Italian Ministry of Defence

Public Key Infrastructure

Certificate Policy

Signature Certificates CA

-

CP – Certificate Policy

Author:	Italian Ministry of Defence
Versione:	1.8
Document date:	13 October 2022
No Doc.:	EN-CP–DS01

Certificate Policy

Signature Certificates CA

Validated by	Carmelo PERGOLIZZI	Systems Technical Operations Manager	*Firmato Digitalmente da/Signed by:* **CARMELO PERGOLIZZI** 1° Lgt. *In Data/On Date:* lunedì 17 ottobre 2022 09:03:42
	Gennaro GIANNINO	Chief Auditor	*Firmato Digitalmente da/Signed by:* **GENNARO GIANNINO** Lgt. *In Data/On Date:* lunedì 17 ottobre 2022 09:30:09
	Mirko Mancini	Security Manager	*Firmato Digitalmente da/Signed by:* **MIRKO MANCINI** *In Data/On Date:* martedì 18 ottobre 2022 14:02:56
	Andrea PERNA	Technical and Logistic Services Manager	*Firmato Digitalmente da/Signed by:* **ANDREA PERNA** *In Data/On Date:* giovedì 20 ottobre 2022 16:54:59
Approved by	Sergio Antonio SCALESE	Qualified Trust Services Provider (QTSP)	*Firmato Digitalmente da/Signed by:* **SERGIO ANTONIO SCALESE** *In Data/On Date:* mercoledì 26 ottobre 2022 08:25:48

Table of Contents

Versione	Sezione	Descrizione	Data
1.8	All	Replaced Security Manager	13 Octpber 2022
1.7	All	Addition Specify of O.I.D. Digital Seal	15 June 2022
1.6	All	Elettronic seal release operating mode indicated Replaced Security Manager	22 November 2021
1.5	Section 1.2 – Section 3.1 – Section 7.1	Addition of O.I.D. Digital Seal Replaced Security Manager Replaced Head of Technical and Logistic Services	06 April 2021
	Section 1.2, Section 1.6, Section 7.1	Added information about AgID OID for Certificate Policy (agIDcert)	
	Section 4.10, Section 6.3.2	Added information about certificate status beyond certificate expiration date	
1.4	All	The indication of the certifier's repository has been modified Added NOTE in paragraph 2.1 concerning the redirection in https of the URL www.pki.difesa.it Added descriptive NOTES in paragraphs 1.3.1 and 3.1 relating to the change of name of the Entity and the OU present in the CA certificate The contact points of the first level help desk have been updated	05 November 2020
1.3	Section 1.2	Added note on OID	24 June 2020
1.2	All	Change name department from"Comando C4" to "Comando COR"	9 March 2020

		Change abbreviation RP with FA Change ITD with OA	
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

1 INTRODUCTION

This paper describes the organization set up by the Ministry of Defence/Comando per le Operazioni in Rete in its capacity as trust services provider accredited to the Digital Italy Agency for issuing signature certificates.

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

A digital signature certificate is installed on a physical device called Mod. ATE (Carta Multiservizi della Difesa)[1]. A Mod. ATE comprises the digital certificates and the corresponding key pairs belonging to the holder.

A Mod. ATE is issued in compliance with Decree of the President of the Republic 851/1967, Decree of the President of the Council of Ministers of 24 May 2010 and Decree of the President of the Council of Ministers of 18 January 2016 and is valid as an electronic identity card (Mod. ATe).

For data enrolment purposes and in view of issuing digital signature certificates, the PKI Difesa uses the issuing system of the Modello ATe (Military ID) called Card Management System (Registration Authority-R.A.) and of the relevant local organizations pertaining to the single services (Local Registration Authority - L.R.A.).

1.1 Overview

This document is the Certificate Policy (CP) of the Ministry of Defence concerning the issuing and management of qualified, remote and automatic signature certificates.

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

This document illustrates the workings and operational procedures of the certification authority called "Ministry of Defence – Qualified Signature" whereby the Ministry of Defence issues and manages qualified signature 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

This CP by the eIDAS Signature CA is referred to, in signature certificates, with the following Object Identifier (OID): 1.3.6.1.4.1.14031.2.1.1.201.

The OID assigned to the Ministry of Defence is 1.3.6.1.4.1.14031.

The OID of the eIDAS Signature CA of the Ministry of Defence - Qualified Signature is 1.3.6.1.4.1.14031.2.1.1.

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

The following table shows both the OIDs of certificates handled by Digital Signatures of the Ministry of Defense accredited in Italy before 1 June 2016. Of the two CAs, the one called *"Ministero della Difesa - PKI di Firma Qualificata"* no longer issues certificates from July 2014 and only executes the lifecycle management of issued certificates (revocation/suspension/reactivation), while the current

[1] TN: a Defence ID card for both military and civilian personnel

CA named *"Ministero della Difesa - CA di Firma Digitale"* performs lifetime emissions and management.

Policy OIDs for certificates issued for holders derive from policies published by the ETSI within eIDAS regulations. See section 7.1 for details regarding relevant profiles.

Description	OID
Basic OID for the Ministry of Defence	1.3.6.1.4.1.14031
Basis for former old PKI Difesa (CPS)	1.3.6.1.4.1.14031.**1**
Policy of the former PKI Difesa as defined in www.pki.difesa.it/firmadigitale.pdf	1.3.6.1.4.1.14031.1.**1**
Basis for the new PKI Difesa (CPS)	1.3.6.1.4.1.14031.**2**
Policy of the new PKI Difesa as defined in www.pki.difesa.it/ManualeOperativoDifesa.pdf	1.3.6.1.4.1.14031.2.**1**
OID of the Signature CA certificate	1.3.6.1.4.1.14031.2.1.**1**
OID of the OCSP certificate for the Signature CA	1.3.6.1.4.1.14031.2.1.1.**1**
OID of the User's signature certificate with no usage limitation	1.3.6.1.4.1.14031.2.1.1.**2**
OID of User's signature certificate with usage limitation [2]	1.3.6.1.4.1.14031.2.1.1.**3**
OID of Test Remote Signature certificate	1.3.6.1.4.1.14031.2.1.1.**4**
OID of Remote Signature certificate	1.3.6.1.4.1.14031.2.1.1.**5**
OID of Users' Signature certificate for testing purposes	1.3.6.1.4.1.14031.2.1.1.**6**
OID of the Automatic (Remote) Signature certificate	1.3.6.1.4.1.14031.2.1.1.**8**
Policy of the new eIDAS PKI as defined in https://pki.difesa.it/tsp	1.3.6.1.4.1.14031.2.**1**
OID of CPS for eIDAS signature service in Italian	1.3.6.1.4.1.14031.2.1.1.**100**
OID of CP for eIDAS signature service in Italian	1.3.6.1.4.1.14031.2.1.1.**101**
OID of the Terms and Condition document for the eIDAS signature service in Italian	1.3.6.1.4.1.14031.2.1.1.**102**
OID of the PKI Disclosure Statement for the eIDAS signature service in Italian and English	1.3.6.1.4.1.14031.2.1.1.**103**
OID of CPS for eIDAS signature service in English	1.3.6.1.4.1.14031.2.1.1.**200**
OID of CP for eIDAS signature service in English	1.3.6.1.4.1.14031.2.1.1.**201**
OID of the Terms and Condition document for the eIDAS signature service in English	1.3.6.1.4.1.14031.2.1.1.**202**
OID of the eIDAS Signature User's certificate with no usage limitation	1.3.6.1.4.1.14031.2.1.1.**12**
OID of the eIDAS signature certificate with usage limitation [3]	1.3.6.1.4.1.14031.2.1.1.**13**
OID of the Remote eIDAS Signature certificate for testing Purposes	1.3.6.1.4.1.14031.2.1.1.**14**
OID of the Remote Signature certificate	1.3.6.1.4.1.14031.2.1.1.**15**

[2] It should be noted that up to 30 June 2017, OID 1.3.6.1.4.1.14021.2.1.1.3 has been used

[3] It should be noted that from 1st July 2017 to 22 June 2020, OID 1.3.6.1.4.1.14021.2.1.1.13 has been used

Description	OID
OID of Users' eIDAS Signature certificate for testing Purposes	1.3.6.1.4.1.14031.2.1.1.**16**
OID of the Automatic (S.G.D.) eIDAS Signature certificate	1.3.6.1.4.1.14031.2.1.1.**18**
OID of the Automatic (S.M.D. COR) eIDAS Signature certificate	1.3.6.1.4.1.14031.2.1.1.**19**
OID of the certificate of Digital Seal eIDAS	1.3.6.1.4.1.14031.2.1.1.**23**
OID of the certificate of Digital Seal AUTOREMOTE eIDAS	1.3.6.1.4.1.14031.2.1.1.**28**

In compliance with recommendations contained in [AGID_LG11] section 4, i.e. "Linee guida contenente le Regole Tecniche e Raccomandazioni...", starting from December 2019, the QTSP is inserting the attribute CertificatePolicies (OID 2.5.29.32) a further PolicyIdentifier element with value **agIDcert** (OID **1.3.76.16.6**), which represents "*When included into a Rec. ITU-T X.509 electronic certificate, it means that all the recommendations issued by the Agency for Digital Italy are fulfilled*".

1.3 PKI participants

This section provides introductory information regarding Certification Authorities and relying parties of the PKI Difesa.

1.3.1 Certification authorities

The Certification Authority is the third, and reliable, party that issues certificates and signs them with its own private key (CA key). The CA designated to issue signature certificates and manage certificate status is called signature CA.

Within this service, the capacity of Signature CA is performed by the Minister of Defence/Stato Maggiore 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 a Trust Services Provider for Defence.

The Certification Authority is a Root-CA that directly issues certificates for holders, 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 organization that:

- Accepts and validates issuance requests, and manages certificates;
- Registrates the applicant and the organization he/she belongs to;
- Authorizes the CA to issue the required digital certificate;
- Provides personnel with the digital certificate and the information required.

This activity is carried out for digital signature certificates comprised in the Modello ATe (Military ID)/Mod. ATE by the Local Registration Authority (LRA) and by the Card Management System (CMS) of the Ministry of Defence.

For automatic signature certificates the Defence Computer Protocol System Manager operates as RA.

For remote signature certificates, the PKI Difesa Certification Centre directly carries out RA tasks.

1.3.3 Subscribers

All Defence personnel and personnel of public administration bodies that have signed a cooperation agreement. For activities, directly or indirectly pertaining to the digital signature services defined in this document, Defence has provided its own employees with a digital signature in view of the job performed within the activities provided for in this document.

End users, namely certificate subscribers will be physical persons who require a certificate and who hold the corresponding private key.

1.3.4 Relying parties

Relying parties are all subjects relying on information comprised in the certificate to validate the documents signed by holders.

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 amongts those (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.

The following profiles are also involved in the certification process:

- Local Manager, a professional profile employed in the organization that requires the qualified certificates to be issued for the Holder.

- Data Processing Operator, a professional profile employed in the organization that supports the prospective certificate holder in submitting the data required for the certificates to be issued. He/she is in charge of identifying correctly the prospective holder.

- User (any real or immaterial organization that uses a qualified certificate to check the validity of the digital signature or authentication.

1.4 Certificate usage

The CA of the Ministry of Defence – eIDAS Digital Signature CA uses its key pair to:

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

The holder of the restricted usage signature certificate comprised in the Modello ATe (Military ID)/Mod. ATE and remote signature HSM uses its key pair to:

- Sign a digital document in the formats provided for by current regulations in compliance with usage limitations defined in the certificate itself.

The holder of the unrestricted usage signature certificate comprised in the Modello ATe (Military ID)/Mod. ATE and remote signature HSM uses its key pair to:

- Sign a digital document in the formats provided for by current regulations.

The holder of the automatic signature certificate in the automatic signature HSM uses its key pair to:

- Sign the inception of an IT process within his/her work context.

The OCSP certificate of the Qualified Signature CA is used to:

- Sign the answers to audit requests regarding the validity status of a signature certificate.

Anything other than usage defined in paragraph 1.4 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 made known.

1.5 Policy administration

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 the 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.

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
- Via the following link: https://servidesk.difesa.it
- The following email address helpdesk@cor.difesa.it
- +39-06-46914444, for the Comando 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 System Technical Operation Manager, the auditing manager, the security manager, the logistic and technical system manager. It was approved by the Comando per le Operazioni in Rete Headquarters Commander as trust services provider for Defence.

1.6 Definitions and acronyms

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

Term/Acronym	Description	Definition
AgID	Digital Italy Agency (formerly run by DigitPA) CA certification	Italian supervisory body
CA	Certification Authority	Body that issues the certficates
CMD	Carta Multiservizi Difesa	A smartcard that Defence personnel is provided with as a valid electronic ID that also contains the holder's certificates
CMS	Card Management System	The system issues ATe models for Defence personnel and for personnel belonging to public adminitration bodies that have signed a cooperation agreement with Defence.
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	A document that explains the practices and operational processes of the CA whereby the Ministry of Defence issues and manages qualified signature certificates.
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 government 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
LRA	Local Registration Authority	Local body in charge of enrollment procedures. It identifies and validates the subject requesting a certificate
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 the 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 secret element of asymmetric cryptography based on key pairs
RA	Registration Authority	Body in charge of enrolment procedures. It identifies and authenticates the subject requesting a certificate
Data Processing Operator	Data Processing Operator	Data Processing Operator, a professional profile employed in the body that supports the prospective certificate holder in submitting the data required for the certificates to be issued. He/she is in charge of identifying correctly the prospective holder.

Term/Acronym	Description	Definition
Local Manager	Local Manager	A professional profile of the body that requests qualified certificates for the Holder
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 (former Certifier)
TSR	Time Stamp Response	A structure comprising a Time Stamp Token and the response received by the corresponding Time Stamp Unit
TST	Time Stamp Token	Time Stamping links definite and legally valid date and time to a digital document
TSU	Time Stamping Unit	A software service that has a time stamping certificate and issues time stampings by signing them digitally with the relevant certificate

REFERENCES

[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 Profile for Certificates issued to Natural Persons » Mar 2014

[ETSI 862] ETSI TS 101 862 v.1.3.3 – "Qualified Certificate profile", Jan 2006.
[ETSI 412] ETSI EN 319 412 v.1.1.3 – "Electronic Signatures and Infrastructures (ESI) ; Certificate Profiles ; Part 3 : Certificate Profile for certificates issued to legal persons" Apr. 2020.

[RFC2560]"Online Certificate Status Protocal - OCSP", (http://www.ietf.org/rfc/rfc2560.txt)
[RFC3647]"Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", (http://www.ietf.org/rfc/rfc3647.txt)

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

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

This chapter comprises provisions concerning the identification of the subject or authority that manages the repository within the PKI Difesa, the accountability of published information and frequency of publication.

"Repository" means a range of archives and on-line logs comprising information of public interest concerning 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…)

- ldap://ldappkiff.difesa.it Directory Server – repository where issued certificates and current CRLs are published. This repository is only reacheable internally from the Defence network and from P.A. bodies that have signed a cooperation agreement with the Ministry of Defence.

The Certification centre is in charge of managing both repositories.

The Certification Authority mantains and manages a repository of its own that is located within the PKI Difesa and protected against external access by means of firewalls and anti-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 www.pki.difesa.it and on https://pki.difesa.it/tsp:

- Certification Practice Statement (CPS)
- Certificate Policy (CP)
- Terms and Conditions (T&C);
- PKI Disclosure Statement (PDS);
- Software for using Modello ATe (CMD API);
- Software for using the Digital Signature (Signature kit);
- The Revocation Lists (CRLs)
- CA certificates

The above web sites are available 24 hours on 24 and 7 days on 7.

Furthermore, the CA published the issued certificates and the CRL in force 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 (www.pki.difesa.it) 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-autorized 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 Online Certificate Status Protocol (OCSP) can be freely accessed at http://ocsppkiff.difesa.it

3 IDENTIFICATION AND AUTHENTICATION (I&A)

This chapter describes the procedures used by the Signature CA 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

Certificates issued by PKI Difesa comply with the X.509v3 standard.

As regards certificates, in the Alternative Subject Name field, the certificate holder's email is indicated as "RFC822 Name".

The details as regards contents are the following:

Signature CA	
Common Name(CN)	Ministero della Difesa – CA di Firma Digitale
SERIALNUMBER	97355240587
Organizational Unit (O)	S.M.D. – C.do C4 Difesa
Organization:	Ministero della Difesa
Country Code (C)	IT

Signature Certificate - Remote / Automatic Signature of SGD	
dnQualifier	ID Carta - ID Ente + Nr progressivo
Common Name (CN)	NOME COGNOME
serialNumber	TINIT-CODICEFISCALE
GN	NOME
SN	COGNOME
Organizational Unit (OU)	NomeUnitàOrganizzativa
Organization (O)	NomeOrganizzazione/CodiceFiscaleOrganizzazione
Country Code (C)	IT

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

Signature Certificate with Digital Seal of S.M.D./COR	
dnQualifier	ID + Nr Univoco Ente
Common Name (CN)	Comando/Ente (AOO)
2.5.4.97 (Organization Identifier)	Codice IPA Ente
Organizational Unit (OU)	IPAIT-AOO_*CODICEAOO* (Codice della AOO secondo IPA)
Organization (O)	NomeOrganizzazione
Country Code (C)	IT

Signature Certificate with Digital Seal on Smart Card	
dnQualifier	ID + Nr Univoco Ente
Common Name (CN)	Comando/Ente (AOO)
2.5.4.97 (Organization Identifier)	Codice IPA Ente
Organization (O)	NomeOrganizzazione
Country Code (C)	IT

Certificates of holders and of signature CA have names with intelligible meanings allowing holders' and signature CA's identity to be determined.

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

Holders' certificates are issued by physical persons. A certificate will comprise a person's data without pseudonyms.

The certificate holder's mail is defined as value RFC822 in the field related to Subject's Alternative Name in the signature certificates that are comprised in the Modello ATe.

The Distinguished Name fields and their contents follow the specifications of the digital signature in Italy, in particular the AgID Determination no. 121/2019 (which replaced CNIPA Resolution 45/2009).

The combination of Distinguished Name fields listed in 3.1 identifies uniquely the name of a single holder thanks to the dnQualifier component, which varies every time a certificate is issued for the same holder.

For signature certificates comprised in Modello ATe uniqueness is provided through the dnQualifier that corresponds to the card ID (i.e. MMDA12345).

For automatic signature certificates, the certificate is uniquely associated with the value of the dnQualiier which is of the form XXXnnnnnn (Entity identification + progressive number). Since the dnQualifier is unique for each self-signed certificate holder, he cannot have more than one active self-signed certificate.

For digital seal certificates, the certificate is uniquely associated with the value of the dnQualiier which is of the form XXXnnnnnn (Entity identification + progressive number). Since the dnQualifier is unique for each digital seal certificate holder, he cannot have more than one certificate.

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

3.2 Initial identity validation

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

The Holder registration process relies on an IT procedure.

SIGNATURE ON MODELLO ATe

Shown below the enrolment options for personnel belonging to Defence and public administration bodies that have signed a cooperation agreement with Defence for issuing the Modello ATe and the certificates included in the card.

The Data Processing Operator collects data to issue the Modello ATe after the person concerned has submitted the following documents:

- A valid ID document;
- a Modello ATe request form, along with the relevant information notice, adequately filled in and signed.

The Data Processing Operator performs the following operations:

- enrol data through specific procedures;
- through its own qualified signatures, he/she validates the data that has been collected and signed by the person concerned by means of a graphometric signature.

The data enrolment procedure (enrollment) is carried out at the Local Registration Centres (LRA) and only starts following a paper request that must be adequately filled in, include the relevant information note, and be signed by the Executive in charge.

Once the data collection procedure is over, the applicant signs the data with a graphometic signature and the Data Processing Operator validates the procedure with his/her qualified signature with the signature certificate in his/her Modello ATe.

Once the capturing procedure is complete, the Local Manager of the LRA validates the data by means of a specific IT procedure through his/her qualified signature and sends the data to the CMS.

Before starting the printing process, the CMS Operator verifies once again the visual quality of the captured data.

The CMS checks the data and asks the signature CA to issue the certificates during the personalization process of the Modello ATe.

Data Processing Operators, Local Managers and CMS operators are appointed by directors in charge through a formal act. They can exclusively operate after performing a strong authentication operation by means of their Modello ATe.

AUTOMATIC SIGNATURE

The identification procedure for issuing automatic signature certificates used in registering systems is as follows:

The applicant, who is appointed by a specific document, fills in the request form, signs it with the signature certificate in his/her Mod. ATE and sends it to the Defence Computer Protocol System Manager. The manager validates the request by countersigning it with the signature certificate in his/her own Mod. ATE.

All certificate request forms comprise at least the following information:

- Name and Surname
- Tax code
- Institutional mail of the defense domain;
- AOO of belonging

AUTOMATIC SIGNATURE / DIGITAL DEFENSE SEAL SMD / COR

For the issue of the automatic signature certificate / digital seal of the Defense, the Holder fills out a preformatted PDF form containing the data relating to the request and the information that will be included in the certificate (e.g. Surname, Name, Tax Code for Signature Automatic while for the Seal descriptive name, organization, AOO, ETC ...) The holder digitally signs the PDF form with his ATE model (the signature certificate is issued by the TSP itself) in PadES format and sends it to the TSP.

Upon receipt of the form, the TSP operator checks the form received with the aid of IT tools in terms of validity of the signature, presence of mandatory data, correctness of internal data.

Once this check is completed, the system automatically creates the user on the signature appliance (HSM) generating the secrets randomly, starts the generation of the private key on the appliance, obtains the certificate request (CSR), submits it to Certification Authority obtaining the certificate that will be written on the HSM.

If successful, therefore, the system creates a PDF digital blank envelope containing the secrets and encrypts this envelope using as the recipient certificate the one corresponding to the user who signed the request form (the certificate is automatically retrieved from the LDAP directory of the TSP).

Finally, the system sends an email to the owner with the notification of the issuance of the requested service and the encrypted digital blank envelope is attached. In this way, only the holder can view the contents of the envelope after decrypting them with their Ate model (cipher certificate) using the Signature Kit software application.

REMOTE SIGNATURE

The user requesting a remote signature certificate sends the certificate request adequately completed and signed with the signature certificate in his/her Modello ATe to the Certification Centre.

For a remote signature certificate to be issued, the certification centre operator receives the certificate request form signed with the applicant’s signature certificate in the Modello ATe and checks it accuracy.

By means of a specific IT process, the operator generates the user within the Remote Signature HSM and informs the user that the operation has been performed.

COMMON CONSIDERATIONS FOR EVERY CERTIFICATE TYPE

The proof of possession by the applicant of the private key corresponding to the requested certificate is based on the cryptographic verification of the CSR (Certificate Signing Request) sent to the Signature CA.

The CMS or the single point of contact for the IT protocol for the CEO o the applicant via the remote signature portal, depending on the type of certificate issue, sends the public key to the Signature CA in the form of CSR in PKCS # 10 format [RFC2314].

Only registered entities (CMS, remote signature portal, single point of contact for the IT protocol for the CEO) can request the issuance of the certificate through a reliable delivery of the certificate request itself.

Each of these entities is equipped with a particular signature certificate with which it countersigns the certificate requests (CSR) which are then submitted to the Registration Authority of the Signature CA. The RA, after checking the integrity of the request, verifies the authorization of the certificate used and, if valid, submits the original CSR request to the Signature CA.

Requests for certificates coming directly from individuals outside the Ministry of Defense and PAs who have entered into a collaboration agreement with Defense are not accepted.

The certificates issued do not contain information that cannot be verified. All the data reported in the certificates issued are verified and signed by the Holder during the acquisition phase.

The applicant is criminally responsible for the correctness of the data signed at the time of the acquisition procedure, pursuant to Presidential Decree 445/2000, Article 76.

The Signature CA does not validate 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

Not applicable since the the signature certificates in the Modello ATe expire when the Modello ATe does. When the Modello ATe expires, a new Mod. ATE is issued with new certificates through the same proccess described in section 3.2.

3.4 Identification and authentication for revocation request

The identification and authentication method for suspension or revocation requests depends on the certificate type.

SIGNATURE ON MODELLO ATE

Qualified signature certificate in the Modello ATe:

- Suspension: the holder's identification and authorization relies on verification of the corresponding emergency code in case the operation is performed in self or aided mode, or by ID validation if the operation is performed at an LRA.
- Revocation: the holder’s identification and authorization are always performed at a LRA by verifying the Holder’s ID. In case this been stolen/lost, the relevant statement to competent authorities shall be verified.

All operators authorized to suspend and/or revoke certificates are identified through a strong authentication process by means of a Modello ATe.

Certificates comprised in the Modello ATe also require identification of the Modello ATe. In case of long-term revocation or suspension, the card must be returned. In case the card is stolen or lost, a statement must be submitted to the competent authorities.

REMOTE SIGNATURE

The user requesting a remote signature certificate sends the revocation request adequately completed and signed with the signature certificate in his/her Modello ATe to the Certification Centre, which revokes the certificate.

For remote signature certificates, the form must also include the RSA OTP Token identification number.

AUTOMATIC SIGNATURE OF SGD

For the automatic signature certificate, the Certificate Holder sends the revocation / suspension request form duly completed and signed with the signature certificate on the AT form to the sole contact person for the IT protocol for the A.D. which countersigns the request and sends it to the Certification Center which proceeds to revoke the certificate.

Revocation of an automatic signature certificate or digital seal may be directly requested to the Defence Computer Protocol System Manager, and signed by the manager only, under the circumstances specified in the form.

A request to suspend/revoke a certificate includes at least the following information:

- Name and Surname
- Tax code
- Justification

AUTOMATIC SIGNATURE / DEFENSE SEAL SMD/COR

For automatic signature and defense seal certificates, the Certificate Holder sends the revocation / suspension request form duly completed and signed with the signature certificate present on the ATe form to the Certification Center which proceeds to revoke the certificate.

The certificate suspension / revocation request includes at least the following information:

- Surname and Name;
- Tax Code;
- Motivation.

SMD/COR DEFENSE SEAL ON SMART CARD

The electronic seal certificate on Smart Card can be requested by the Public Administration. who have signed a collaboration agreement with the Ministry of Defense, this certificate is required only and exclusively for proving the organizational needs of the Public Administration. and is issued directly by the Certification Center to the requesting Holder.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

A signature certificate request can be submitted to the Signature CA:

- By the CMS, following authorization by the Local Manager for signature certificates in the Modello ATe.
- By the operator in the Certification Centre following approval by the Defence Computer Protocol System Manager, when automatic signature certificates are concerned;
- By the user who requests it, upon approval by the Certification Centre, when remote signature certificates are concerned.

For a certificate to be issued, the procedures described in paragraph 3.2 must be followed.

During the identification and authentication process, the applicant is legally liable for his/her declarations, while the various operators are liable for verifying the accuracy and thoroughness of the data provided by the user as per the Presidential Decree n.445/2000 Art.76.

4.2 Certificate application processing

SIGNATURE ON MODELLO ATE

The Data Processing Operator and the Local Manager approve the request for a Mod. ATE and signature certificate only if the data provided by the applicant has been succesfully identified and validated.

The rejection and/or approval for issuing a Mod. ATE and the relevant signature certificate may depend on the:

- Data Processing Operator verifying the accuracy and thoroughness of data provided by the user.
- Local Manager of the LRA who, on the basis of the verification of data collected by the Data Processing Operator, can decide whether to approve or reject a Mod. ATE request.
- CMS Operator who, prior to the issuance of the modello ATe, further checks data to verify the correspondence of the applicant's photo captured by the ITD and validated by the RT in compliance with established standards.

AUTOMATIC SIGNATURE OF SGD

The Defence Computer Protocol System Manager approves the request for automatic signature certificates only if the data provided by the applicant has been succesfully identified and validated.

For automatic signature certificates, approval or rejection depends on verification of the applicant’s data which is carried out by the Defence Computer Protocol System Manager first and by the operator of the Certification Centre of the operator later.

AUTOMATIC SIGNATURE / DIGITAL DEFENSE SEAL SMD/COR

For Defense automatic signature / digital seal certificates, the Head of Certification Center approves the request for issuing the automatic signature / digital seal certificate if successful identification and authentication of all data provided by the requesting user.

REMOTE SIGNATURE

For remote signature certificates, the Certification Centre Manager approves the request for a remote signature certificate if the data provided by the applicant has been succesfully identified and validated.

For signature certificates, the approval or rejection of a certificate request directly depends on the Chief of the Certification Centre who can decide either to approve or reject the request once he/she has verified the accuracy of data provided by the applicant.

COMMON CONSIDERATIONS FOR EVERY CERTIFICATE TYPE

The Signature CA 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.

Although there is no set timescale, requests are processed within reasonable time limits.

For specific service requirements, requests may be approved by urgent procedure. However, such procedures do not alter the processes described in this document, but only affect queue management in terms of priority.

4.3 Certificate issuance

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

A signature certificate enclosed in a Mod. ATE is generated and issued as soon as the CMS submits a CSR in the PKCS#10 format to the Signature CA.

Remote signature certificates are generated and issued by the Signature CA as soon as the applicant completes the issuing procedure through the remote signature portal.

Automatic signature certificates and digital seal are issued as soon the Operator of the Certification Centre has completed the preliminary procedures to submit a request and has submitted the CSR in the PKCS#10 format to the Signature CA.

The CMS notifies the applicant that the Modello ATe has been issued along with the enclosed certificates by emailing a specific visualization code to the person concerned. The code can only be used once and is required for delivering a card, as well as recovering PIN and PUK codes to use the card and the certificates.

Users are notified that remote signature certificates have been issued through the remote signature portal as soon as the generating procedure is completed.

For automatic signature certificates, the Certification Center communicates the successful generation of the certificate to the single point of contact of the IT protocol for the A.D. who is responsible for notifying the Holder, for generating the certificate.

For certificates of automatic signature / digital seal of the SMD / COR Defense, the Certification Center communicates the successful generation of the certificate and the activation of the requested service to the holder by means of an encrypted email.
The aforementioned email is generated automatically by the system.

4.4 Certificate acceptance

When the card is delivered to the holder at the LRA, the holder accepts the certificates and ackowledges such acceptance through graphometric signature.

For automatic signature and / or remote signature certificates, the certificate is considered accepted by the Holder if they are not highlighted by the sole contact person of the IT protocol for the A.D. or / and by the Owner himself of the errors in the certificate data within a reasonable time.

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

Issuance of the signature certificate comprised in the Modello ATe, and of the remote signature certificate, is notified to the certificate holder only. Issuance of the signature certificate is notified via mail while issuance of the remote signature certificate is notified through the remote signature portal.

The issuance of the automatic signature certificate is communicated via email to the sole contact person for the IT protocol for the A.D. which in turn, having completed the IT procedures for uploading the certificate within the HSM, forwards the communication to the holder of the certificate.

For SMD/COR Defense automatic signature / digital seal certificates, the certificate is considered accepted by the Holder if errors in the certificate data are not highlighted by the Holder himself within a reasonable time.

4.5 Key pair and certificate usage

Using a private key corresponding to a public key is only allowed after the Holder has accepted the Certificate Policy and the certificate.

The certificate must be used in compliance with the regulations and terms specificied in the CP and CPS. The subscriber uses the key pair and the certificate to sign digital documents.

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 extension of the certificate itself (i.e. if the value of the extension differs from "Non-Repudiation", the certificate cannot be used for the signature).
- The status of certificate through CRL/OCSP and the status of the issuing Signature CA 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 Signature CA.

4.6 Certificate renewal

At present, no signature certificate can be renewed.

The signature certificate in the Modello ATe expires when the Modello ATe does. Upon expiration, the Holder shall ask for a new card and a new certificate to be issued.

Upon expiration, new remote and automatic signature certificates and digital seal will be issued and usage of previous ones will be inhibited.

4.7 Certificate re-key

Not allowed for the reasons specified in 4.6 and 3.3.

If the end user (Holder) decides to use a new key, he/she must necessarily request a new certificate and a new Modello ATe to replace the current one.

A new key pair is generated for each new signature certificate through the same key and certificate generation process described in 4.1, 4.2, and 4.4.

4.8 Certificate modification

Being signed by an issuing CA, a certificate cannot be "modified". Therefore, to amend errors in generating the certificate it is necessary, for security reasons, to revoke the wrong certificate and 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:

- Suspected compromise;
- in case the card is stolen or lost;
- when the chip is not working or the Modello ATe has been damaged;
- for erroneous data in the certificate;
- for termination of employment (layoff, discharge, retirement, death);
- for loss of certificate usage credentials as regards automatic and remote signature certificate.

4.9.2 Who can request revocation

Revocation can be requested by the:

- Certificate holder;
- Local Manager or CMS in case of alleged inappropriate certificate usage;
- Certification Centre;
- Person in charge of the Defence Computer Protocol System;

4.9.3 Procedure for revocation request

SIGNATURE ON MODELLO ATE

In case the card is stolen or lost, as a first thing the certificate holder requests emergency suspension through the portal and by providing the tax code and the emergency code.

If the holder cannot access to the portal, the holder contact the call center and asks for the suspension after he/she is identified through a set of questions on his/her personal data and a part of the Emergency Code.

If also this is not possible, he/she contacts his/her LRA and request for the suspension of the certificate to the Data Processing Operator; the Data Processing Operator then gives response to the request.

The suspension is transformed in a revocation request after the denunciation of theft and/or loss is produced to the Data Processing Operator; the Data Processing Operator identifies the requesting user through a valid ID document and collect the needed data.

The Local Manager validates the revocation request then sending the data to the CMS, where the operator executes the revocation.

In case of card or chip deterioration, the revocation request is directly performed at the LRA. The Data Processing Operator insert the required data, signs them and send them to the Local Manager; the Local Manager valides data for the sending to the CMS, where an authorized operator executes the revocation.

In every case, a suspension is transformed in a revocation after 15 days from the suspension date and the need of reactivate the certificate has not been manifested. This procedure doesn't apply to long term suspended certificates.

The revocation "ex officio" is directly executed from the CMS operator or from the PKI Difesa in the cases expected from SMD-I-009.

REMOTE AND AUTOMATIC SIGNATURE AND DIGITAL SEAL

For remote and / or automatic signature certificates, the Certificate Holder requests the revocation of the certificate by filling in and signing the appropriate form.

The form for the revocation of the remote signature certificates is sent to the Certification Center while the one for the automatic signature and digital seal certificates is first sent to the single contact person for the IT protocol for the A.D. who countersigns it and forwards it to the Certification Center.

The single point of contact for the IT protocol for the CEO may directly request the revocation of a third-party automatic signature certificate due to cessation of activity or incorrect data.

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 issued at least once a day and is valid for 7 days.

If the card is damaged, 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 users having an application that performs the checking process in accordance with the RFC 2560.

4.9.8 Other forms of revocation advertisements available

Upon revocation, the holder is notified by email.

4.9.9 Circumstances for suspension

A signature certificate is suspended as a precautionary measure in case a card has been allegedly stolen or lost.

Moreover, a certificate may be suspended for specific service requirements:

- Personnel who are held in custody;
- Personnel who have been temporarily suspended from work;
- Any other reason that may lead to inappropriate card usage.

In case suspension evolves into a definite revocation, its effective date is the same as the suspension date.

4.9.10 Who can request suspension

The request to suspend a signature certificate is submitted by the holder:

- to any Local Registration Authority (LRA) or via WEB or by telephone for a signature certificate comprised in the Modello ATe;
- to the Defence Computer Protocol System Manager as regards automatic signature certificates;
- directly to the Certification Centre as regards remote signature certificates.
- for certificates of automatic signature and digital seal of the SMD/COR Defense directly to the Certification Center.

The LRA manager or the Defence Computer Protocol System Manager, as well as the CMS can take direct action to suspend a certificate for justifiable reasons. The operation is immediately notified to the holder along with its justification.

4.9.11 Procedures for suspension request

Procedures to request standard suspension are the same as those for revocation described in 4.9.3.

For specific service requirements, the CMS may perform long-term suspension for Mod. ATE holders.

After 15 days, suspension is changed into revocation starting from the suspension date.

Conversely, long-term suspension has no time limit and depends on the organization's requirements.

4.10 Certificate status services

The PKI Difesa 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 signature CA also provides an OCSP service (On-line Certificate Status Provider) in accordance with the specific [RFC2560].

The certificate status service keeps track of certificate status even after they expire. In particular, as regards the CRL, this is done by extending the CRL as specified in section 7.2.

The certificate status service keeps track of certificate status even after they expire. In particular, as regards the CRL, this is done by extending the CRL as specified in section 7.2.2.

The information of the revocation status in the CRLs is renewed at least on a daily basis while on the OCSP it occurs in real time.

In case of CA compromise, the QTSP will publish on its website the last CRL issued before the ascertained compromise, including the relative emission data. At the same time, a new CRL will be issued with an expiration date extended to the expiration date of the CAs. The two CRLs will be made available for a period of 20 from the CA's expiration date.

In the event of termination of the QTSP service, the OCSP service will not be kept alive while a single extended CRL will be issued with an expiration date equal to that of the CA itself. This CRL will be published on the certifier's website and provided to AgiD for legal retention.

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;
- By 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 a new suspension, renewal or revocation due to serious causes.

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. 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.

4.11 End of subscription

The signature certificate is issued only to the employees of the Ministry of Defence and other organisations of the Public Administration that have subscribed a cooperation agreement with the Ministry of Defence. It is contained in the Modello Ate, which is also the civil civil/military personnel ID card, as per the regulations in force.

The service agreement with employees expires as soon as an employee loses the status of defence civil/military personnel.

The remote, automatic and seal signature certificates are issued only to employees of the Defense and the Authorities / Public Administration. who have signed a collaboration agreement that need these types of certificates.

Similarly, to the certificates included in the Modello ATe, the service agreement expires as soon as an employee is no longer on active duty.

4.12 Key escrow and recovery

No Key Escrow or Key Recovery are included in signature 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 Signature CA will maintain a backup copy of the 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 defense structures (surrounding walls or perimeter access gates controlled remotely, armored doors), elements of active defense (armed surveillance service) and application components such as systems based on cryptographic tokens and personal codes or knowledge of login username and password.

The integrity of equipment and systems is constantly maintained and checked, in accordance with current regulatory provisions in order to avoid failures that may cause interruption to the continuous operation of the services.

The structure where the primary site of the PKI Difesa infrastructure is located is the Command for Network Operations in via Stresa n. 31b, 00135 Rome.

The Disaster Recovery site of the PKI Difesa infrastructure is located at the CED of the Ciarpaglini barracks - Command C4 Army located in via Guido Reni n. 22, 00196 Rome.

Physical access to the building and internal rooms is allowed only to authorized personnel. Guests must be previously authorized and registered before accessing them and must be accompanied by qualified personnel.

Access to the data center of the primary site is allowed only to authorized personnel after authentication using the ATe form.

The PKI Difesa infrastructure is kept inside Racks located in the Command Data Center. Access to the Data Center is allowed only to authorized personnel by electronic identification with Mod. ATe. Access to the PKI Infrastructure racks is allowed only to the personnel of the Certification Center by means of exclusive electronic keys.

Access to the PKI Difesa DR structure is protected by burglar-proof doors, accessible only with the prior authorization of the surveillance staff.

The premises are equipped with an air conditioning system and the electrical system is protected from voltage drops by a UPS system and a generator.

The primary site is located in an elevated place above the city and far from the sea. For both sites, the Ministry of Defense has taken reasonable precautions to minimize the impact of exposure to water.

All sites are equipped with sophisticated fire detection and suppression systems. The staff is also adequately trained to learn the building evacuation and assembly procedures at the designated collection point.

All media containing software, data, audits, archiving and backup information are recorded in redundant archiving systems and protected with adequate physical and logical controls to limit access to authorized personnel and protect such media from accidental damage (example water, fire, electromagnetism, etc.).

All sensitive documents and materials are shredded prior to disposal. Media used to collect or transmit sensitive information are rendered illegible before disposal.

Cryptographic devices are physically destroyed or erased according to manufacturers' guidance before disposal.

PKI Difesa routinely backs up critical system data, audit log data, and other sensitive information.

Backup media are securely stored on storage drives.

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:

- Data Processing Operators;
- the Local Managers;
- CMS Operators;
- The Defence Computer Protocol System Manager;
- 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.

Such delicate tasks, such as the activation of the Signature CA 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.

For all trusted roles, identity is verified mainly via the Modello ATe, or a valid ID document.

The roles that require separation of duties are those for:

- the acquisition and validation of requests for cards and/or certificates;
- operations on hardware and/or software devices where the Signature CA keys are stored;
- revocation request operations.

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 have 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 ("Nulla Osta di Segretezza" – NOS).

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;
- 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:

- PKI Difesa basic 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 competence, to operate safely, and ensure service continuity of service.

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. In case of unauthorised access, the independent contractor shall be reported to police authorities.

Independent contractors who have not completed the background check procedure mentioned in section 5.3 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, and all movements deemed useful to monitor events.

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 media.

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

- Key life cycle management events concerning the Signature CA, 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 CA 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:
  - Physical access to the racks through the electronic keys of the Data Center;
  - 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 also 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	

The certificates' 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 the CA 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 maintained 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 CA activities, all software systems and hardware are subject to manual and/or automated vulnerability checks.

5.5 Records archival

The Signature CA maintains all information related to issuance and certificate management processes, including:

- Issuance requests;
- The documentation provided to applicants;
- The CSR (Certificate Signing Requests) submitted by applicants;
- Biographical data of applicants and end users (should they be separate subjects);
- The results of Signature CA audits;
- The request 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 maintained in an external storage device.

Copies of paper documents are maintained in a specific reinforced 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 Signature CA certificate life, the Ministry of Defence renews the key pair and the CA 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.

Following situations of compromise of the private key of the Signature CA, a specific procedure is envisaged for the recovery of the certification services. The procedure is indicated within the Command Security Plan for Network Operations.

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, e.g., disclosure to unauthorised third parties and/or loss of one or more private certification 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 Signature CA keys are maintained in a reinforced rack, access to which is only restricted to authorised personnel. Only authorised personnel can access the area where the rack is hosted.

In case of corrupted equipment, software, or data the Certification Centre Manager shall inform the Defence Community Emergency Response Team (CERT) as the 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 suspected compromise of the CA or the infrastructure, the CERT Difesa and the Certification Center activate the key compromise procedures.

The CERT Difesa, which includes security personnel, and the Certification Center and other representatives who are in charge of the operational management of the PKI Difesa, assess the situation, develop an action plan, and implement the action plan with the approval by the Commander of the Network Operations Command as Qualified Trust Service Provider.

Should the Signature CA revocation of certificate be required:

- All certificate holders and relying parties shall be notified;
- All Ministries/Public bodies with which cooperation agreements are in place shall be notified;
- The Italian Supervisory Authority shall be informed;
- A new private key for the Signature CA is generated, unless a decision is made to cancel the service.

In case of private key compromise, notification is given that all certificates and information on revocation distributed through such private key are no longer valid. In case an algorithm in use is compromised, notification of revocation for the affected certificates is given.

The Certification Centre has created a Disaster Recovery site similar to the structure of the primary site in order to limit the 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. Notification should also be given to certificate holders the provider has issued with indication that all unexpired certificates will be revoked upon termination.

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 Trust Services Provider also indicates the depositary of the keeper of the register of certificates and the relevant documentation [DLGS82], in addition to registration information, revocation status information, event log archives.

The reasons for the termination of the service could be of a voluntary nature”Service not considered to be of public utility”,”£High costs of the service not convenient for the A.D.”,” Radical modification of the Ate Model, involuntary: “Compromise of the entire infrastrucuture”.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

The key pair used by the Signature CA to sign certificates and the CRL 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.

When the Modello Ate is issued, the CMS generates the key pair inside the card, which is also Common Criteria EAL4+ certified.

The Computer Protocol System Manager for Defence generates the key pair within the automatic signature HSM for the automatic signature certificates.

Through a special digital procedure, the holder generates his/her key pair within the remote signature HSM for remote signature certificates.

The operator of the Certification Center with a special computer procedure generates the key pair internally to the HSM for automatic signature / seal, for the automatic signature / seal certificates of the SMD / COR Defense.

Upon receiving the certificate issued from the Signature CA – and therefore the public key – , the requesting CMS automatically writes the certificate inside the Modello Ate of the owner. When the holder receives the Modello Ate, he/she will also receive the public key linked to the certificate.

The holder automatically receives the remote signature certificate – and therefore the public key – together with the very system of remote signature.

The operator of the Certification Centre then e-mails the automatic signature certificate – and therefore the public key – to the Defence Computer Protocol System Manager.

The operator of the Certification Center sends an email with an attached encrypted envelope containing the secrets of the automatic signature certificate and / or Digital Seal of the SMD/COR Defense and the communication of the provision of the requested service directly to the holder.

The Certification Centre shall make available to the public the Signature CA certificate on the www.pki.difesa.it website.

The Signature CA Key is 4096 bits in length.

A signature certificate key is 2048 bits in length.

An OCSP certificate key is 2048 bits in length.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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+.

The key pair of the signature certificate holder is stored within the Modello Ate, i.e. a Common Criteria EAL 4+ certified device.

The key pair of the remote and automatic signature certificate and digital sea holder is stored within a high-quality HSM with FIPS PUB 140-2 Level 3 security certification, Common Criteria EAL 4+, and Italian standard-compliant.

In order to protect the Signature CA 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 Signature CA 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 Signature CA private key cannot be exported from the HSM.

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

The Signature CA 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 that hosts the copy used for operations (within the HSM).

The signature certificates private key is generated within the Modello ATe and no backup or key recovery is allowed.

The signature certificate remote and automatic private key is generated within the remote signature HSM.

The key pair associated with the Signature CA 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 Signature CA generate its key pair inside the first HSM, which also 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 Signature CA private key is stored within the HSM according to the HSM protection and cyphering methods.

The Signature CA private key shall be enabled as soon the HSM and the Signature CA service are enabled.

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

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

The Certification Centre uses the "zeroization" function of the HSM and other adequate tools to ensure the complete destruction Signature CA private keys.

6.3 Other aspects of key pair management

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

The Signature CA 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 the same of the corresponding certificate.

The following table indicates the maximum duration of individual certificates:

Certificate	Certificate Lifecycle	Key Lifecycle
Signature CA Certificate	Up to 30 years	Up to 20 years
User Signature Certificate on Mod. ATE	Up to 10 years	Up to 10 years
User Remote/Automatic Signature Certificate/Seal	Up to 10 years	Up to 10 years
OCSP Certificate	Up to 5 years	Up to 5 years

The QTSP does not issue certificates with expiration date higher than the expiration date of the CA certificate and it will provide in time when needed to renew and issue the new CA keys and the corresponding certificate.

6.4 Activation data

The Signature CA HSM activation process requires a certain number of keys and PINs held by the operators under the responsibility of the Certification Manager.

In order for a holder of a signature certificate to use it, the PIN for the login to the Modello ATe must be used together with a PIN to authorise the use of signature. The holder of the smartcard is the only person to know both PINs. Before the signature key can be used for the first time, the holder shall verify his/her signature has not been used before by inputting a SIGNATURE PIN. If successful, the procedure will unlock the signature key.

For the holder to use an automatic signature key or remote signature, he/she shall have a smartcard PIN or OTP PIN and/or password only known to him/her.

The data required to protect tokens and enable private key activation are 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.

6.5 Computer security controls

The Operational Systems used by the Signature CA 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 the one from the other and from the Defence network by a high-quality firewall system that filters connections as required.

Signature CA 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 Signature CA 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 public specification [RFC 5280].

The basis for the profiles of issued certificates is the ETSI policy known as **QCP-n-qscd** "*policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a device for the creation of qualified electronic signatures/seals*" and identified with the following OID: `Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)`, for legal person, the ETSI policy known as **QCP-l-qscd "**policy for EU Qualified Certificates issued to a legal person where the private key and the related certificated reside on QSCD" and identified with the following OID itu-t(0) identified-organization (4) etsi(0) qualified certificate policies (194112) policy-identifiers (1) qcp-legal-qcsd (3)

PROFILE OF THE SIGNATURE CA CERTIFICATE

The profile of the Signature CA 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=1.3.6.1.4.1.14031.2.1.1 - Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.pki.difesa.it/ManualeOperativoDifesa.pdf
Authority Information Access (AIA)	• Authority Info Access - Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsppkiff.difesa.it/
CRL Distribution Points (CDP)	• CRL Distribution Point URL=http://www.pki.difesa.it/cafirmadigitale.crl

FIELD	VALUE
	• CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa - CA di Firma Digitale,OU=S.M.D. – Comando per le Operazioni in Rete,O=Ministero della Difesa,C=IT

PROFILE OF THE SIGNATURE CERTIFICATE

The default profile of signature certificates for holders of the Modello ATe is as follows:

During personal data acquisition, users can request that a signature profile with no limitations in the use of OID 1.3.6.1.4.1.14031.2.1.1.12 is added.

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 CA, 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 CA
Subject Key Identifier (SKI)	Variable and calculated as per RFC 5280
Key Usage	Non Repudiation (40)
Certificate Policies	• Certificate Policy: - Policy Identifier=1.3.6.1.4.1.14031.2.1.1.13 User Notice: Il Titolare fa uso del certificato solo per le finalita' di lavoro per le quali esso e' rilasciato. The certificate holder must use the certificate only for the purposes for which it is issued. Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://pki.difesa.it/tsp • Certificate Policy: - Policy Identifier=1.3.76.16.6
Subject Alternative Name (SAN)	RFC822 Name. Same as the work e-mail.
Authority Information Access (AIA)	• Authority Info Access - Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.pki.difesa.it/cafirmadigitale.crt - Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsppkiff.difesa.it/
CRL DistributionPoints (CDP)	• CRL Distribution Point URL=http://www.pki.difesa.it/cafirmadigitale.crl

	• CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa - CA di Firma Digitale,OU=S.M.D. – Comando per le Operazioni in Rete,O=Ministero della Difesa,C=IT
Qualified Certificate Statements	• NO information on the limit of negotiations (QcLimitValue) • Retention period (QcRetentionPeriod): 20 years • Key protected by a secure device for creation of signature (QcSSCD) • Qualified Certificate (QcCompliance) • Certificate for electronic signature complies with eIDAS Regulation (EU Regulation 910/2014) (QcType=id-etsi-qct-esign) • PKI Disclosure Statements (QcEuPDS) Publication Addresses: - https://pki.difesa.it/tsp/ (ENGLISH) - https://pki.difesa.it/tsp/ (ITALIAN)

PROFILE OF THE REMOTE SIGNATURE CERTIFICATE

The profile for the signature certificates of remote signature holders 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 CA, 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 CA
Subject Key Identifier (SKI)	Variable and calculated as per RFC 5280
Key Usage	Non Repudiation (40)
Certificate Policies	• Certificate Policy: - Policy Identifier=1.3.6.1.4.1.14031.2.1.1.15 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://pki.difesa.it/tsp • Certificate Policy: - Policy Identifier=1.3.76.16.3 User Notice: Il Certificatore garantisce che le firme basate su questo certificato qualificato sono valide in quanto il certificato ad esse associato era valido al momento della generazione delle firme User Notice: The qualified certification service provider that issued this certificate ensures that the signatures based on this certificate have been generated during the period of validity of the certificate • Certificate Policy: - Policy Identifier=1.3.76.16.6
Subject Alternative Name (SAN)	RFC822 Name. Same as the work e-mail.

Authority Information Access (AIA)	• Authority Info Access - Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.pki.difesa.it/cafirmadigitale.crt - Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsppkiff.difesa.it/
CRL DistributionPoints (CDP)	• CRL Distribution Point URL=http://www.pki.difesa.it/cafirmadigitale.crl • CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa - CA di Firma Digitale,OU=S.M.D. – Comando per le Operazioni in Rete,O=Ministero della Difesa,C=IT
Qualified Certificate Statements	• NO information on the limit of negotiations (QcLimitValue) • Retention period (QcRetentionPeriod): 20 years • Key protected by a secure device for creation of signature (QcSSCD) • Qualified Certificate (QcCompliance) • Certificate for electronic signature complies with eIDAS Regulation (EU Regulation 910/2014) (QcType=id-etsi-qct-esign) • PKI Disclosure Statements (QcEuPDS) Publication Addresses: - https://pki.difesa.it/tsp/ (ENGLISH) - https://pki.difesa.it/tsp/ (ITALIAN)

PROFILE OF THE AUTOMATIC SIGNATURE CERTIFICATE OF SGD

The profile for the signature certificates of automatic signature holders 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 CA, 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 CA
Subject Key Identifier (SKI)	Variable and calculated as per RFC 5280
Key Usage [Critical]	Non Repudiation (40)
Certificate Policies	• Certificate Policy: - Policy Identifier=1.3.6.1.4.1.14031.2.1.1.18 User Notice: Il presente certificato è valido solo per firme apposte con procedura automatica./This certificate may only be used for unattended/automated digital signatures. Policy Qualifier Info: Policy Qualifier Id=CPS

	Qualifier: https://pki.difesa.it/tsp • Certificate Policy: - Policy Identifier=1.3.76.16.6
Subject Alternative Name (SAN)	RFC822 Name. Same as the work e-mail.
Authority Information Access (AIA)	• Authority Info Access - Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.pki.difesa.it/cafirmadigitale.crt - Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsppkiff.difesa.it/
CRL DistributionPoints (CDP)	• CRL Distribution Point URL=http://www.pki.difesa.it/cafirmadigitale.crl • CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa - CA di Firma Digitale,OU=S.M.D. - C.do C4 Difesa,O=Ministero della Difesa,C=IT
Qualified Certificate Statements	• NO information on the limit of negotiations (QcLimitValue) • Retention period (QcRetentionPeriod): 20 years • Key protected by a secure device for creation of signature (QcSSCD) • Qualified Certificate (QcCompliance) • Certificate for electronic signature complies with eIDAS Regulation (EU Regulation 910/2014) (QcType=id-etsi-qct-esign) • Pki Disclosure Statements (QcEuPDS) Publication Addresses: - https://pki.difesa.it/tsp/ (ENGLISH) - https://pki.difesa.it/tsp/ (ITALIAN)

PROFILE OF CERTIFICATE AUTOMATIC SIGNATURE SMD COR

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

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

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

EIDAS DIGITAL SEAL CERTIFICATE PROFILE

The profile defined for the signature certificates of holders of automatic signatures is shown below.

CAMPO	VALORE

Version	3
Serial Number	Variable as per RFC 5280
Signature	RSA signature affixed by the CA as per RFC 5280
Issuer	Corresponding to the Subject of the CA, as indicated in section 3.1
Validity	Variable, as indicated in section 6.3
Subject	As indicated in section 3.1
Subject Public Key Info	RSA public key (modulo and public exponent) as per RFC 5280
ESTENSIONE	**VALORE**
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier (AKI)	Corresponding to the CA SKI
Subject Key Identifier (SKI)	Variable and calculated as per RFC 5280
Key Usage [Critical]	Non Repudiation (40)
Certificate Policies	• Certificate Policy: - Policy Identifier=1.3.6.1.4.1.14031.2.1.1.23 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://pki.difesa.it/tsp • Certificate Policy: - Policy Identifier=1.3.76.16.6
Subject Alternative Name (SAN)	RFC822 Name corresponding to the institutional email
Authority Information Access (AIA)	• Authority Info Access - Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.pki.difesa.it/cafirmadigitale.crt - Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsppkiff.difesa.it
CRL DistributionPoints (CDP)	• CRL Distribution Point URL=http://www.pki.difesa.it/cafirmadigitale.crl • CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa - CA di Firma Digitale, OU=S.M.D. - C.do C4 Difesa,O=Ministero della Difesa,C=IT
Qualified Certificate Statements	• NO information on the trading limit (QcLimitValue) • Retention period (QcRetentionPeriod) of 20 years • Key protected by a secure signature creation device (QcSSCD • Qualified Certificate (QcCompliance) • Certificate for the Electronic Signature as per the Regulations eIDAS (Regolamento UE N. 910/2014) (QcType=id-etsi-qct-esign) • Publication addresses of the PKI Disclosure Statements (QcEuPDS): - https://pki.difesa.it/tsp/ (lingua EN) • https://pki.difesa.it/tsp/ (lingua IT)

PROFILE OF THE AUTOREMOTE EIDAS DIGITAL SEAL CERTIFICATE

The profile defined for the signature certificates of holders of automatic signatures is shown below.

CAMPO	VALORE
Version	3
Serial Number	Variable as per RFC 5280
Signature	RSA signature affixed by the CA as per RFC 5280
Issuer	Corresponding to the Subject of the CA, as indicated in section 3.1
Validity	Variable, as indicated in section 6.3
Subject	As indicated in section 3.1
Subject Public Key Info	RSA public key (modulo and public exponent) as per RFC 5280
ESTENSIONE	**VALORE**
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Authority Key Identifier (AKI)	Corresponding to the CA SKI
Subject Key Identifier (SKI)	Variable and calculated as per RFC 5280
Key Usage [Critical]	Non Repudiation (40)
Certificate Policies	• Certificate Policy: - Policy Identifier=1.3.6.1.4.1.14031.2.1.1.28 User Notice: Il presente certificato è valido solo per firme apposte con procedura automatica./This certificate may only be used for unattended/automated digital signatures. Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://pki.difesa.it/tsp • Certificate Policy: - Policy Identifier=1.3.76.16.6
Subject Alternative Name (SAN)	RFC822 Name corresponding to the institutional email
Authority Information Access (AIA)	• Authority Info Access - Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://www.pki.difesa.it/cafirmadigitale.crt - Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsppkiff.difesa.it/
CRL DistributionPoints (CDP)	• CRL Distribution Point URL=http://www.pki.difesa.it/cafirmadigitale.crl • CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa - CA di Firma Digitale, OU=S.M.D. - C.do C4 Difesa,O=Ministero della Difesa,C=IT

Qualified Certificate Statements	• NO information on the trading limit (QcLimitValue) • Retention period (QcRetentionPeriod) of 20 years • Key protected by a secure signature creation device (QcSSCD • Qualified Certificate (QcCompliance) • Certificate for the Electronic Signature as per the Regulations eIDAS (Regolamento UE N. 910/2014) (QcType=id-etsi-qct-esign) • Publication addresses of the PKI Disclosure Statements (QcEuPDS): • https://pki.difesa.it/tsp/ (lingua EN) - https://pki.difesa.it/tsp/ (lingua IT)

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 CA, as stated in Section 3.1.
Effective Date	Date of issue
Next Update	Date not lather than a new CRL will be issued
Revoked Certificates	List of revoked certificates. For every item, the following is specified: • Revoked certificate serial number, • Date and time of revocation, • ID code of reason for revocation
CRL Extensions	Extensions as per following table
CRL Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11) algorithm
CRL Signature	RSA Signature from CA as per RFC 5280

EXTENSION	**Value**
Authority Key Identifier	Same as SKI of CA
CRL Number	Issued CRL serial number
Id-ce-expiredCertsOnCRL (2.5.29.60) Extension	Date since when the CRL also includes the expired revoked certificates.

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 CA as per RFC 5280
Issuer	Same as Subject of CA, 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 CA
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=1.3.6.1.4.1.14031.2.1.1.1 - Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://pki.difesa.it/tsp
CRL DistributionPoints (CDP)	• CRL Distribution Point URL=http://www.pki.difesa.it/cafirmadigitaleeidas.crl • CRL Distribution Point URL=ldap://ldappkiff.difesa.it:389/CN=Ministero della Difesa - CA di Firma Digitale eIDAS,OU=S.M.D. – Comando pee le Operazioni in Rete,O=Ministero della Difesa,C=IT

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 and 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 frequencies (monthly and annual) for the different technical and operational aspects of the Signature CA 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 Signature CA 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 integrity of the “audit log” and compliance with the operational procedures concerning the Signature CA.

8.5 Actions taken as a result of deficiency

In case of deficiencies, Ag.ID requires Signature CA 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 ad-hoc 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

Since it is a Public Administration, 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 provisions of applicable laws.

PKI Difesa ensures confidentiality of information treated as confidential.

9.4 Privacy of personal information

The Ministry of Defence is the controller of the personal data provided by the card applicant and shall notify the applicant of personal data processing, within the meaning and for the purposes of the Reg. (EU) 2016/679 (GDPR). Applicants' personal data shall be processed by authorised personnel, by means of paper records and appropriate computer tools that ensure their security and confidentiality in compliance with the modalities laid down in the above-mentioned regulation.

Data provided by the applicants include mandatory and optional data. Mandatory data are necessary for service provision; failure to provide mandatory data shall result in the impossibility to enter into the contract. It should be noted that the publication of the certificate implies the dissemination to third parties of the information contained in the certificate. Optional data simply make the service easier; failure to provide optional data is not an obstacle to completing the acquisition process.

Data provided by the applicant are processed solely for the purpose of issuing or renewing certificates.

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

PKI participants who obtain private information shall protect it from 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 Certification Centre and PKI Difesa.

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

Signature CA undertakes 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 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

The RA and LRA udertake to:

- comply with this CP and CPS;
- identify applicants as described in this CP and CPS;
- timely report possible compromise of their private key;
- provide clear and comprehensive information on service procedures and requirements;
- ensure that personal data are processed in compliance with current regulations;

If the LRA is a subject outside the Ministry of Defence, LRA repesentations are defined in the ad-hoc cooperation agreement and are based at least on the representations contained herein.

9.6.3 Subscriber representations and warranties

The Applicant or Subscriber has the obligation to:

- read, understand and fully accept this CP and CPS;
- request the certificate in accordance with the procedures laid down in this CP and CPS;
- provide Signature CA, RA and LRA with true and accurate information during registration;
- take appropriate technical and organisational actions to avoid compromise of his/her private key;

- request the immediate suspension of the certificate in case of suspected or ascertained compromise of his/her private key and than make the revocation request if the suspicion is confirmed;
- Request the immediate revocation of certificate in case one or more items of information contained in the certificate (i.e. surname, name, tax code, etc..) are incorrect or no more valid;
- after issuance of the certificate and until its expiration or revocation, promptly inform Signature CA of any change to the information provided on application.
- upon revocation of the certificate, return or immediately cease use of the certificate.

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 regarding 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

Signature CA ha 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

Signature CA 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 Defense Administration, in view of:

- misrepresentation in the application for certification;
- failure to provide information on essential actions or circumstances for negligence or with a view to deceiving the Ministry of Defence;
- use of names in violation of individual property rights;
- use of the Mod. ATE and relevant certificates for activities not covered by existing legislation.

of the data holders, initiates all the procedures provided for by law, for the detection of any criminal liability (pursuant to Art.76 of Presidential Decree no. 445/2000), civilian (subject to the conditions) and administrative (for eventual damage to the office).

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 RA shall notify issuance or change of certificate status to the mail address indicated by the holder upon enrollment.

The certification centre notifies the certificate holder, via an informatic process in the signature software, that a new version of the signature software has been published.

The CA accepts notifications by the holder according to the modalities specified in paragraph 1.5.

9.12 Amendments

The Ministry of Defense reserves the right to modify this CP at any time. For each change, a new version of this CP will be produced and published, giving appropriate notice.

An OID must be changed only when a reorganization of the main OID is needed for reasons that are not attributable to PKI Difesa.

9.13 Dispute resolution provisions

Any litigation or other dispute shall be settled in the Court of Rome.

9.14 Governing law

This CP is governed by, construed and enforced in accordance with the laws of Italy. For all matters non-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

As the signature certificate is provided together with the Modello ATe, all existing provisions concerning use of the Modello Ate within the Ministry of Defence and other Ministries shall apply.

For the Ministry of Defence employees, the signature certificate is issued on the Modello ATe, the employee ID card, and is considered as a working tool.

For employees of other Ministries, the modello ATe and relevant certificates are issued only if a cooperation agreement has been entered into by those Ministries and the Ministry of Defence.

If any clause or provision of this CP is found 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.