



TRUST SERVICE POLICY APPLIED

The Ministry of Defence's Timing Stamping Authority eIDAS Certification Authority is identified by OID 1.3.6.1.4.14031.2.1.7 and issues the following types of certificates:

- OCSP for Time Stamping Unit eIDAS – OID 1.3.6.1.4.14031.2.1.7.1;
- Time Stamping Unit eIDAS – OID 1.3.6.1.4.14031.2.1.7.2.

The Time Stamping Unit (TSU) certificates are used only in the manner specified in the CPS and within this document and may only be used in accordance with Regulation (EU) No 910/2014 of the European Parliament and of the Council of July 23, 2014 *on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*.

All Time Stamping Units certificates have a maximum validity of 10 years. The key of these certificates is renewed every 3 months, generating a new key and issuing a new certificate. The TSU certificate is kept by the TSP for a duration of 20 years from the expiry date of the certificate.

The time stamp service meets the ETSI certificate requirements according to the BSTP policy "best practices policy for time-stamp" issued by ETSI and identified by the following OID: itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy(1), or 0.4.0.2023.1.1

LIMITATIONS ON THE USE OF THE SERVICE

Time marking services are offered free of charge to employees of the Ministry of Defence and other P.A. who have signed an agreement with the Ministry of Defense.

SUBSCRIBERS'S OBLIGATIONS

End Users, or Time Stamping Units, are internal hardware / software devices that require a digital certificate containing the corresponding private key of the applicants in order to produce time stamps in their favour.

Time stamps issued by Time Stamping Unit services are kept by the TSP for a duration of 20 years from the date of issue

By internal authentication and authorization procedures, it is ensured that only TSP TSU services are enabled to request and use certificates issued for this purpose

The obligations of the subscriber are the same as the obligations of the TSP, namely:

- operate in accordance with the CPS;
- promptly report possible compromise of your private key;
- provide clear and complete information on the procedures and requirements of the service

Users of Time Stamp Services as well as third parties are required to:

- Take a look at the Operational Manual, the CPS and the legislation listed there
- They can check the status of a certificate by downloading the certificate revocation list (CRL) or querying the OCSP service.

The user assumes all responsibility for any damage that may result from the Ministry of Defense or third parties in the event of improper use of the timing service.

INFORMATION FOR RELYING PARTIES

Time stamp service data are not considered personal data.

Any personal data will be processed by the Ministry of Defence in accordance with the Personal Data Processing Act. The applicable privacy laws are DLGS



MINISTRY OF DEFENCE

Trust Service Provider – Time Stamping CA

TERMS AND CONDITIONS – v1.6

196/2003, also referred to as the "*Personal Data Protection Code*".

EVENT LOGS RETENTION

Major events related to the management of the certificate lifecycle, including certification requests, suspension or revocation, etc., are recorded in paper or electronic form. Other events are also logged, such as logical access to the certificate management system, operations carried out by the Ministry of Defence personnel, entry and exit of visitors on the premises where certification activities are performed, etc. .

Each event records the type, date and time of occurrence and, if available, other useful information to identify the actors involved in the event and the outcome of the transactions.

The set of records constitutes the "audit log". The files that compose it are transferred periodically to permanent support with a retention period of 20 years.

LIMITATIONS OF LIABILITY

The Ministry of Defence declines any liability for any damage suffered by the staff due to the failure to receive Time Stamping CA communications as a result of a wrong email address provided at the time of the request.

LIMITS TO CLAIMS FOR DAMAGES

To the extent permitted by law, the Ministry of Defence cannot guarantee everything that is indicated in this contract when one or more major events occur.

For events considered "force majeure" are meant wars, acts of terrorism, natural disasters, failures of power supply equipment or failures of the Internet or other infrastructures.

APPLICABLE LEGAL SYSTEM

This contract is subject to Italian law and as such will be interpreted and executed.

COMPLAINTS AND DISPUTE SETTLEMENT

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

CONFORMITY ASSESSMENT

The Ministry of Defence eIDAS Time Stamping Authority Certification Authority and its PKI structure have been evaluated in accordance with the standard set out in European Parliament and Council Regulation (EU) No. 910/2014 of July 23, 2014 *on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*.

Following the Conformity Inspection conducted by one of the Italian CABs, the Ministry of Defence's PKI structure was accredited at AgID.

CONTACT INFORMATION

Legal person: STATO MAGGIORE DELLA DIFESA – COMANDO PER LE OPERAZIONE IN RETE.
Address: Via Stresa 31b 00135 Roma
Employer Identification Number: 97355240587
ISO Object Identifier: 1.3.6.1.4.1.14031
Email address: info_pkiff@smd.difesa.it
Telephone: +39 06 46914444
Websites: www.pki.difesa.it and <https://pki.difesa.it>

AVAILABILITY

Time Stamping Authority and Timekeeping services are offered by the Ministry of Defence and are available at h24, 7 days a week.

Sergio Antonio SCALESE	Qualified Trust Services Provider (QTSP)	
------------------------------	--	--