difesa.it/ManualeOperativoDifesa.pdf;	1.3.6.1.4.1.14031.2.**1**
OID of the CA TSA certificate	1.3.6.1.4.1.14031.2.1.**3**
OID of the OCSP certificate for the CA TSA	1.3.6.1.4.1.14031.2.1.3.**1**
OID of the TSU certificate	1.3.6.1.4.1.14031.2.1.3.**2**
Basis for the new PKI eIDAS structure (CPS)	1.3.6.1.4.1.14031.**2**
Policy of the new PKI structure as defined at https://pki.difesa.it/tsp	1.3.6.1.4.1.14031.2.**1**
OID of the eIDAS CA TSA Certificate	1.3.6.1.4.1.14031.2.1.**7**
OID of eIDAS CA TSA OCSP Certificate	1.3.6.1.4.1.14031.2.1.7.**1**
OID of the eIDAS TSU certificate	1.3.6.1.4.1.14031.2.1.7.**2**
OID of CPS for eIDAS timestamping service in Italian	1.3.6.1.4.1.14031.2.1.7.**100**
OID of CP for eIDAS timestamping service in Italian	1.3.6.1.4.1.14031.2.1.7.**101**
OID of the PKI Disclosure Statement for the eIDAS timestamping service in Italian	1.3.6.1.4.1.14031.2.1.7.**102**
OID of the PKI Disclosure Statement for the eIDAS timestamping service in Italian and English	1.3.6.1.4.1.14031.2.1.7.**103**
OID of CPS for eIDAS timestamping service in English	1.3.6.1.4.1.14031.2.1.7.**200**
OID of CP for eIDAS timestamping service in English	1.3.6.1.4.1.14031.2.1.7.**201**
OID of the Terms and Conditions document for the eIDAS timestamping service in English	1.3.6.1.4.1.14031.2.1.7.**202**

1.3 PKI participants

This section provides basic information regarding the Certification Authority, Registration Authorities, and parties interested in the PKI Difesa.

1.3.1 Certification authorities

The Certification Authority is the third and trusted party that issues certificates and signs them with its own private key (CA key). The CA entrusted to issue timestamping certficates and manage their status is called Time Stamping authority (TSA).

As for this service, the capacity of TSA is performed by the Ministry of Defence/Stato Maggiore della Difesa Comando per le Operazioni in Rete identified as follows:

Legal person	STATO MAGGIORE DELLA DIFESA – COMANDO PER LE OPERAZIONI IN RETE-
Address	Via Stresa 31b 00187 Rome
Legal Representative	Commander of Comando per le Operazioni in Rete
Tax code	97355240587
ISO Object Identifier	1.3.6.1.4.1.14031
General Website	www.difesa.it
Certification Centre Website	https://pki.difesa.it/tsp

Email address	info_pkiff@smd.difesa.it
Directory Server	ldap://ldappkiff.difesa.it

The Commander of the Comando per le Operazioni in Rete is also the Trust Services Provider for Defence.

The Certification Authority is a Root-CA that directly issues certificates for Time Stamping Unit, it doesn't issue SubCA certificates and it is not involved in Cross-Certification processes.

NOTE – On 9 March 2020, the department in whitch QTSP is located, has changed its name to COR Command with deed of 4 March 2020.

1.3.2 Registration authorities

The Registration Authority (RA) is the person, structure, or organisation performing several tasks as specified below. As such it:

- accepts and validates issuance requests, and manages digital certificates;
- registrates the applicant for digital certificate and the organization he/she belongs to;
- authorizes the TSA to issue the required digital certificate;
- provides Defence personnel and the personnel of public administration bodies that have signed a cooperation agreement for the timestamping service and the information required for its use.

For timestamp certificates, this activity is performed directly by the Certification Centre of the Ministry of Defence, with no interaction with external stakeholder, for issued digital certificates are only used within the PKI Difesa.

1.3.3 Subscribers

End users, i.e., Time Stamp Unit services, are hardware/software devices that require digital certificates containing the private key of requesting personnel, so that such personnel can be issued timestamps.

1.3.4 Relying parties

Relying parties are all subjects relying on information included in the digital certificate to validate the documents timestamped by users.

1.3.5 Other participants

Personnel in charge of administering and supervising the certification service are organized in compliance with Art. 38, par. 1 of the Decree of the President of the Council of Ministers dated 22/ 2/2013.

In particular, the following profiles are established:

- Security manager;
- Certification and Time Validation Service Manager;
- System Technical Administration Manager

- Technical and logistic services manager;
- Audits and inspections manager.

In compliance with the above-mentioned decree, the same subject cannot be tasked to perform more than one function amongst those listed above (cfr. art. 38/2, Decree of the President of the Council of Ministers of 22/02/2013).

Within the organizational functions of the certification service, the **Certification and Time Validation Manager** is also the **Head of the PKI Difesa Certification Centre** and, as its delegate, reports to the Trust Services Provider as regards the application of current regulations for the certification process, appropriate operation of technical services and correct management of service.

1.4 Certificate usage

This paragraph lists the applications for which digital certificates are issued.

The eIDAS CA Time Stamp Authority of the Ministry of Defence uses its key pair to:

- sign issued digital certificates:
- sign issued Certification Revocation Lists (CRLs).

The holder of the timestamp certificate, i.e., the Time Stamping Unit (TSU), uses its key pair to:

- sign the digest of a document to generate a Time Stamp Response in the formats pursuant to current regulations.

Timestamps are issued only when a stamping request is received through hashing algorythms type SHA-256, SHA-384, and SHA-512. The accuracy of time/date included in the issued timestamps is +/- one (1) second UTC time.
Time stamps issued by Time Stamping Unit services are kept by the TSP for a duration of 20 years from the date of issue

Anything other than usage defined in this paragraph is considered a non-authorized use of the certificate.

Any improper use of certificates issued by the Ministry of Defence on the basis of this CP is not allowed and causes the certificate to be immediately cancelled, should the circumstance be known by the Ministry of Defence.

1.5 Policy administration

The personnel of the Certification Centre holds and keeps this document updated. In his/her capacity of legal representative of the Certification Centre and Trust Services Provider, the Commander of Comando per le Operazioni in Rete approves the document.

This CP is written, published, and updated by the Certification Centre of the Ministry of Defence/Stato Maggiore Difesa – Comando per le Operazioni in Rete, via Stresa 31b, 00135 Rome, Italy.

This document is also revised and updatet when changes are made to the organization (for example, for the change of one of the managers) or for changes in the rules of reference.

For further information or details concerning this CP, please contact:

- the email address of the PKI Difesa certification centre info_pkiff@smd.difesa.it
- the following link: https:/servicedesk.difesa.it;
- the following email address helpdesk@cor.difesa.it
- number +39 (06) 46914444, for the Comando per le Operazioni in Rete Help Desk, which will forward the request to the certification centre.

This CP and the policies therein are assessed by a Certification Authority (CAB).

This CP and the policies therein comply with the policies issued by the Ministry of Defence.

This CP was read and validated in its relevant parts by the Systems Technical Operation Manager, the Auditing Manager, the Security Manager, the Logistic and Technical System Manager. It was approved by the Commander of Comando per le Operazioni in Rete Headquarters as Trust Services Provider for Defence.

1.6 Definitions and acronyms

This paragraph includes a list of definitions of the terms used in this document, as well as a list of the acronyms and their meanings.

Term/Acronym	Description	Definition
Agid	Digital Italy Agency (formerly run by DigitPA) CA certification	Italian Supervisory Body
CA	Certification Authority	A body that issues certificates
CMD	Carta Multiservizi Difesa	A smartcard issued to Defence personnel as a valid electronic ID that also contains the holder's certificates
CP	Certificate Policy	A defined set of rules specifying the applicability of a certificate for a specific community and/or class of applications with specific security requirements.
CPS	Certification Practice Statement	
CRL	Certificate Revocation List	The list of revoked certificates
CSR	Certificate Signing Request	Certificate request
DN	Distinguished Name	Single certificate identifier for the holder
DR	Disaster Recovery	Infrastructure back-up site
FIPS	Federal Information Processing Standard	Shared rules and measures that US state departments must comply with
HSM	Hardware Security Module	Hardware module for safe storage of keys for cryptographic operations
LDAP	Lightweight Directory Access Protocol	The Directory Server where certificates are published
OCSP	On-line Certificate Status Protocol	Verification service for certificate status
OTP	One Time Password	A password that is only valid for one access or transaction
P.A.	Public Administration	Public Administration Bodies
P.D.S.	PKI Disclosure Statement	A document summing up the main concepts in of CP and CPS.
PKI	Public Key Infrastructure	Equipment and Personnel tasked to issue certificates
Private key	Private key	The secret element of asymmetric cryptography based on key pairs
Public key	Public key	The shared element of asymmetric cryptography based on key pairs
RA	Registration Authority	The body in charge of enrolment procedures. It identifies and authenticates the subject requesting a certificate
Public Connectivity Service Network	Public Connectivity Service	Public Administration Interconnection Network
TSA	Time Stamping Authority	The Certification Authority tasked to issue time stamping certificates only
TSP	Trust Service Provider	Trust Services Provider (formerly, Certifier)
TSR	Time Stamp Response	A structure comprising a Time Stamp Token and the response received by the corresponding Time Stamp Unit

Term/Acronym	Description	Definition
TST	Time Stamp Token	Time Stamp: Time Stamping links associates a legally valid date and time to a digital document.
TSU	Time Stamping Unit	A software service that has a time stamping certificate and issues timestamps by signing them digitally with the relevant certificate.

REFERENCE

[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.

[PKCS1] B. Kaliski, "CS#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 Protocol - 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 PUBLICATION AND REPOSITORY RESPONSIBILITIES

This chapter includes the provisions to identify the subject or the authority responsible for managining the repository within the PKI Difesa, publishing information, and the frequency of publication.

'Repository' means a set of archives and on-line logs comprising information of public interest about the certificates and their issuing and management as described in this CP.

2.1 Repositories

The Certification Centre of the Comando per le Operazioni in Rete provides end users with the following repositories:

- https://pki.difesa.it/tsp websites where the CRLs are published along with the documents related to PKI (CP, CPS, PDS, etc…)
- directory server at ldap://ldappkiff.difesa.it as the repository where the issued certificates and the valid CRL are published. This repository can only be accessed from withing the Defence Network and from within the networks of public administration bodies that have signed a collaboration agreement with the Ministry of Defence.

The Certification Centre is in charge of managing both repositories.

The Time Stamping Authority maintains and manages its own repository located within the PKI Difesa, which is protected from external access by firewall and counter intrusion devices.

NOTE – The repository http://www.pki.difesa.it has been redirected to https://pki.difesa.it/tsa

2.2 Publication of certification information

The Certification Centre publishes the following documentation and software on its website: https://pki.difesa.it/tsp:

- Certification Practice Statement (CPS)
- Certificate Policy (CP)
- Terms and Conditions (T&C);
- PKI Disclosure Statement (PDS);
- software for using the Digital Signature (Signature kit);
- the list of digital certificates revocation lists (CRL);
- TSA certificates.

These web sites are available 24 hours a day, 7 days a week.

Furthermore, the TSA publishes the issued certificates and the valid CRL on the Directory Server.

2.3 Time or frequency of publication

All documents and software on the website are published at each update. Documents are published in the PDF format.

Certificates are published on the directory server when they are issued.

CRLs are issued and published at least every day. For further details see section 4.8.

2.4 Access controls on repositories

All material published on the certification centre website (https://pki.difesa.it/tsp) can be freely accessed and/or downloaded.

The register of certificates can be accessed through the Lightweight Directory Access Protocol (LDAP) and referred to in read-only mode in the signature section and exclusively within the Defence network and internally by the public administration bodies that have signed a cooperation agreement with the Ministry of Defence.

Non-autorised users can refer to the LDAP in read-only mode exclusively to recover CRLs.

Only personnel belonging to the certification centre or the CA is allowed to change the contents of the register of certificates.

The Time Stamping Unit (TSU) can be accessed via the following URL: http://tsapkiff.difesa.it/tsa

The Online Certificate Status Protocol (OCSP) can be freely accessed at URL: http://ocsppkiff.difesa.it

3 IDENTIFICATION AND AUTHENTICATION

This chapter describes the procedures used by the TSA or the Registration Authority (RA) to confirm the identity and/or other features related to the holder's certificate before this is issued.

3.1 Naming

The certificates issued by the PKI Difesa follow the X.509v3 standard.

The details as regards contents are as follows:

Time Stamp CA (TSA)	
Common Name (CN)	Ministero della Difesa - Time Stamping Authority eIDAS
SERIAL NUMBER	97355240587
Organizational Unit (O)	S.M.D. - C.do C4 Difesa
Organization (O):	Ministero della Difesa
Country Code (C)	IT

Timestamping Certificates (TSU)	
Common Name (CN)	Ministero della Difesa – Time Stamp Unit *YYYYMMDDHHmm*
Organizational Unit (OU)	S.M.D. - C.do C4 Difesa
Organizzazione (O)	Ministero della Difesa
Country Code (C)	IT

In the timestamp certificate, the CN part indicated as YYYYMMDDHHmm changes every time a certificate is issued and is updated to the date and time of issuance (e.g., 201612140000 for February 14, 2016 00:00)

The certificates of the Time Stamping Unit and of the Time Stamping Authority (TSA) include names whose semantics can be easily understood, in order to facilitate the identification of the very TSU and TSA.

The names of TSU certificates holder and of the issuing authority are registered as Distinguished Name in the subject and issuer fields of certificates.

The Ministry of Defence does not envisage issuing digital certificates with these attributes.

The fields related to Distinguished Name and relevant contents comply with the Italian requirements for digital signature, in particular the determination n. 121/2019 of AGID.

A time stamp certificate is made unique by the Common Name that includes its issuing date.

An OCSP certificate is made unique by the Common Name that includes its issuing date.

The Ministry of Defence does not envisage adopting such service.

3.2 Initial identity validation

This paragraph describes the identification and validation procedures for initial registration of each type of subject.

The holders' registration process, i.e., of TSU services, takes place via an automated digital procedure.

The TSA only recognizes TSU services from within the PKI Difesa as identifiable entities. The initial validation of TSU service identity is made within the Certification Centre as the TSU service is set up.

The TSU can prove it has a private key corresponding to the requested certificate by means of cryptographic verification of the CSR (Certificate Signing Request) previously sent to the TSA.

Automatically and within the PKI Difesa, the TSU sends the public keyt to the CA as a CSR and in PKCS#10 [RFC2314] format.

No organisation other than the Ministry of Defence can request digital timestamping certificates.

No certificate request from subjects not belonging to the Ministry of Defence or public administration bodies that have signed a cooperation agreement with Defence is accepted.

Every TSU within the PKI Difesa has a digital certificate to authenticate itself as a service that can request the issue/renovation of keys/certificates.

The survey and start up of a TSU within the PKI Difesa is a task of the Certification Centre.

Issued certificates do not contain information that cannot be verified.

The TSA does not verify the applicant's data. It only checks that the DN is unique for valid certificates and that the public key is unique.

3.3 Identification and authentication for re-key requests

As far as routine key and the relevant digital certificate re-issue, the provisions set forth in Section 3.2 and its subsections concerting the issue of the first certificate apply.

In case a Time Stamp certificate is revoked, the same procedure for re-keying (see Section 4.7) applies. Only TSU authorised within the PKI Difesa can perform this operation.

3.4 Identification and authentication for revocation request

The request for revocation of a time stamp certificate is submitted by the personnel of the Certification Centre only. All provisions for the identification and authentication of personnel set forth in Section 5.2 and its subsections do apply.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

A time stamping certificate request can be submitted to the TSA exclusively and automatically by the TSU service withi the PKI Difesa. Just an authorized TSU service can submit a digital certificate request.

As the TSU carries out the automatic process to request a digital certificate, the service generates a new key pair on the Hardware Security Module (HSM), generates the information to be included in the Distinguished Name of the certificate, signs a certificate request (CSR) a submits to the TSA.

4.2 Certificate application processing

The digital certificate request procedure is automatic and within the PKI Difesa. Therefore, it is to be considered identified and validated if the TSU service is recognized a such through the verification of the mutual authentication certificate used for identification and authentication.

The TSA accepts certificate requests in the PKCS#10 format in compliance with RFC 2986 specifications. This kind of request proves possession of the corresponding private key.

The certificate request procedure is a automatic within the PKI Difesa and therefore, except in case of technical failure, it is to be considered always approved.

Issuing requests are processed in real time and in simultanously.

4.3 Certificate issuance

As soon as a certificate request is submitted to the signature TSA, the latter issues the certificate, enters it in its database, and publishes it on the Directory Server. The certificate is returned to the TSU service.

Not applicable since the issuing process is automatic and internal.

4.4 Certificate acceptance

The certificate is considered accepted by the TSU as soon as it is entered on the HSM and it is activated for use.

The TSA publishes issued certificates on the Directory Server at the following address: ldap://ldappkiff.difesa.it

Issuing a time stamping certificate does not require any notification to other bodies.

4.5 Key pair and certificate usage

Usage of the private key corresponding to the public key is only allowed by the TSU services within the PKI Difesa.

The certificate must be used in compliance with the regulations and terms specified in the CP and CPS. The TSU service uses the key pair and the digital certificate only to issue time stampings according to standard.

Relying parties must independently assess:

- Appropriate certificate usage for a specific purpose that is not forbidden by this CP. The Trust Services Provider is not responsible for such assessment.
- Certificate usage in accordance with the KeyUsage and EnhancedKeyUsage extension of the certificate itself (for instance: If the value of the KeyUsage extension differs from "Digital Signature - value 80) and the value of the EnhancedKeyUsage extension differs from "Time Stamping (OID 1.3.6.1.5.5.7.3.8), the certificate cannot be used for time stamping;
- The status of certificate through CRL/OCSP and the status of the issuing TSA through the European and/or national Trusted List.

Supposing certificate usage is appropriate, relying parties must use appropriate software and/or hardware to verify signatures that have been put through certificates issued by this TSA.

In order to facilitate verification procedures, each time stamping issued always comprises the TSu service certificate used for the stamping.

4.6 Certificate renewal

Digital certificate renewal is not allowed while maintaining the previous private key. For this reason any new time stamping certificare for a TSU service requires the key to be renewed and, consequently, a new corresponding certificate to be issued. For further details see section 4.7.

4.7 Certificate re-key

According to best practices, time stamping services require the operational lifecycle of a key pair to be shorter than the actual term of the related certificate. For this reason, and according to timelines specified in section 6.3, the key is renewed along with the associated certificate.

Procedures are similar to those described in the sections concerning the issuing of a new time stamping certificate.

Rrenewal is scheduled according to the timelines specificied in section 6.3.

A time stamping certificate request can be submitted to the TSA exclusively and automatically by the TSU service within the PKI Difesa.

As soon as a certificate request is submitted to the signature CA, the latter issues the digital certificate, enters it in its database and publishes it on the Directory Server. The digital certificate is returned to the TSU service.

Not applicable since the issuing process is automatic and internal.

The certificate is considered accepted by the TSU as soon as it is entered on the HSM and its usage is activated.

The TSA publishes the certificates issued on the Directory Server at the following ldap address ldap://ldappkiff.difesa.it

Issuing a time stamping certificate does not require any notification to other bodies.

4.8 Certificate modification

Being signed by an issuing CA, a certificate cannot be modified. Therefore, to amend errors in generating a certificate it is necessary to issue a new one. Required procedures have already been described in this document.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Revocation of a certificate may be requested for the following reasons:

- In case of alleged compromise of the TSU service in the period of validity of the private key;
- For end of the TSU service.

Any other circumstance implying the replacement of the private key (and therefore of the certificate), that however does not entail malaware, is considered as a re-keying procedure and does not cause the previous certificate to be revoked preemptively.

4.9.2 Who can request revocation

Revocation can be requested by the:

- Certification Centre;

4.9.3 Procedure for revocation request

Revocation can only be requested by the personnel of the Certification Centre. When a certificate needs to be revoked, the authorised operator proceeds through the appropriate IT tools.

4.9.4 Revocation request grace period

Revocation requests must be processed as soon as possible and, in any case, no more than 30 days from the request.

Revocation requests are processed as soon as they are submitted to the CA.

4.9.5 CRL issuance frequency (if applicable)

The CRL is published at least every day and is valid for 7 days.

If the certificate/key is revoked, compromised, stolen or lost or if it is suspended or renewed, the CRL is issued at the same time as the relevant operation is performed.

A CRL is published in the above-mentioned repositories immediately, and at least in a reasonably short time, after it has been issued.

4.9.6 On-line revocation/status checking availability

The revocation status may be verified by OCSP query. The OCSP service is available 24 hours a day, except in case of maintenance or failure.

The Online Certificate Status Protocol (OCSP) can be freely accessed at http://ocsppkiff.difesa.it

4.9.7 On-line revocation checking requirements

The service is available to all users having an application that can perform verification in accordance to RFC 2560.

4.9.8 Other forms of revocation advertisements available

Not applicable.

4.9.9 Circumstances for suspension

Suspension of a time stamping certificate is not allowed. If required, the certificate is revoked and a new one is issued.

4.9.10 Who can request suspension

Not applicable for the reasons specified in 4.9.9.

4.9.11 Procedure for suspension request

Not applicable for the reasons specified in 4.9.9.

4.10 Certificate status services

The Defence PKI provides certificate status services such as CRL and OCSP.

The status of a certificate (active, suspended or revoked) is available to all persons concerned by publication of the Certificate Revocation List (CRL) in the format defined by the specific [RFC5280].

The TSA also provides an OCSP service in accordance with the RFC2560 specification.

The CRL is available in two modes:

- Through LDAP [RFC2251] protocol on the ldappkiff.difesa.it server. This can only be accessed by the Difenet network and through the SPC network for public administration bodies that have signed a cooperation agreement with the Ministry of Defence;
- via HTTP protocol [RFC2616] on the www.pki.difesa.it server.

Complete LDAP and HTTP addresses of the CRL are included in the CRLDistributionPoints extension of the certificate.

The CRL is generated and published again:

- at least every 24 hours, even where there are no new suspensions or revocations;
- Following revocation (no suspension or re-activation is executed).

The address of the OCSP server is included in the AuthorityInformationAccess extension of the certificate.

The OCSP service can be freely accessed by anybody.

The OCSP service follows the RFC 2560 standard and can be accessed through the following URL: http://ocsppkiff.difesa.it

Access to the CRL and OCSP service is always available (24 hours a day) except in the event of maintenance or failure.

4.11 End of subscription

The time stamping certificate is exclusively issued by the TSU services within the PKI Difesa. The subscription is considered complete when the TSU service ends. In the case of prolonged unavailability for causes not dependent on the TSP, the latter commits itself to restoring at least the certificate status service through CRL within 24 hours.

4.12 Key escrow and recovery

No Key Escrow or Key Recovery are included in time stamping certificates.

Certification key recovery is possible in case of involuntary cancellation, failure, or replacement of the HSM device. In order to recover the key, the TSA will maintain a backup copy of the TSA key in accordance with the certified methods of the HSM Device manufacturer.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

The security infrastructure consists of passive defence structures (i.e., perimeter walls, remotely-controlled access gates, steel-reinforced doors), active protection elements (i.e., armed guards), and applications, such as systems based on cryptographic tokens, personal codes, username-password combinations to grant access.

The integrity of equipment and systems is constantly maintained and verified, in accordance with applicable regulations with a view to avoid faults that can distrupt services.

The data processing centre comprising the primary location of the PKI Difesa is within the Comando per le Operazioni in Rete, Via Stresa 31b, 00135, Rome, Italy.

The Disaster Recovery site of the PKI Difesa is located within the data processing centre of the Ciarpaglini Barracks – Army C4 Headquarters, Via Guido Reni 22, 00196, Rome, Italy.

Only authorised personnel are granted physical access to the building and internal premises. To access these guests are registered beforehand. If they lack the necessary security and qualification credentials they must be accompanied.

Only authorised personnel can access the data processing centre of the primary site pending authentication via the Modello ATe/CMD.

The PKI Difesa lies within a security perimeter that only personnel of the Certification Centre can access by authentication via the Modello ATe/CMD.

Access to the Disaster Recovery infrastructure of the PKI Difesa is protected by antitampering doors and can only be authorised by surveillance personnel.

All premises are served by air conditioning systems. The power lines are protected against power losses by means of a UPS and a power generator.

The primary site is away from the sea, in an elevated part of the city. For both sites, the Ministry of Defence has adopted reasonable precautions to minimise the impact of water exposure.

All sites are equipped with state-of-the-art systems to detect and suppress fire. All personnel are adequately instructed regarding building evacuation and gathering procedures at designated collection points.

All media containing software, data, audit data, storage and backup information are stored in redundant storage systems. The latter are applied physical and logic protection to prevent unauthorised access and prevent accidental damage to media, e.g., water spills, fire, electromagnetic radiations, etc.

Before they are disposed of, all sensitive documents and alike are shredded. Media used to collect or transmit sensitive information are rendered unusable.

Before they are disposed of, cryptographic devices are physically destroyed or wiped clean according to manufacturers' guidance.

The PKI Difesa backups the system crucial data, controls register data, and other sensitive information regularly.

Backup media are securely stored within the storage units.

5.2 Procedural controls

The Ministry of Defence takes care to draft and update a Security Plan about the assets and the technical and organisational procedures to achieve adequate levels of operational security.

Among people with trusted roles are all employees, support personnel, and consultants who access the authentication and control systems or the cryptography operations that may actually impact on:

- the conduct and validation of PKI Difesa operations;
- the acceptance, rejection, or other process concerning certificate issuance, revocation, renovation, or enrolment information;
- the holder enrolment process.

The following are considered trusted roles:

- the Certification Centre Operators;
- The Trust Services Provider;
- external personnel identified and authorised beforehand.

The PKI Difesa established, maintains and strengthens control procedures to ensure separation of duties based on job-related accountability, so that multiple people can perform delicate tasks.

Sensitive tasks, such as the activation of the TSA and the activation of cryptographic modules require the presence of multiple trusted roles.

The internal audit procedures have been established to ensure at least two people with trusted roles have both the physical and logical access to a device.

The identity of all trusted personnel is verified by using an electronic ID issued by Defence (Modello ATe/CMD).

The roles that require separation of duties are those for:

- operations on hardware and/or software devices where the CA keys are stored;

5.3 Personnel controls

The expertise of assigned personnel in terms of drafting, development and management of PKI Difesa services spans over multiple years. Such personnel has been adequately trained with respect to the procedures and instruments that will be used in all phases of operations.

The experience of personnel operating within the PKI Difesa covers several years. Each operator holds special security clearance.

Before an employee is cleared to take a role at the Certification Centre, several background checks are performed to ascertain:

- his/her previous posting;
- professional background;
- current status of security clearance;

- professional certifications or other similar academic credentials;
- Any criminal records.

The Ministry of Defence provides training to its personnel as soon as they are assigned to the certification centre. It also provides for on-the-job training to fulfil tasks effectively and satisfactorily.

The Ministry of Defence Training Programmes are consistent with individual responsibilities and cover the following topics:

- Basic PKI concepts;
- daily responsibilities;
- operational and procedural security and policies;
- use and operation of installed and distributed hardware and software;
- Security incident management and event communication;
- Disaster Recovery and Business Continuity.

The Ministry of Defence organises training and update courses for its personnel whose duration and frequency are adequate to maintain proper levels of skill, to operate in a compentent and satisfactory manner.

Within the PKI Difesa, job rotation is such that a period of operational guidance is always guaranteed to ensure knowledge is transferred between the incumbent and incoming operators.

Job rotation frequency is part of the personnel employment policies in force at the Ministry of Defence.

Penalties for unauthorised access are envisaged in the Uniform Military Code.

All activities are subject to Italian law.

In a limited number of cases, independent contractors may be authorised to assume trusted roles. Independent contractors are applied the same functional and security criteria of PKI Difesa personnel serving in a similar position.

Independent contractors who have not completed the background check procedure mentioned in section 5.3.2 will only be authorised to access the secure facilities of PKI Difesa if escorted by trusted roles of the certification centre.

The certification centre provides its employes with training and documentation so that they can perform effectively.

5.4 Audit logging procedures

The main events related to certificate life cycle management, including requests for certification, suspection or revocation are stored electronically.

Other events are also stored, namely physical access to the infrastructure, logical access to the certificate management system, entry and exit from premises where certification is issued, etc.

The type, date, and time of the event is recorded, together with the information useful to identify involved personnel and the outcome of actions.

Information are stored in the audit log. The audit log files are backed up daily on a permanent medium.

The PKI Difesa records the following significant events, either manually or automatically:

- Key life cycle management events concerning the TSA, including the following:
  - Generation, backup, storage, recovery, preservation, and destruction of key;
  - Events connected to the life cycle of cryptographic HSM devices.
- Management events concerning the TSA certificates life cycle and subscribers, including:
  - requests, revocation, suspension, re-activation of certificates;
  - successful or unsuccessful processed requests;
  - generation and issuance of certificates.
- Security-related events, such as:
  - access to the security perimeter;
  - access to systems;
  - Firewall logs;
  - Security-related actions performed by operators;
  - System crash events, hardware faults, or other anomalies.
- Registry entries include the following elements:
  - record date and time;
  - Serial or sequential number for the audit log entries;
  - Identity of the operator signing the audit log entry;
  - type of entry;
  - description text

Audit logs are generated in real time and are extracted and checked on a daily basis.

System logs and firewall logs are generated in real time and stored daily.

Moreover, the certification centre generates the following reports:

Report Name	Frequency
Disaster Recovery Effectiveness Report	Annual
Practice Compliance Report	Half-yearly
Hardware Compliance Report	
HSM Keys Activation Verification Report	
Asset Survey	
Audit Log Content Check Report	Bimonthly
Audit Log Integrity Verification Report	Monthly
Individual Audit Logs Integrity Verification Report	

Certificate life cycle logs shall be retained for 20 years.
Server logs shall be retained for 3 months.
Access logs for the security perimeter shall be retained for at least 1 year.
Firewall logs shall be retained for no longer than 1 year.
Cryptographic devices logs shall be retained for 4 months.

Audit logs are stored within the database; a backup copy is maintained at the Disaster Recovery site.

The audit logs of theTSA are extracted on a daily basis and signed by the Technical Services Manager.

On a daily basis, a copy of the audit logs is automatically extracted from the database and copied on an external storage system, digitally signed and preserved.

Server logs are extracted on a daily basis.

System logs are stored locally and backed up on external storage systems, where they are kept for 3 months.

The infrastructure has an audit log supervisory system to monitor events in real time.

Internal monitoring processes are active on the servers, which send notifications to the certification centre operators in case of error.

Apart from issuance and change of certificate status, no additional notifications are sent to certificate holders.

During regular Signature TSA activities, all software systems and hardware are subject to manual and/or automated vulnerability checks.

5.5 Records archival

The Signature TSA stores all information related to issuance and certificate management processes, including:

- the CSRs (Certificate Signing Requests) provided by TSU services;
- TSU services data;
- the results of CA audits;
- the requests for revocation or suspension;
- all issued certificates;
- audit logs, for at least 20 years;

A backup copy of data, applications, audit log, and any other file required for the full recovery of service is made daily and mirrored on the Disaster Recovery site.

The PKI Difesa collects and manages the following:

- all audit logs listed in section 5.4;
- Information on certificate requests;
- supporting documents;
- information on the life cycle of certificates.

As far as event logs are concerned, see section 5.4.

All certificates and the related requests are stored for 20 years after expiration.

The PKI Difesa protects the archive so that only authorised personnel and trusted roles are granted access.

The archive is protected against unauthorised access, modification, cancellation or other alteration by unauthorised personnel.

The PKI Difesa backups digital archives and stores information according to the internal policies of the Comando per le Operazioni in Rete. Backups are kept in an external storage device.

Copies of paper documents are kept in a specific rack.

Database entries and certificates contain information about the date and time as obtained from a certain source.

Storage systems are internal systems.

Only authorised personnel and trusted roles are granted access to the archive. Integrity of information is checked during both the backup and restore phases.

5.6 Key changeover

Within two thirds along the SignatureTSA certificate life, the Ministry of Defence renews the key pair and the TSA Certificate. From that moment on, the new certificates and new CRL are signed using the new key.

5.7 Compromise and disaster recovery

The expression 'key compromise' means the violation of one or more binding conditions required to deliver the CA service; 'disaster' indicates a harmful event whose consequences make the service unavailable under regular conditions.

In case of Signature TSA private key compromise a special procedure exists for the recovery of certification services. The procedure is included in the Security Plan for the Comando per le Operazioni in Rete.

By all means, recovery from compromise or disaster always takes place when one of the following occurs:

- Fault of one or more pieces of equipment used to deliver certification services;
- Compromise (i.e. disclosure to non autorized third parties, loss, etc.) of one or several certification private keys.

Backup of data stored in primary and replica databases takes places several times during the day. Data are saved on backup storage devices at the site(s) in order to increase reliability.

Backups can be used to restore the database in case of compromise or faults.

In case of faults, services can be activated on the Disaster Recovery site to limit inconveniences.

Backups of TSA keys are stored in a reinforced rack, access to which is restricted to authorised personnel. Only authorised personnel can access the area where the rack is placed.

In case of corrupted equipment, software, or data the Certification Centre Manager shall inform the Defence Community Emergency Response Team (CERT) and the Comando per le Operazioni in Rete as Defence Trust Services Provider to trigger all required incident management and investigation procedures.

If necessary, the compromise or Disaster Recovery procedures will be activated.

In case of supposed compromise of TSA or infrastructure, the Defence CERT and the Certification Centre shall activate the key compromise procedures.

The Defence CERT is composed of security personnel, the Certification Centre, and other representatives who manage operations at the PKI Difesa, evaluate situations, decide on and

implement the action plan with the approval of the Commander of the Comando per le Operazioni in Rete as Provider of Trust Services.

Should revocation ofthe TSA certificate be required:

- The Italian Supervisory Authority shall be informed;
- a new private key for the TSA is generated, unless a decision is made to cancel the service.

The certification centre has created a Disaster Recovery site similar to the structure of the primary site in order to limit disruption to services in case the primary site suffers damages.

What is more, it has implemented, tested, and keeps up-to-date a plan to activate the Disaster Recovery plan to mitigate any effect due to natural disaster or man-made actions.

5.8 CA or RA termination

Should the Trust Services Provider terminate its activity, the Digital Italy Agency shall be notified at least sixty days before termination. Holders of certificates issued by the Trust Service Provider should also be notified that all unexpired certificates will be revoked upon termination. When possible, the Trust Service Provider shall also notify users of time stamping service regarding the suspension of the service.

The Trust Services Provider shall destroy private keys, including the backup copies, so that recovering such keys is impossible.

The Trust Service Provider also communicates with the cessation the eventual disclosure of any information required by another Trust Service Provider or its cancellation (the replacement of a Certifier prevents the revocation of the certificates and the related documentation).

The Certification Authority appoints another depositary for the certificate log and the relevant documentation [DLGS82].

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

The key pair used by the TSA to sign certificates and the CRLs shall be generated within a FIPS 140-2 Level 3 or above certified cryptographic device (HSM) with Common Criteria EAL4+ in a physically safe environment.

While the new time stamping certificate is being issued, the TSU generates the key pair within a FIPS 140-2 Level 3 or above certified cryptographic device (HSM) with Common Criteria EAL4+.

There is no delivery of private key.

The certificate, and therefore the public key, is automatically delivered through an automatic procedure to the software system that performs the time stamping service (TSU).

The Certification Centre makes the TSA certificate available on its web site.

The TSA Key is 4096 bit in length.

A time stamping certificate key is 2048 bit in length.

An OCSP certificate key is 2048 bit in length.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The key pair used by the TSA to sign the certificates and the CRLs is stored within a high-quality HSM (Hardware Security Module) with FIPS PUB 140-2 Level 3 security certification and Common Criteria EAL 4+.

The key pair used by the Signature CA to sign the certificates and the CRL is stored within a high-quality HSM (Hardware Security Module) with FIPS PUB 140-2 Level 3 security certification and Common Criteria EAL 4+.

In order to protect the TSA and the TSU private key, the PKI Difesa uses Hardware Security Modules (HSM) with FIPS 140-2 Level 3 Certificates and Common Criteria EAL 4+.

For the execution of particularly sensitive operations, such as cryptographic operations connected to TSA activation, the PKI Difesa has implemented a procedure that requires multiple operators, each of whom holds a part of the 'secret' required to finalise the operation.

The TSA private key cannot be exported from the HSM.

In order to ensure continuity of service, the TSA stores the key pair in multiple highly realiable HSM devices on the primary and secondary site.

The TSA also creates a backup copy of the key pair on a protected removable media according to the HSM-related certified procedures.

The backup copy is stored at a safe site other than the site where the copy used for operations (within the HSM) is kept.

The time stamping private key is generated within the dedicated HSM and no backup or key recovery is allowed.

The key pair associated with the TSA certificate is safely stored only using backup methods certified by the HSM device manufacturer and have the same levels of security as the HSM itself.

The TSA generates its key pair inside the first HSM, which safely transfers the key to high reliability devices using the certified method of the HSM itself.

The key is transferred to the DR HSM via the certified backup and recovery procedure.

The TSA private key is stored within the HSM according to the HSM protection and cyphering methods.

Thee TSA private key is activated as soon as the HSM and the TSA are.

The TSA private key shall be disabled as soon as the HSM and the TSA service are.

Where required, the Certification Centre shall destroy the CA private key to ensure no residual data exists that permits rebuilding the key.

The certification centre uses the 'zeroization' function of the HSM and other adequate tools to ensure the complete destruction of TSA CA private keys.

6.3 Other aspects of key pair management

The TSA certificate is stored in a dedicated database to which adequate backup and preservation policies apply.

The TSA certificate and all issued certificates are stored in the Directory Server during the entire period of validity.

The operational lifecycle of a certificate ends as soon as it expires or is revoked.

The operational lifecycle of a key pair is not the same as the corresponding certificate, which is generated again every 3 months for security reasons.

The following table indicates the maximum duration of individual certificates:

Certificate	Certificate Lifecycle	Key Lifecycle
TSA Certificate	Up to 30 years	Up to 20 years
TSU Certificate	Up to 10 years	Up to 3 months
OCSP Certificate	Up to 5 years	Up to 5 years

6.4 Activation data

Activating a TSA HSM requires a certain number of keys and PINs that are only known to personnel in charge of the operational management of service, under the responsibility of the Certification Manager.

Activating a TSU HSM requires a certain number of keys and PINs that are only known to personnel in charge of the operational management of service, under the responsibility of the Certification Manager.

The data required to protect tokens and enable private key activation is generated during the Key Ceremony procedure consistently with the security specifications for HSM Certification. All information about keys distribution is recorded.

The data required to activate tokens and the key are stored in a reinforced rack that can only be opened by authorized personnel. Only authorised personnel can access the area where the rack is placed.

6.5 Computer security controls

The operational systems used by the TSA to manage certificates are applied proper security levels and controls and hardened regularly.

The operational systems are configured to require user identification by means of username and password. Alternatively, for more crucial systems, by smartcard/token and associated PIN.

Access is logged as defined in Section 5.4.

PKI Difesa shall ensure that management systems for software and Signature CA files are reliable and protected from unauthorised access. Moreover, the PKI Difesa shall limit access to server to authorised personnel only.

Regular users have no accounts on servers.

The PKI Difesa network is logically separated from the other networks. This separation only allows access as a result of the application processes running from within the network. The PKI Difesa uses a firewall system to protect the network from internal and external break-ins and limits the nature of sources that can access production systems.

PKI Difesa servers require passwords with a certain number of characters in length and a combination of alphanumeric and special characters.

Direct access to databases supporting PKI operations is only limited to trusted roles.

6.6 Life cycle technical controls

Within the PKI Difesa Infrastructure, development indicates the security of development environment and developers, the configuration management system during product maintenance, software engineering, software development methodologies, and premises.

The PKI Difesa is equipped to manage security and procedures so that operating systems and networks comply with configured security standards and policies.

These tools include integrity controls on software, hardware, and application flows with a view to ensure proper infrastructure operations.

6.7 Network security controls

The PKI Difesa comprises several security levels separated one from the other and from the Defence network by a high-quality firewalls system that filters connections as required.

TSA servers are located deep into the infrastructure to provide the highest levels of security.

All unnecessary communication ports on servers are disabled. Only the services supporting the protocols and functions required for the application to run shall be active.

6.8 Time-stamping

All processing systems used by the TSA are aligned to a time server synchronised with a GPS satellite network.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Certificates are consistent with ISO/IEC 9594-8:2005 [X.509] international standard and [RFC 5280] public specification.

PROFILE OF THE TSA CERTIFICATE

The profile of the TSA certificates is as follows:

FIELD	VALUE
Version	3
Serial Number	Variable, as per RFC 5280
Signature	Rsa Signature from CA as per RFC 5280
Issuer	Same as Subject
Validity	Variable, as stated in Section 6.3
Subject	As stated in Section 3.1
Subject Public Key Info	RSA public key (module and public exponent) as per RFC 5280.
EXTENSION	**VALUE**
Basic Constraints [Critical]	Subject Type=CA Path Length Constraint=0
Subject Key Identifier (SKI)	Variable and calculated as per 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

TIMESTAMPING UNIT (TSU)

The profile of Time Stamping Units is as follows:

FIELD	VALUE
Version	3
Serial Number	Variable, as per RFC 5280
Signature	Rsa Signature from CA as per RFC 5280

Issuer	Same as Subject of TSA, as stated in Section 3.1
Validity	Variable, as stated in Section 6.3
Subject	As stated in Section 3.1
Subject Public Key Info	Rsa public key (module and public exponent) as per RFC 5280.
EXTENSION	**VALUE**
Basic Constraints [Critical]	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier (AKI)	Same as SKI of TSA
Subject Key Identifier (SKI)	Variable and calculated as per 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 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

As stipulated in standard X.509, the Version field indicates the release number. Currently, release number is 3 (three).

Extensions contained in certificates are specified in Section 7.1.

Certificates are signed using the following algorithm:

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

Every type of certificate has an OID generated from within the PKI Difesa to identify its possible use. The same OID has been included in extension X.509v3 Certificate Policies. Possible values are indicated in Section 2.1.

The following is included in the Certificate Policies extension within certificates:

- OID of the relevant policy;
- URL to access the CPS/Operating Manual;
- in some cases, a User Notice text to specify details (e.g., for test certificates).

7.2 CRL profile

CRLs are consistent with ISO/IEC 9594-8:2005 [X.509] international standard and public specification RFC 5280.

Together with every CRL voice is the reasonCode extension to indicate the reason for suspension or revocation.

CRL	
Version	2
Issuer DN	Same as Subject of TSA, as stated in Section 3.1
Effective Date	Date of issue
Next Update	Deadline for a new CRL issuance
Revoked Certificates	List of revoked certificates. For every item, the following are specified: • Revoked certificate serial number, • Date and time of revocation, • ID code of reason for revocation
CRL Extensions	Extensions as per Section 7.2
CRL Signature Algorithm	Sha256withrsaencryption (1.2.840.113549.1.1.11) algorithm
CRL Signature	RSA Signature from CA as per RFC 5280

ESTENSION	VALUE
Authority Key Identifier	Same as SKI of CA
CRL Number	Issued CRL serial number

7.3 OCSP profile

The OCSP is compliant with public specification RFC 2560.

The characteristics of the profile for this certificate are as follows:

FIELD	VALUE
Version	3
Serial Number	Variable, as per RFC 5280
Signature	RSA Signature from TSA as per RFC 5280
Issuer	Same as Subject of TSA, as stated in Section 3.1
Validity	Variable, as stated in Section 6.3
Subject	As stated in Section 3.1
Subject Public Key Info	RSA public key (module and public exponent) as per RFC 5280.
EXTENSION	**VALUE**
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier (AKI)	Same as SKI of TSA
Subject Key Identifier (SKI)	Variable and calculated as per 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 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

Release number 1 (one) of OCSP specifications is supported as per RFC 2567.

Extensions contained in certificates are specified in Section 7.3.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

In order to receive (and maintain) the trust services operator qualification in accordance with Regulation EU No 910/2014 of the European Parliament and of the Council, every 24 months the Ministry of Defence will request a report to assess conformity to the requirements of the Regulation to be issued by a Certification Body (CAB – Conformity Assessment Body) accredited in accordance with Regulation (EC) 765/2008.

The Ministry of Defence shall also conduct periodic internal inspections.

8.1 Frequency or circumstances of assessment

External audits conducted by the CAB shall take place every 2 years (24 months).

Internal audits shall take place in accordance with a plan providing for different frequency (monthly and annual) for the different technical and operational aspects of the TSA service.

8.2 Identity/qualifications of assessor

External audits are performed by independent third parties that meet adequate standards in terms of organization and technology and have adequate audit skills.

Internal audits are conducted by personnel from the CA services governing body who have the appropriate audit qualifications.

8.3 Assessor's relationship to assessed entity

No relationship exists between external assessors and the certification centre that might influence the outcome of audits in favour of the Ministry of Defence.

The internal auditor of the Ministry of Defence is a Defence employee working within the Certification Centre who is therefore employed by the body responsible for the provision of the TSA service.

8.4 Topics covered by assessment

Audits conducted by external organizations aim at assessing compliance of CA services with reference international standards in the field from the technical and organizational viewpoints.

CAB audit follows guidelines based on EU Rule ETSI EN 319 401- "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

The internal audit is mainly aimed at assessing the integrity of the "audit log" and compliance with the operational procedures of the CA.

8.5 Actions taken as a result of deficiency

In case of deficiencies, Ag.ID requires the TSA to take the necessary corrective measures in a given period of time, on penalty of suspension or revocation of accreditation.

8.6 Communication of results

The results of any inspection or audit are reported to the nationally competent supervisory body (Ag.ID for Italy) to request for or maintain qualification.

Internal audit results shall be communicated to the certification centre and specific minutes shall be drawn up.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

PKI Difesa was made possible through an overall centralized investment; this service is offered free of charge to Ministry of Defence personnel for their institutional activities. Moreover, at the signing of the cooperation agreements, the ministries/public entities were required to share, in a manner proportionate to the number of issued ATe forms, in the costs borne by the Ministry of Defence for the operation of the Card Management System (CMS) and of the Public Infrastructure Key (PKI). The service is therefore offered free of charge also to the employees of other ministries that have entered a cooperation agreement with the Ministry of Defence

The Ministry of Defence is a government body that provides free of charge the service of cerficate issuance, management and renewal to its employees and to the employees of other ministries that have entered into a cooperation agreement with the Ministry of Defence.

For this reason, there are no costs for the following items:

- Certificate access
- Revocation or status information access
- Other PKI services

So there are no refund policies.

9.2 Financial responsibility

No insurance coverage is envisaged.

9.3 Confidentiality of business information

The Ministry of Defence, as the holder of the personal data collected during identification and registration of the subjects applying for certificates, undertakes to process these data with the utmost confidentiality and in compliance with Reg. (UE) 2016/679 (GDPR), also referred to as "Code on the Protection of Personal Data".

Where the identification and registration of users take place within a delegated structure (RA), the latter is qualified as “in charge of processing”.

The organization shall keep the following information confidential at all times:

- Disaster Recovery site activation plan;
- infrastructure addressing plan and network structure;
- Keys activation procedures and secrets (password, PIN, etc…);
- Transaction and audit logs.

The information contained in the certificate, the addressing modes to access the services of certificate status verification or CRL download are treated as non-confidential.

Information not included in this paragraph is treated as non-confidential.

This section is subject to the regulations in force.

PKI Difesa ensures confidentiality of information treated as confidential.

9.4 Privacy of personal information

Time stamping service data are not considered personal data.

The Defense PKI complies with Reg. (EU) 2016/679 (GDPR), on the subject of privacy management and protection of personal data.

Any information concerning the Subscriber which is not available on the public directory server is treated as private.

Under the national legislation any information publicly available through the certificate is not deemed private.

The PKI operators who obtain private information shall protect it against compromise and disclosure to third parties and shall comply with local legislation on privacy.

Unless otherwise indicated in this CP, in the privacy law or in agreements entered into between the Parties, private information shall not be used without the written consent of the data subject.

PKI Difesa has the right to disclose restricted/confidential information if it believes in good faith that disclosure is necessary pursuant to judicial, administrative or other proceedings during an administrative or civil trial, such as subpoenas, interrogatories, requests for admission and production of documents.

In particular:

- PKI Defense provides data, information, and documents to the Requesting Judicial Authority, excluding those covered by the State Secret.
- PKI Defense instructs the various access requests (in accordance with the internal procedure of the SMD, addressed by letter M_DSSMD REG2017 0056082 of 12-04-2017) in relation to the typology (*generalized* pursuant to Legislative Decree no. 33/13 and *documented* pursuant to Art.22 of Law No. 241/90), assessing the absolute and qualitative limitations in the first case (Article 5-bis of Legislative Decree No.33/2013) and those of exclusion from documents concerning national security and defense, international relations, public order, the prevention and suppression of crime, the safeguarding of the confidentiality of third parties, persons, groups and businesses (referred to in Presidential Decree No.352 / 92, Art.8 and related Art. 1048, 1049 and 1050 of Presidential Decree No. 90/10 - TUOM)

9.5 Intellectual property rights

This document is the property of the Ministry of Defence/Stato Maggiore della Difesa – Comando per le Operazioni in Rete which reserves all rights therein.

The document is drawn up and updated by the subordinate PKI Difesa Certification Centre.

As concerns the property of other data and information, the provisions in force in this area shall apply.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The CA remains committed to:

- comply with this CP and CPS;
- identify applicants as described in this CP and CPS;
- Issue and manage certificates as outlined in this CP and CPS;
- provide an effective service of certificate suspension or revocation;
- ensure that the holder possessed the paired private key upon issuance of the certificate;
- promptly report possible compromise of its private key;
- provide clear and comprehensive information on service procedures and requirements;
- Make a copy of this CP available to any applicant at his/her request;
- ensure that personal data are processed in compliance with current regulation;
- Provide an effective and reliable information service on the status of certificates.

9.6.2 RA representations and warranties

Not applicable since the RA and the very Certification Centre are the same body.

9.6.3 Subscriber representations and warranties

Not applicable since the holder and the very Certification Centre are the same body.

9.6.4 Relying party representations and warranties

Relying parties are both informed and, insofar as it falls within their responsibility, they expressly confirm that they have sufficient information to make a decision regardind the extent to which they elect to rely on the information contained in a certificate and are the sole responsible for deciding whether or not to rely on such information, thus becoming liable for their not being able to fulfill the obligations of a relying party as defined in this document.

9.6.5 Representations and warranties of other participants

All service providers that have an impact on the delivery of PKI services are controlled by the Ministry of Defense. The corresponding contracts are deposited at the Ministry of Defense and report the SLAs for intervention (eg for connectivity services, electricity supply, system assistance, air conditioning system).

9.7 Disclaimers of warranties

The TSA has no further obligations and offers no additional warranties than those expressly indicated in this CP or granted under the rules in force.

9.8 Limitations of liability

The TSA accepts no responsibility or liability whatsover for any damage to personnel arising out of the failure in receiving Signature CA communications due to a wrong e-mail address provided on application.

9.9 Indemnities

The Ministry of Defense does not foresee any indemnity in case of disservice.

9.10 Term and termination

This CP enters into force upon its publication (see chapter 2) and remains in force until it is replaced by a new version.

This CP remains in force until a new version is published.

Upon termination of this CP some provisions of the entire agreement may remain in force in recognition of intellectual property rights and of the provisions on confidentiality.

9.11 Individual notices and communications with participants

The certification centre notifies the certificate holder, via PKI Difesa electronic process in the signature software, that a new version of the signature software has been released.

The CA accepts notifications by the holder in the forms specified in paragraph 1.5.

9.12 Amendments

The Ministry of Defence reserves the right to amend this CP at any time. In case of amendments a new version of this CP shall be drawn up and published, giving appropriate notice.

An OIC should be replaced only when the general OID is reorganised for reasons the PKI Difesa has no control over.

9.13 Dispute resolution provisions

Any dispute shall be resolved in court.

9.14 Governing law

This CP is governed by, construed and enforced in accordance with the laws of Italy. For all matters not expressly covered in this CP, current regulations shall apply.

9.15 Compliance with applicable law

This CP is subject to existing national and international rules including, but not limited to, restrictions on export or import of software, hardware or technology.

9.16 Miscellaneous provisions

Should any clause or provision of this CP be deemed unenforceable by a competent judicial body, the remainder of the CP shall still apply.

PKI Defense may, due to reasons of interest to the Defense Administration, unilaterally terminate the collaboration agreement with other Public Administrations pursuant to Article 15 and Article 11, paragraphs 2 and 3 of Law No 241/90.

To the exent permitted by law, PKI Difesa is not liable for failure to perform the obligations set forth in this CP if such failure is the result of one or more events of force majeure.

Events of "force majeure" means war, acts of terrorism, natural disasters, electrical power outage, breakdown of the Internet network or in other facilities.

9.17 Other provisions

Document 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 use.

The aforementioned publication is salso a reference for the Public Administration bodies that have signed a service agreement with the Ministry of defence.