POLICY APPLICATA DAL SERVIZIO FIDUCIARIO

La Certification Autority del Ministero della Difesa emette i seguenti tipi di certificati di firma eIDAS:

- firma con limitazioni d'uso [1] – OID 1.3.6.1.4.14031.2.1.1.13 Inserito all'interno della smart card Modello ATe per default;
- 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 Autoremote 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 e i sigilli elettronici devono essere utilizzati solo nelle modalità indicate all'interno del CPS e all'interno del presente documento 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 e i sigilli elettronici 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)

LIMITAZIONI SULL'USO DEI SERVIZI

I Servizi di Certification Autority e di Firma sono offerti a titolo gratuito per i dipendenti del Ministero della Difesa e delle altre P.A. che hanno stipulato un accordo con il Ministero della Difesa.

I limiti d'utilizzo del certificato sono riportati all'interno del CPS e del certificato stesso.

OBBLIGHI DEL SOTTOSCRITTORE

Il Contraente ha l'obbligo di:

- prendere visione del CPS e della normativa in essi citata prima della compilazione del modulo di registrazione;
- fornire all'Operatore di Registrazione, durante la fase di registrazione, informazioni esatte e veritiere ai sensi del D.P.R. n.44/2000 Art.76;
- custodire con la massima diligenza i PIN/codici riservati ricevuti, al fine di preservarne la segretezza;
- avvisare prontamente l'Operatore di Registrazione di ogni variazione delle informazioni fornitegli in fase di registrazione;

[1] Si fa presente che dalla data del 1 Luglio 2017 al 22 Giugno 2020 è stato utilizzato l'OID 1.3.6.1.4.1.14021.2.1.1.13

- in caso di furto o smarrimento del Modello Ate denunciare immediatamente l'accaduto all'organizzazione di appartenenza, facendo seguire copia cartacea della denuncia resa innanzi all'autorità giudiziaria (Polizia o Carabinieri), e chiedere la sospensione o revoca del certificato secondo la procedura descritta nel manuale operativo e nel CPS;
- provvedere all'attivazione della firma (ove previsto);
- prima di cominciare ad utilizzare la chiave privata corrispondente al certificato ottenuto, controllare attentamente che il certificato abbia il profilo previsto e contenga informazioni corrette in ogni suo campo ed estensione, incluse le eventuali limitazioni d'uso;
- astenersi dall'uso della chiave privata, nel caso in cui il corrispondente certificato presenti qualsiasi difformità rispetto alle attese;
- utilizzare la firma digitale solo nell'ambito e con le modalità previste.
- di custodire con la massima diligenza le proprie chiavi private ed i dispositivi di firma che le contengono al fine di preservarne l'integrità e la riservatezza;
- di richiedere immediatamente la revoca delle certificazioni relative alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi;

Il Contraente assume ogni responsabilità in merito alla veridicità dei dati comunicati.

Il Contraente si assume ogni responsabilità per qualsiasi danno possa derivare al Ministero della Difesa o a soggetti terzi dall'aver celato la propria identità, dall'aver dichiarato falsamente di essere soggetto diverso nonché dall'aver fornito informazioni inesatte, garantendo e sollevando sin d'ora il Ministero della Difesa per le conseguenti richieste di risarcimento danni pervenute alla medesima il Ministero della Difesa. Il Contraente dichiara di sollevare il Ministero della Difesa e/o terzi da eventuali pretese avanzate da terzi con riferimento a dichiarazioni, attestazioni false o omissioni del medesimo in relazione alla propria identità.

INFORMAZIONI PER LE PARTI INTERESSATE

Il Ministero della Difesa è titolare del trattamento dei dati forniti dal Titolare con la compilazione della Richiesta per il rilascio del modello ATE o di certificato di Firma Automatica e/o Remota.e Sigillo Elettronico, informa il Titolare stesso, ai sensi e per gli effetti di cui al Reg. (UE) 2016/679 (GDPR), che tali dati personali saranno trattati mediante archivi cartacei e strumenti informatici e telematici, idonei a garantirne la sicurezza e la riservatezza nel rispetto delle modalità indicate nel succitato Decreto e degli obblighi di riservatezza.

In relazione ai predetti trattamenti dei dati, il Titolare potrà esercitare i diritti di cui previsti dagli art. dal 15 al 21 del Reg. (UE) 2016/679 (GDPR)".

CONSERVAZIONE DEGLI EVENTI DI LOG

I principali eventi relativi alla gestione del ciclo di vita dei certificati, incluse le richieste di certificazione, sospensione o revoca, ecc, sono registrati in forma cartacea od elettronica. Sono inoltre registrati anche altri eventi quali: gli accessi logici al sistema di gestione dei certificati, le operazioni svolte dal personale del Ministero della Difesa, l'entrata e l'uscita di visitatori nei locali in cui si svolge l'attività di certificazione, ecc.

Di ogni evento viene registrata la tipologia, la data e l'ora di occorrenza e, se disponibili, altre informazioni utili ad individuare gli attori coinvolti nell'evento e l'esito delle operazioni.

L'insieme delle registrazioni costituisce il "giornale di controllo" (audit log). I file che lo compongono vengono trasferiti periodicamente su supporto permanente e vengono conservati per 20 anni.

LIMITAZIONI DI RESPONSABILITÀ

Il Ministero della Difesa declina ogni responsabilità per gli eventuali danni sofferti dal personale a causa della mancata ricezione delle comunicazioni della CA di

Firma in conseguenza di un errato indirizzo di e-mail fornito in fase di richiesta.

LIMITI AL RISARCIMENTO DANNI

Nella misura consentita dalla legge, il Ministero della Difesa non può garantire tutto ciò che è indicato nel presente contratto quando uno o più eventi di forza maggiore si verifichino.

Per eventi considerati di "forza maggiore" si intendono guerre, atti di terrorismo, disastri naturali, guasti alle apparecchiature per la fornitura di energia o guasti della rete Internet o ad altre infrastrutture.

SISTEMA LEGALE APPLICABILE

Il presente contratto è soggetto alla legge italiana e come tale sarà interpretato ed eseguito

RISOLUZIONE DELLE CONTESTAZIONI E DELLE DISPUTE

Per ogni eventuale controversia e disputa il Foro competente è quello di Roma.

VALUTAZIONE DI CONFORMITÀ

La Certification Authority del Ministero della Difesa e la relativa struttura di PKI è stata valutata conforme allo standard indicato nel 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*.

A seguito dell'ispezione di Conformità eseguita da uno dei CAB Italiani, la struttura di PKI del Ministero della Difesa è stata accreditata presso AgID.

INFORMAZIONI DI CONTATTO

Soggetto Giuridico: STATO MAGGIORE DELLA DIFESA - Comando per le Operazione in Rete.
Via: Stresa 31b 00135 Roma
Codice Fiscale: 97355240587
ISO Object Identifier: 1.3.6.1.4.1.14031
Indirizzo di Posta Elettronica: info_pkiff@smd.difesa.it
Recapito Telefonico: +39 06 46914444
Sito Web: https://pki.difesa.it/tsp

DISPONIBILITÀ

I servizi di Certification Authority offerti dal Ministero della Difesa sono disponibili h24, 7 giorni su 7. Per quanto riguarda la disponibilità inerente l'informazione sullo stato di revoca dei certificati dopo il loro periodo di validità il certificatore si impegna a renderla disponibile secondo quanto indicato nel documento CPS al paragrafo 4.10

Gen. Div. AAran Sandro SANASI	Prestatore di Servizi Fiduciari Qualificati (QTSP)	*Firmato Digitalmente da/Signed by:* **SANDRO SANASI** *In Data/On Date:* **venerdì 28 marzo 2025 16:24:56**