Digital Signature Certification Authority

PKI Disclosure Statement

Statement types	English	Italiano
TSP contact info **(Informazioni di contatto del TSP)**	Ministero della Difesa - Comando per le Operazione in Rete Via Stresa 31b 00135 Roma telephone number: +39 06 46914444 Mail: info_pkiff@smd.difesa.it Website: https://pki.difesa.it/tsp	Ministero della Difesa - Comando per le Operazione in Rete. via Stresa 31b 00135 Roma telefono: +39 06 46914444 email: info_pkiff@smd.difesa.it sito web: https://pki.difesa.it/tsp
Certificate type, validation procedures and usage **(Tipo di Certificato, procedure di validazione ed uso)**	The signature certificate is issued only after applicant's ID check. ID check is performed by: ▸ Data Processing Operators (RDT) and the Local Manager in the Local Registration Authority for signature certificates issued in the Modello ATe; ▸ by the Computer Protocol System Manager for automatic signature certificates of SGD; ▸ the Certification Centre for remote signature certificates, automatic signature of SMD-COR and elettronic seals. The Signature CA of the Ministry of Defence issues the following types of signature certificates: ▸ Restricted usage signature - OID 1.3.6.1.4.14031.2.1.1.13 comprised by default in the smart card (Modello ATe)	Il certificato di firma è emesso solo dopo la verifica di un documento di identità del richiedente. La verifica viene svolta: ▸ dagli Operatori Autorizzati all'inserimento dei dati (OA) e dal Funzionario Autorizzato alla Validazione dei Dati (FA) presenti nella Local Registration Authoriry per i certificati di firma rilasciati all'interno del modello ATe; ▸ dal responsabile del Sistema di protocollo informatico per i certificati di firma automatica di SGD; ▸ dal Centro di Certificazione per i certificati di firma remota e automatica SMD-COR, sigilli elettronici. La CA di Firma del Ministero della Difesa emette i seguenti tipi di certificati di firma: ▸ firma con limitazioni d'uso – OID 1.3.6.1.4.14031.2.1.1.13 Inserito all'interno della smart card (Modello ATe) per default;

	▸ Unrestricted usage signature - OID 1.3.6.1.4.14031.2.1.1.12 - comprised in the smart card (Modello ATe) as requested by the holder in the data enrolment phase ▸ Remote signature - OID 1.3.6.1.4.14031.2.1.1.15 ▸ Automatic signature SGD - OID 1.3.6.1.4.14031.2.1.1.18 issued to activate specific computer processes ▸ Automatic signature SMD-COR- OID 1.3.6.1.4.14031.2.1.1.19 issued to activate specific computer processes ▸ eSeal eIDAS – OID 1.3.6.1.4.1.14031.2.1.1.23 issued to enabled special electronic processes; ▸ eSeal Automatic 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). Signature certificates shall be used exclusively in the ways specified in the CPS and in the Terms and Conditions and only in compliance with the EU Regulation no. 910/2014 of the European Parliament and of the Concil of 23 July 2014 *regarding electronic identification and trust services for electronic transactions in the domestic market, which repeals Directive 1999/93/EC*. All signature certificates are valid for a maximum of 10 years and comply with the requirements of ETSI certificates according to the QCP-n-qscd policy as identified in the following OID: Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2), and to the QCP-l-qcsd policy (as identified by OID itu-t(0) identified-organization(4) etsi(0)	▸ firma senza limitazioni d'uso - OID 1.3.6.1.4.14031.2.1.1.12 - Inserito all'interno della smart card (Modello ATe) su richiesta del titolare in fase di acquisizione dei dati ▸ firma remota – OID 1.3.6.1.4.14031.2.1.1.15 ▸ firma automatica SGD – OID 1.3.6.1.4.14031.2.1.1.18 rilasciato per attivare appositi processi informatici ▸ firma automatica SMD-COR – OID 1.3.6.1.4.14031.2.1.1.19 rilasciato per attivare appositi processi informatici ▸ Sigillo eIDAS – OID 1.3.6.1.4.1.14031.2.1.1.23 per attivare appositi processi informatici ▸ Sigillo automatico eIDAS – OID 1.3.6.1.4.1.14031.2.1.1.28 per attivare appositi processi informatici. A partire da Dicembre 2019, i certificati riportano anche un ulteriore Policy Identifier con valore agIDcert (OID 1.3.76.16.6). I certificati di firma devono essere utilizzati solo nelle modalità indicate all'interno del CPS e nel documento Terms and Conditions e possono essere usati solo in accordo con il Regolamento (EU) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 Luglio 2014 *in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la Direttiva 1999/93/EC*. Tutti i certificati di firma hanno una validità massima di 10 anni e rispettano i requisiti dei certificati ETSI secondo la policy QCP-n-qscd identificata dal seguente OID: Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2), per le persone legali, la policy ETSI chiamata **QCP-l-qscd**"" è identificata dal seguente OID: itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3)

	qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3))	
Reliance limits **(Limiti di Affidamento)**	Log events regarding certificates are stored for at least 20 years. Remaining log events are stored according to policies of the Ministry of Defence.	Gli eventi di log riguardanti i certificati sono conservati per almeno 20 anni. I restanti eventi di log sono conservati secondo le policy del Ministero della Difesa.
Obligations of subscribers **(Obblighi dei sottoscrittori)**	Subscribers must: ▸ accept all clauses in the CPS, CP and in the Terms and Conditions; ▸ inform the relevant LRA or the Certification Centre of any error, defect or change in the data included in the certificate; ▸ acknowledge the contents of the SECURITY MEMORANDUM delivered to the user.	I sottoscrittori sono obbligati ad: ▸ accettare tutte le clausole contenute nel CPS, nel CP e nel documento di Terms and Conditions; ▸ informare la rispettiva LRA o il Centro di Certificazione di un qualsiasi errore, difetto o cambiamento nei dati contenuti nel certificato; ▸ prendere visione di quanto indicato nel MEMORANDUM DI SICUREZZA consegnato all'utente.
Certificate status checking obligations of relying parties **(Obblighi degli utilizzatori nella verifica dello stato del certificato)**	Certificate holders as well as third parties can verify the status of a certificate by downloading the list of revoked certificates (CRL) or by querying the OCSP. The CRL is published at the following URL http://www.pki.difesa.it/cafirmadigitale.crl The OCSP service can be contacted at the following URL: http://ocsppkiff.difesa.it For employees belonging to Defence and to public administration bodies who have entered into an agreement with the Ministry of Defence, the status of a certificate can be verified also by contacting the directory server: ldap://ldappkiff.difesa.it	I titolari dei certificati così come i soggetti terzi possono verificare lo stato di un certificato scaricando la lista dei certificati revocati (CRL) o interrogando il servizio di OCSP. La CRL è esposta al seguente URL http://www.pki.difesa.it/cafirmadigitale.crl Il servizio di OCSP è contattabile al URL http://ocsppkiff.difesa.it Per i dipendenti della Difesa e delle P.A. che hanno stipulato un accordo con il Ministero della Difesa, la verifica dello stato del certificato è disponibile anche contattando il directory server ldap://ldappkiff.difesa.it

Limited warranty and disclaimer/Limitation of liability **(Limitazioni sulla garanzia e sull'assistenza. Limitazioni sulla responsabilità)**	As regards activities that are directly or indirectly relevant to the TPS service defined in this document, Defence does not provide for any form of remuneration, compensation or reimbursement, without prejudice to the remuneration paid and/or due to its own employees as a consequence of the regular work performed to carry out the activities described in this document.	La Difesa per le attività direttamente o indirettamente pertinenti al servizio TPS definito in questa documento non prevede in alcun modo forme di retribuzione, rimborso o indennizzo, fermo restando la corresponsione in essere e/o dovuta ai propri dipendenti in virtù del normale rapporto di lavoro espletato nell'ambito delle attività previste dal presente documento.
Applicable agreements, CPS, CP **(Accordi Applicabili CPS, CP)**	The CP and CPS must be applied. These can be found at: https://pki.difesa.it/tsp Laws in force regarding privacy, the Reg. (UE) 2016/679, also referred to as *"GDPR".* The Defence infrastructure is available to other public administration bodies through cooperation agreements that are valid for 3 years starting from the subscription date. The parties can decide to renew the agreement provided its premises are still extant and the parties are still mutually interested in extending the agreement. All provisions in force regarding the use of the Modello Ate within the Ministry of Defence and public administration bodies shall also be applied.	Debbono essere applicati il CP, CPS reperibili sul sito https://pki.difesa.it/tsp I dati personali acquisiti per il rilascio della carta sono trattati dal Ministero della Difesa ai sensi del Reg. (UE) 2016/679 detto anche GDPR**.** L'infrastruttura della Difesa è resa disponibile ad altre P.A. attraverso accordi di collaborazione della durata indicati negli stessi dalla data di sottoscrizione e potrà essere rinnovato, concordemente tra le parti, solo dopo il preventivo accertamento della permanenza dei presupposti e della sussistenza del reciproco interesse alla proroga. Sono inoltre da ritenersi applicabili tutte le disposizioni vigenti relative all'impiego e all'uso della Modello ATe in ambito Ministero della Difesa e Pubbliche Amministrazioni.
Privacy policy **(Politica sulla riservatezza)**	Subscribers' data are processed by the Ministry of Defence in compliance with the Reg. (UE) 2016/679, also referred to as *"GDPR".*	I dati personali acquisiti per il rilascio della carta sono trattati dal Ministero della Difesa ai sensi del Reg. (UE) 2016/679 detto anche GDPR.
Refund policy	The Ministry of Defence shall not pay any reimbursement.	Il Ministero della Difesa non prevede alcun rimborso.

(Politica per il rimborso)		
Applicable law, complaints and dispute resolution **(Legge applicate, reclami e risoluzione delle dispute)**	In case of dispute in the interpretation or delivery of service, the matter shall be settled in an amicable way. If this is not possible, Rome shall be the competent court.	In caso di controversia nell'interpretazione o esecuzione del servizio, la questione verrà in prima istanza definita in via amichevole. Qualora non fosse possibile, il foro competente sarà quello di Roma
TSP and repository licenses, trust marks, and audit **(TSP e repository delle licenze, marchi e audit)**	Defence keeps a software inventory constantly updated, and every six months monitors the usage trend of licences by systematically collecting information in order to understand their usage and distribution.	La Difesa mantiene costantemente aggiornato un inventario del software in uso e provvede a monitorare semestralmente il trend di utilizzo delle licenze, attraverso una raccolta sistematica di informazioni, al fine di comprenderne l'effettivo utilizzo e la distribuzione.

Firmato Digitalmente da/Signed by:
SERGIO ANTONIO SCALESE

In Data/On Date:
giovedì 16 giugno 2022 15:07:21