TRUST SERVICE POLICY APPLIED

The Certification Authority of the Ministry of Defence issues the following signature certificates:

- default limited signature [1]– OID 1.3.6.1.4.14031.2.1.1.13 – included within the smart card of the Modello ATe/CMD;
- unlimited signature – OID 1.3.6.1.4.14031.2.1.1.12 – included within the smart card of the Modello ATe/CMD during data acquisition on request by the subscriber (hereinafter referred to as 'holder');
- remote signature – OID 1.3.6.1.4.14031.2.1.1.15;
- automated signature (SGD) – OID 1.3.6.1.4.14031.2.1.1.18 - issued to enabled special electronic processes;
- automated signature (SMD-COR) – OID 1.3.6.1.4.14031.2.1.1.19 - issued to enabled special electronic processes;
- seal eIDAS – OID 1.3.6.1.4.1.14031.2.1.1.23 issued to enabled special electronic processes;
- seal Autoremote eIDAS – OID 1.3.6.1.4.1.14031.2.1.1.28 issued to enabled special electronic processes.

Starting from December 2019, the certificates include a further Policy Identifier with value agIDcert (OID 1.3.76.16.6).

All signature certificates shall be used in accordance with the provisions of the CPS and this document. They can only be used as set forth in EU Regulation no. 910/2014 of the European Parliament and of the Council of 23 July 2014 regarding *electronic identification and trust services for electronic transactions in the domestic market, which repeals Directive 1999/93/EC*..

[1] 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

The expiration for all signature certificates is 10 years at the latest. The certificates comply with ETSI certificates requirements according the QCP-n-qscd policy identified from the following OID: Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2), and the QCP-l policy identified by OID itu-t(0) identified-organizzation (4) etsi(0) qualified-organization-policies (194112) policy identifiers (1) qcp-legal-qcsd (3)

LIMITATIONS ON THE USE OF THE SERVICE

The TSP provides CA and Signature Services free of charge to military and civil personnel employed by the Ministry of Defence and to the personnel from other governmental bodies who have signed an agreement with the Ministry of Defense.

The limits concerning the use of the certificate are included in the CPS and the certificate itself.

SUBSCRIBERS'S OBLIGATIONS

The holder shall:

- read the CPS and the regulations mentioned therein before he/she fills the registration/subscription form;
- provide complete, correct and truthful information to the registration operator during the enrolment process, according to D.P.R. n.44/2000 Art.76;
- safely store the PIN/codes received in order to protect their confidentiality;
- promptly notify the Data Processing Operator of any change in the information provided to him/her during enrolment;

- In case of theft or loss of the Modello ATe/CMD, immediately report the incident to the membership organization, following a written copy of the complaint made before the judicial authority (Police or Carabinieri) and request the suspension or revocation of the certificate according to the procedure described In the operating manual and CPS;
- activate the signature (if required);
- check that the profile of issued certificate is correct in all its fields and extensions, including the limitations to use, before the private key connected with the certificate is used;
- refrain from using the private key, should the corresponding certificate show discrepancies against what is expected;
- use the digital signature only in compliance with the provisions in the CPS and the current laws;
- maintain their private keys and signature devices with the utmost care, in order to preserve their integrity and confidentiality;
- request the immediate revocation of the certificates for the keys inside the signature devices he/she has lost or that are no longer functioning;

As for the truthiness of data, the Holder shall be fully accountable.

The holder shall have full responsibility for any damage caused to the Ministry of Defence or third parties from: concealment of identity, false statements concerning one's own identity, or provision of incorrect and/or incomplete information; the improper use of certificates and of the Modello ATe/CMD; or activities not covered by the regulations in force. The Holder shall guarantee and hold harmless the Ministry of Defence from any claim against it. The holder hereby acknowledges he/she shall guarantee and hold harmless the Ministry of Defence and/or third parties from claims submitted by third parties for holder' statements, false certifications, or omissions related to his/her identity and/or for improper use of certificates and/or the Modello ATe/CMD, or for activities not covered by the regulations in force.

INFORMATION FOR RELYING PARTIES

The Ministry of Defence is the legal person in charge for processing personal data that the Holder/ subscriber provides as he/she submits the request to issue the Modello ATe/CMD and the Certificate for Automated Signature and/or Remote Signature. The Ministry of Defence hereby informs the holder that, pursuant to Legislative Reg. (UE) 2016/679 (GDPR), the holder's personal data will be stored on both paper documents and electronically, The ICT systems used provide proper levels of security and confidentiality, as set forth in the above mentioned legislative decree and in the confidentiality requirements.

In relation to the aforementioned data processing, the Data Controller may exercise the rights referred to in art. from 15 to 21 of Reg. (EU) 2016/679 (GDPR) ".

EVENT LOGS RETENTION

Major events connected with the life cycle of certificates, including certificate issue, suspension or revocation, etc. should be stored on paper or in digital form. Other events are also logged, such as: logical access to the certificate management system, operations executed by personnel of the Ministry of Defence, entry/exit of visitors to/from the premises where certificates are issued, and so on.

The type, date, and time of each event and – where available – all information about who was involved in the event and the outcome of activities are logged.

The whole of logged entries represents the audit log. The files of the audit log are periodically backed up with a retention period of 20 years.

LIMITATIONS OF LIABILITY

Without prejudice to the applicable laws and with respect to this terms and conditions, the Ministry of

Defence will only be liable for gross negligence of wilful misconduct.

LIMITS TO CLAIMS FOR DAMAGES

In accordance with limits established by the law, the Ministry of Defence cannot guarantee all terms included in this contractual terms and conditions will be met in case one or more events of force-majeure occur.

The following are considered events of force-majeure: wars, terrorist action, natural disasters, failure of power supply equipment, failures preventing Internet access or failures affecting other infrastructures.

APPLICABLE LEGAL SYSTEM

This contract is subject to the Italian Law and should be interpreted and executed as such.

COMPLAITS AND DISPUTE SETTLEMENT

For any controversy and dispute the competent forum is that of Rome.

CONFORMITY ASSESSMENT

The Certification Authority of the Ministry of Defence and its PKI infrastructure are compliant with the standard mentioned in EU Regulation no. 910/2014 of the European Parliament and the European Council dated 23 July 2014 concerning *electronic identification and trust services for electronic transactions in the internal market, which supersedes EU Directive 1999/93/EC*.

Based on the compliance inspection conducted by one of the Italian CABs, the Ministry of Defence PKI infrastructure has been accredited before AgID.

CONTACT INFORMATION

Legal person: STATO MAGGIORE DELLA DIFESA – Comando per le Operazioni in Rete.
Address: Via Stresa 31b 00135 Roma
Employer Identification Number: 97355240587
ISO Object Identifier: 1.3.6.1.4.1.14031Email address: info_pkiff@smd.difesa.it
Telephone: +39 06 46914444
Website: https://pki.difesa.it/tsp

AVAILABILITY

The Certification Authority services offered by the Ministry of Defence are available 24/7.

With regard to the inherent availability of information on the revocation status of the certificates after their period of validity, the certifier undertakes to make it available as indicated in the CPS document in paragraph 4.10

Gen. Div. AAran Sandro SANASI	Qualified Trust Services Provider (QTSP)	*Firmato Digitalmente da/Signed by:* **SANDRO SANASI** *In Data/On Date:* **venerdì 28 marzo 2025 16:15:31**