LINEE GUIDA

PER IL RILASCIO DELL'IDENTITA' DIGITALE DIFESA AL PERSONALE CHE PRESTA ATTIVITA' LAVORATIVA PRESSO L'A.D. IL CUI STATO GIURIDICO NON RIENTRA TRA QUELLI PREVISTI DAL DPR 28 LUGLIO 1967, N. 851

EDIZIONE 2021

Pagina intenzionalmente bianca

STATO MAGGIORE DELLA DIFESA

Dirigente Generale responsabile per la transizione al digitale

VISTO il D.Lgs. 7 marzo 2005 n. 82 e successive modificazioni, recante il "Codice dell'amministrazione digitale" e, in particolare, l'articolo 17, rubricato "Responsabile per la transizione digitale e difensore civico digitale", che ai commi da 1 a 1-*quinquies*, stabilisce che:

- le pubbliche amministrazioni garantiscano l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione definite dal Governo affidando a un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, la transizione alla modalità operativa digitale nonché la cura di tutti i conseguenti processi di riorganizzazione;
- tale ufficio dirigenziale generale presso le singole amministrazioni è dotato di adeguate competenze tecnologiche, di informatica giuridica e manageriali e risponde delle proprie specifiche attività direttamente al vertice politico;
- le Forze Armate, compresa l'Arma dei carabinieri, il Corpo delle capitanerie di porto e i Corpi di polizia hanno facoltà di individuare propri uffici senza incrementare il numero complessivo di quelli già previsti nei rispettivi assetti organizzativi;
- presso l'Agenzia per l'Italia Digitale è istituito l'ufficio del difensore civico per il digitale a tutela dei diritti di cittadinanza digitali previsti dal Codice dell'amministrazione digitale.

VISTO il Decreto del Ministro della Difesa 18 settembre 2020, di aggiornamento mediante sostituzione del DM 8 novembre 2011, concernente individuazione, compiti e funzioni del Responsabile per la transizione digitale (RTD) del Dicastero della difesa, ai sensi dell'art. 17 del Codice dell'amministrazione digitale recato dal D.Lgs. 7 marzo 2005, n. 82 e successive modificazioni.

VISTA la Direttiva SMD-I-020 del 27 dicembre 2009, concernente "L'attuazione delle Disposizioni del Dirigente Generale Responsabile per i sistemi informativi dell'Amministrazione della Difesa (D.G.Re.S.I.A.D.) in aderenza alle politiche governative in materia di informatizzazione della pubblica amministrazione e norme applicative in materia di trattamento dei dati personali", quale referente dell'Ag.I.D. e del Ministro della Difesa che, fra l'altro:

a. individua le criticità dei dati da proteggere;

b. definisce le misure fisiche, logiche e procedurali da adottare nei vari contesti operativi, sulla base dell'analisi del rischio, adottando tutte le misure idonee per prevenire l'utilizzo non corretto della rete e dei servizi di rete;

c. svolge attività di coordinamento per la prevenzione e il contrasto di incidenti che possano portare alla sottrazione, alterazione, cancellazione dei dati o interruzione del servizio;

d. rende note le procedure di informatizzazione agli utenti della propria struttura e, se necessario, stabilisce ulteriori disposizioni per i servizi con validità interna alla struttura, conformemente ai regolamenti dell'A.D. e a quanto stabilito dalla normativa vigente;

e. espleta tutti i propri compiti coordinandosi:

(1) con il Comando per le Operazioni in Rete per l'area centrale della Difesa;

(2) con i Referenti dei Sistemi Informativi Automatizzati nell'ambito degli Stati Maggiori di Forza Armata, che operano secondo le direttive e le procedure impartite dal Dirigente Generale Responsabile per la transizione al digitale/RTD e sono responsabili della loro applicazione,

A D O T T O

le presenti Linee Guida *"per il rilascio dell'identità digitale Difesa al personale che presta attività lavorativo presso l'A.D. il cui stato giuridico non rientri tra quelli previsti dal dPR 28 luglio 1967, n. 851.* - Edizione 2021**.**

Roma, lì _____

Il Dirigente Generale
responsabile per la transizione al digitale/RTD

Gen. D.A. Enrico DEGNI

ELENCO DI DISTRIBUZIONE

ENTE/COMANDO	N° COPIE	
	STAMPA	SW
Diramazione Esterna		
STATO MAGGIORE ESERCITO		1
STATO MAGGIORE MARINA		1
STATO MAGGIORE AERONAUTICA		1
SEGRETARIATO GENERALE DIFESA E DIREZIONE NAZIONALE DEGLI ARMAMENTI		1
COMANDO OPERATIVO DI VERTICE INTERFORZE		1
COMANDO PER LE OPERAZIONI IN RETE		1
CENTRO ALTI STUDI DELLA DIFESA		1
COMANDO INTERFORZE PER LE OPERAZIONI DELLE FORZE SPECIALI		1
COMANDO DELLE OPERAZIONI SPAZIALI		1
ISPETTORATO GENERALE DELLA SANITA' MILITARE		1
RAGGRUPPAMENTO AUTONOMO DEL MINISTERO DELLA DIFESA		1
CIRCOLO UFFICIALI DELLE FORZE ARMATE D'ITALIA		1
UFFICIO GENERALE PRE.V.A.T.A		1
UFFICIO GENERALE SPAZIO		1

Diramazione Interna		
UFFICIO GENERALE DEL CAPO DI SMD		1
DIPARTIMENTO PUBBLICA INFORMAZIONE E COMUNICAZIONE		1
UFFICIO DEL SOTTOCAPO DI SMD		1
I REPARTO – PERSONALE		1
II REPARTO – INFORMAZIONI E SICUREZZA		1
III REPARTO – POLITICA MILITARE E PIANIFICAZIONE		1
IV REPARTO – LOGISTICA E INFRASTRUTTURE		1
V REPARTO – AFFARI GENERALI		1
UFFICIO GENERALE PIANIFICAZIONE PROGRAMMAZIONE E BILANCIO		1
UFFICIO GENERALE AFFARI GIURIDICI		1
UFFICIO GENERALE DI AMMINISTRAZIONE		1
UFFICIO PROTOCOLLO UNICO		1
COMANDO CC PM DELLO SMD		1

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI

Nr. Variante	Nr. Protocollo e data della variante	Data registrazione	Grado, cognome, nome e firma di chi apporta la variante
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

INDICE

Elenco degli Annessi alla Direttiva

1. PREMESSA

Il modello ATe emesso dalla Difesa risponde al quadro normativo di riferimento per il rilascio delle tessere di riconoscimento rilasciate dalle amministrazioni dello Stato con modalità elettroniche. Per tale motivo, il modello ATe può essere rilasciato al solo personale in possesso dei requisiti previsti dal d.P.R. 28 luglio 1967, n. 851[1].

Il progetto CMD si inquadra, però, nel più ampio programma d'iniziative intraprese dal Comparto, finalizzate a dotarsi di strumenti elettronici di autenticazione e di identificazione in rete che consentono l'accesso a servizi *online* della Difesa.

In tale ambito, per il personale che presta una attività lavorativa a favore della Difesa (esempio supporto specialistico comparto industriale, *contractors* presso le Addettanze, ecc.) non rientrante tra quelli definiti dal d.P.R. 28 luglio 1967, n. 851 e che necessita di impiegare servizi e sistemi informativi propri della Difesa il cui accesso è possibile solo attraverso il possesso di una identità digitale su un supporto tipo smart card, è stata predisposta una specifica procedura all'interno del Portale CMD[2] che potrà essere utilizzata per richiedere il rilascio di un certificato di autenticazione Difesa equipollente per caratteristiche tecniche alla Carta Nazionale dei Servizi (CNS) presente in tutti i modelli ATe ma riconosciuto funzionalmente unicamente in ambito Difesa. In alcuni casi specifici, su esplicita richiesta dell'interessato e la cui necessità dovrà essere avallata dall'Ente richiedente, potrà essere rilasciato anche un certificato firma digitale il cui utilizzo sarà limitato alla sola attività lavorativa svolta a favore della Difesa.

I certificati in parola saranno inseriti all'interno di un supporto tipo *smart card* avente caratteristiche tecniche e di sicurezza[3] identiche a quelle del modello ATe prodotto dall'Istituto Poligrafico Zecca dello Stato (IPZS).

2. REQUISITI PER RICHIEDERE IL RILASCIO DEL SUPPORTO

La richiesta di emissione del supporto potrà essere esperita a favore del personale che non appartiene al dicastero della Difesa e che ha con una articolazione di quest'ultimo un rapporto lavorativo non inferiore ai 12 mesi continuativi. Nella richiesta per l'emissione del supporto dovrà essere sempre indicata:

- l'attività lavorativa svolta presso l'A.D. (esempio frequentatore di corso, supporto specialistico, medico);
- la tipologia dei sistemi informativi e dei servizi informatici a cui il personale dovrà accedere ovvero per il controllo automatizzato della presenza all'interno di un sedime militare;
- la durata del rapporto di impiego che non dovrà essere inferiore ai 12 mesi continuativi ad eccezione del personale frequentatore di corsi presso gli istituti di formazione della Difesa.

I certificati digitali inseriti nel supporto potranno essere impiegati per la sola attività lavorativa e tutte le azioni con essi svolte dovranno essere strettamente aderenti alle *policy* di utilizzo adottate in ambito Difesa ed essere soggette a costante controllo da parte degli Enti presso i quali il personale presta la propria attività lavorativa.

---

1 Ai dipendenti civili dello Stato di ruolo e non di ruolo, in attività di servizio ed in quiescenza, nonchè ai militari, in attività di servizio ed in quiescenza.

2 http://portalecmd.difesa.it/sezione_ate/redirect.aspx

3 Il chip ed il sistema operativo sono certificati *Common Criteria* EAL5+. Ciò realizza il livello più elevato di certificazione di sicurezza richiesto in Europa per le smartcard usate per la firma digitale.

Al termine dell'esigenza, i supporto dovranno essere ritirati e revocati tramite il Portale CMD a cura dell'Ente richiedente e restituiti al *Card Management System* Unico (CMS) per la successiva distruzione.

Per ogni ulteriore indicazione non esplicitata nelle presenti linee guida si dovrà fare riferimento alla direttiva SMD-I-009[4].

3. POSSESSORE DEL SUPPORTO DI AUTENTICAZIONE RILASCIATO DALLA DIFESA

Il possessore del supporto dovrà:

- prendere visione della documentazione relativa all'attuazione della disciplina in materia di utilizzo dei certificati digitali e di protezione dei dati adottati dalla Difesa;
- prendere visione dell'informativa ai sensi dell'art.13 del Reg. (UE) 2016/679 (GDPR) sull'attività di raccolta dei dati personali predisposta in **Annesso 1** alle presenti linee guida;
- custodire il codice di emergenza della carta, unico e non replicabile e valido per 10 anni, necessario per il recupero dei segreti della carta[5] e le comunicazioni di smarrimento ovvero furto;
- conservare il supporto in modo conforme alle presenti linee guida al fine di non comprometterne il corretto e sicuro utilizzo;
- utilizzare il supporto solo sulle postazioni di lavoro dell'Amministrazione della Difesa;
- custodire segretamente i codici necessari all'autenticazione e all'apposizione della firma digitale dei quali è l'unico responsabile dal punto di vista legale;
- approntare le adeguate contromisure in caso di furto, smarrimento o compromissione del supporto, segnalando immediatamente l'evento all'Ufficio preposto dell'Ente presso il quale fornisce le propria prestazione lavorativa e, successivamente, presentando formale denuncia agli organi di polizia preposti;
- al termine del periodo di prestazione dell'attività lavorativa svolta presso la Difesa, restituire il supporto all'Ente di impiego.

In caso di recidività ovvero grave inosservanza da parte del possessore del supporto nella gestione e nell'utilizzo dello stesso è fatto divieto all'Ente di richiedere una nuova emissione.

4. DESTINATARI DEL SUPPORTO

Il supporto tipo smart card contente l'identità digitale Difesa del possessore, può essere rilascio al personale che presta attività lavorativa presso una articolazione della Difesa per un periodo non inferiore a 12 mesi, ad eccezione del personale frequentatori di corsi presso gli istituti di formazione della Difesa per i quali tale limite può essere ridotto in funzione della reale esigenza, e che non è in possesso dei requisiti previsti dal d.P.R. n. 851 del 1967.

La richiesta di emissione del supporto contente l'identità digitale può avvenire:

- nel momento in cui nuove risorse umane sono chiamate a prestare una attività lavorativa presso l'A.D.;
- nei casi in cui sussiste la necessità di fornire al personale in parola un nuovo supporto perché scaduto, con chip inefficiente ovvero revocato; in quest'ultimo caso dovrà essere verificata la

---

4 Direttiva SMD-I-009 "Procedure per il rilascio in formato elettronico della tessera personale di riconoscimento modello ATe e dei certificati digitali emessi dalla *Public Key Infrastructure* (PKI) della Difesa" (Edizione 2020).

5 *https://portalecmd.difesa.it/Activation/ActivationNG.aspx*

recidività del richiedente.

In particolare, il supporto potrà essere rilasciato ai seguenti soggetti:

- personale dell'Arma dei carabinieri impiegato presso gli enti interforze della Difesa e che necessita di utilizzare un certificato di autenticazione Difesa e/o di firma digitale per poter interagire con i sistemi informativi e i servizi informatici della Difesa;
- personale che per prestare la propria attività lavorativa ha necessità di accedere ai sistemi informativi e ai servizi informatici della Difesa;
- contrattisti civili che per la tipologia di attività lavorativa svolta a favore delle articolazioni della Difesa necessitano di utilizzare il sistema di controllo accessi;
- personale medico esterno che presta la propria attività a favore dell'A.D..

Il supporto potrà essere richiesto anche per esigenze non espressamente indicate nelle presenti linee guida ma dovranno essere preventivamente autorizzate dal VI Reparto dello Stato Maggiore della Difesa.

Il supporto dovrà essere ritirato e revocato a cura dell'Ufficio/Sezione Personale dell'EDRC dove il personale presta servizio per essere poi consegnato alla LRA di competenza che provvederà alla sua restituzione al CMS unico per la successiva distruzione, nei seguenti casi:

- scadenza del rapporto di lavoro con la Difesa;
- adozione di un provvedimento cautelare a norma delle disposizioni vigenti;
- inosservanza delle *policy* di utilizzo adottate dalla Difesa.

5. PKI - LA FUNZIONE DI FIRMA DIGITALE E DI AUTENTICAZIONE DIFESA

L'Infrastruttura a chiave Pubblica della Difesa (PKI) ospitata presso il CORDIFESA - Ente di Certificazione accreditato presso l'Ag.ID - fornirà al supporto due certificati digitali di:

- firma digitale con limitazione d'uso;
- autenticazione DIFESA.

Il certificato di Firma Digitale, garantisce l'autenticità della sottoscrizione, l'integrità del documento e la non ripudiabilità da parte del possessore del supporto. Per il personale indicato nelle presenti linee guida, un documento firmato con firma digitale di che trattasi (rilasciato con limitazione all'attività di servizio), pur rispettando tutti i requisiti dell'art. 24 del CAD e, quindi, avendo pieno valore legale opponibile a terzi nell'ambito di impiego, non ha però l'efficacia prevista dall'art. 2702 del Codice Civile (efficacia della scrittura privata), essendo specificato all'interno del certificato la limitazione summenzionata.

Il certificato di Autenticazione DIFESA consente al possessore del supporto di essere "riconosciuto in rete" con assoluta certezza e, quindi, permettergli di accedere ai servizi della Difesa. Il certificato di autenticazione Difesa non è supportato per l'accesso ai servizi *on-line* delle Pubbliche Amministrazioni e per i quali è richiesto un accesso a mezzo "*strong authentication*" (Es. servizi per il cittadino esposti su alcuni siti istituzionali delle Pubbliche Amministrazioni centrali e locali).

I certificati digitali verranno installati su due tipologie di supporto fisico denominate "carte bianche":

- Carta Bianca con chip non certificato, per il rilascio del solo certificato di Autenticazione Difesa;
- Carta Bianca con chip certificato, per il rilascio del certificato di Autenticazione Difesa e del certificato di Firma Digitale con limitazione d'uso.

Il Certificatore Accreditato dall'Ag.ID, responsabile della conduzione, della sicurezza, dell'operatività dell'infrastruttura tecnologica e del sistema di certificazione, è identificato nello:

STATO MAGGIORE DIFESA - Comando per le Operazioni in Rete - Via Stresa, 31 B - 00135 Roma.

In considerazione della particolarità dei servizi offerti e delle possibili implicazioni legali cui si potrebbe incorrere a seguito dell'utilizzo improprio dei certificati digitali, ogni possessore del supporto è tenuto a prendere visione e approfondire gli aspetti inerenti la firma digitale e l'autenticazione Difesa attraverso la consultazione dei Manuali Operativi e degli avvisi agli utenti resi disponibili dal Certificatore all'indirizzo:

http://cor.difesa.it/Sistemi/CertificazioneConservazione/Pagine/default.aspx

o, in alternativa, sul sito dell'Ag.ID:

https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/prestatori-di-servizi-fiduciari-attivi-in-italia

All'interno dei Manuali Operativi, infatti, l'utente può approfondire tutti gli argomenti correlati al corretto utilizzo dei certificati digitali, quali:

- procedure per apporre una firma digitale (predisposizione client e software);
- tipologie di firma digitale (CAdES, PAdES, XAdES e ASiC);
- procedura per apporre una marcatura temporale e sua importanza;
- modalità di verifica della validità di una firma digitale (Certificate Revocation List/CRL – Online Certificate Status Protocol/OCSP);
- modalità per il rilascio, la sospensione e la revoca dei certificati digitali;
- obblighi del Certificatore, dei titolari e dei terzi interessati.

6. PROCEDURE DI ACQUISIZIONE DATI E RILASCIO DEL SUPPORTO CONTENENTE I CERTIFICATI DIGITALI

La procedura di acquisizione dei dati (*enrollment*), avviene presso i Locali Centri di Registrazione[6] (***Local Registration Authority*** - LRA) predisposti dalle F.A. e abilitati dal Comando per le Operazioni in Rete [7] previa nomina del personale autorizzato alla validazione e di quello autorizzato al trattamento[8] dei dati. La procedura può avere inizio solo dopo la presentazione della richiesta cartacea (Annesso 1) debitamente compilata dal richiedente e attestata dalla firma del Comandante di Corpo/Delegato dell'Ente presso cui il personale presta la propria attività lavorativa.

Il personale autorizzato alla validazione dei dati, effettuata l'identificazione del richiedente attraverso l'esibizione di un documento di riconoscimento in corso di validità, provvede:

- prima dell'inizio del trattamento (cioè antecedente alla fase di *enrollment*), a far prendere visione al richiedente, in modalità certa attraverso la verifica della presenza della firma sull'Annesso 1, dell'informativa specifica relativa all'utilizzo dei dati personali che dovrà essere accettata dal richiedente pena l'impossibilità di procedere con la procedura di emissione del supporto;

6 La soppressione/creazione di una LRA deve essere preventivamente formalizzata al Certificatore (CORDIFESA).
7 Elenco LRA attive: http://portalecmd.difesa.it/
8 Decreto legislativo 10 agosto 2018, n. 101 "Codice in materia di protezione dei dati personali", art. 2-quaterdecies.
28 Che potrebbe essere anche di un soggetto diverso dal genitore.
29 Art. 330 del codice civile "decadenza dalla responsabilità genitoriale sui figli".

- all'acquisizione dei dati anagrafici (nome, cognome, data di nascita, comune di nascita, codice fiscale), attraverso specifiche procedure, oltre alla email di servizio ovvero privata e numero telefonico per l'invio delle comunicazioni legate al supporto;
- alla conferma da parte del richiedente, con firma grafometrica (nome e cognome) leggibile, dei dati raccolti;
- a convalidare i dati raccolti controfirmandoli con la propria firma digitale.

Terminata la procedura d'inserimento, il personale della LRA autorizzato alla validazione dei dati convalida l'acquisizione attraverso un'apposita procedura di approvazione apponendo la propria firma digitale; la procedura si conclude contestualmente all'opposizione della firma digitale con l'invio della richiesta di emissione al CMS.

Per tutti i casi non esplicitati nelle presenti linee guida, si rimanda alla direttiva SMD-I-009 e alle normative vigenti in materia di rilascio dei documenti d'identità e dei documenti validi per l'espatrio.

7. SOSPENSIONE DEL SUPPORTO E DEI CERTIFICATI DIGITALI

I possibili eventi che possono portare alla sospensione del supporto sono:

- la verifica sulle alterazioni del supporto "logico" (ovvero delle componenti elettroniche – chip, con conseguente malfunzionamento o indisponibilità dei dati e/o dei certificati contenuti all'interno del supporto: ad es. impossibilità di accedere alle funzioni di firma digitale e/o errore nell'accesso ai servizi/sistemi informativi della Difesa con relativa mancata operatività della carta, ecc.);
- sospetto smarrimento del documento. A riguardo, entro il termine massimo di 10 giorni l'interessato deve confermare/annullare l'avvenuto smarrimento. In caso di conferma, contestualmente alla procedura di acquisizione, deve essere presentata presso la LRA anche copia della denuncia di smarrimento;
- furto/compromissione dei codici PIN e PUK: contestualmente alla procedura di acquisizione deve essere presentata presso la LRA anche copia della denuncia di furto;
- provvedimento di sospensione cautelare obbligatoria a norma delle disposizioni vigenti;
- uso improprio del supporto da parte dell'interessato.

La sospensione dei certificati digitali è istanziata ogni qual volta risulti necessario verificare la persistenza di tutti i requisiti di sicurezza previsti dalle norme. La sospensione porta a una temporanea invalidità dei certificati presenti sulla carta.

Al termine del periodo di sospensione, la cui durata è di volta in volta fissata dal Certificatore a seconda delle circostanze e delle motivazioni a contorno, i certificati digitali possono essere:

- RIATTIVATI: i certificati tornano a essere validi e sono considerati come mai sospesi;
- REVOCATI: i certificati non sono più validi a far data dall'inizio del periodo di sospensione.

8. REVOCA DEL SUPPORTO E DEI CERTIFICATI DIGITALI

Il processo di revoca è avviato per termine del rapporto di lavoro con l'amministrazione della Difesa, smarrimento, furto, compromissione dei certificati digitali, ovvero quando vi è un utilizzo del supporto non conforme agli scopi e ai metodi di utilizzo previsti dalle presenti linee guida, dalla direttiva SMD-I-009 e/o dal quadro normativo in materia in vigore al momento dell'evento. La compromissione, in modo particolare, prevede la revoca dei certificati perché espone il supporto e i dati in esso contenuti, al rischio di corruzione e/o manipolazione.

Il processo di revoca consiste nella disattivazione permanente di uno o più dei certificati contenuti nel supporto. Tale processo è irreversibile e può essere preceduto da un periodo di sospensione, utilizzato dal Certificatore per condurre le previste verifiche.

La responsabilità dell'attivazione del processo di revoca durante il periodo di sospensione è a carico dell'Ente dove il personale presta la propria attività lavorativa. In caso di revoca, il supporto deve essere ritirato a cura della LRA e consegnato per la distruzione al CMS.

9. REVOCA PER FURTO/SMARRIMENTO

In caso di furto/smarrimento, l'interessato deve dare immediata comunicazione all'Ente dove presta la propria attività lavorativa. Qualora ciò non sia possibile, l'interessato deve contattare il numero telefonico 0646914444 (Comando per le Operazioni in Rete) richiedendo all'operatore la **sospensione** immediata del supporto. Inoltre, l'interessato deve presentare formale denuncia alle autorità competenti entro le 24 ore successive alla comunicazione, consegnando copia della documentazione alla LRA. Copia della denuncia dovrà essere custodita dall'Ente dove il personale presta la propria attività lavorativa che avrà comunque l'obbligo di trasmettere al CMS i riferimenti della pratica di smarrimento. Qualora non ci siano ulteriori comunicazioni, trascorsi 15 giorni il supporto dovrà essere revocato.

10. MODALITÀ DI FUNZIONAMENTO DELLA PROCEDURA INFORMATIZZATA PER IL RILASCIO DEL SUPPORTO

a. Prima dell'inizio del trattamento, antecedente alla fase di *enrollment,* il personale richiedente dovrà prendere visione sia sul portale CMD che nell'Annesso 1, dell'informativa specifica relativa all'utilizzo dei dati personali, in particolare:

   - che i dati personali in argomento sono acquisiti esclusivamente per consentire al Ministero della Difesa di rilasciare un supporto tipo smart card contenete una identità digitale Difesa secondo le specifiche previste dai dPCM del 24 maggio 2010 e del 18 gennaio 2016 "Regole tecniche delle Tessere di riconoscimento (mod. AT) di cui al d.P.R. n. 851 del 1967 rilasciate con modalità elettronica dalle Amministrazioni dello Stato, ai sensi dell'articolo 66, comma 8, del decreto legislativo n. 82 del 2005 e ss.mm.;
   - in caso di un eventuale rifiuto al trattamento di tali dati, il Ministero della Difesa non potrà emettere il supporto con conseguente limitazione per il personale all'autenticazione nelle reti della Difesa necessario a garantire l'accesso sicuro ai sistemi informativi;
   - all'interessato sono riconosciuti i diritti previsti dagli artt. da 15 a 21 del Reg. (EU) 679/2016 relativi ai propri dati;
   - il Titolare del trattamento dei dati è lo Stato Maggiore della Difesa, con sede in Via XX Settembre, 8 – 00100 Roma.

b. Il sistema di acquisizione dei dati per il rilascio del supporto (anagrafici e generici) prevede un sottosistema di "*Enrollment*", le cui funzionalità sono accessibili solo presso le *Local Registration Authority* (LRA), dove opera personale preventivamente nominato dal Comandante di Corpo/Responsabile dell'EDRC con atto formale. La raccolta dei dati avviene tramite un portale *web* unico a cui può accedere il solo personale abilitato preventivamente censito all'interno del sistema.

   Il *Card Management System* unico (CMS), preposto all'emissione (stampa) del supporto, espone via web il servizio di acquisizione, attraverso il quale vengono raccolti i dati del personale (anagrafici e generici) e scritti all'interno del *filesystem* del supporto. Durante il processo di emissione del supporto, il CMS si interfaccia con le *Certification Authority* (C.A.)

della Difesa, per il rilascio del certificato di autenticazione Difesa e di firma digitale.

La sicurezza minima richiesta nello scambio dei dati è garantita tramite l'impiego delle funzionalità erogate da una infrastruttura proprietaria della Difesa a chiave pubblica, certificata dall'Ag.ID.

ANNESSO 1

MODULO RICHIESTA SUPPORTO DIGITALE

DICHIARAZIONE SOSTITUTIVA DI CERTIFICAZIONE

(resa ai sensi del DPR 445/2000 per il rilascio del modello ATe, art 46 [1])

VALIDA AI FINI DEL RILASCIO DEL SUPPORTO CONTENENTE I CERTIFICATI DIGITALI EMESSI DALLA DIFESA.

Il/la sottoscritto/a _____
(COGNOME) (NOME)

Ente/società di appartenenza _____ Codice fiscale _____

Presta la sua attività lavorativa per l'A.D. presso _____ Tel. Uff. _____

Data assunzione in servizio ___/___/____ scadenza vincolo ___/___/____ .

DICHIARO/A QUANTO SEGUE:

DATI ANAGRAFICI

Nato/a a _____ Prov. di (_____) il ___/___/____

Residente a _____ Prov. di (_____) c.a.p. _____

Via/piazza _____ nr. _____

DATI AMMINISTRATIVI

Ditta di appartenenza _____

Incarico_____

Account email _____@_____

Timbro lineare del Comando/Ente	Timbro tondo	Timbro e firma del Comandante di Corpo/Delegato dell'Ente

1 Articolo 46 (R) Dichiarazioni sostitutive di certificazioni. Sono comprovati con dichiarazioni, anche contestuali all'istanza, sottoscritte dall'interessato e prodotte in sostituzione delle normali certificazioni i seguenti stati, qualità personali e fatti: … omissis …z. tutti i dati a diretta conoscenza dell'interessato contenuti nei registri dello stato civile;… omissis …

SEGUE ANNESSO 1

Il sottoscritto dichiara inoltre:

a. Di aver preso visione e conoscere il contenuto della Direttiva SMD-I-009 "Procedure per il rilascio in formato elettronico della tessera personale di riconoscimento Modello ATe e dei certificati digitali emessi dalla *Public Key Infrastructure* (PKI) della Difesa.

a. Di aver preso visione e conoscere il contenuto delle Linee Guida per richiedere il rilascio di un supporto per l'autenticazione ai servizi e sistemi informativi della Difesa al personale che presta una attività lavorativo presso l'A.D. e il cui stato giuridico non rientri tra quelli previsti dal dpr 28 luglio 1967, n. 851.

b. Di aver preso visione dei documenti *"Condizioni generali di contratto"* e *"PKI Disclosure Statement"* della CA di Firma Digitale e della CA di Marcatura Temporale, disponibili sul sito web https://pki.difesa.it/tsp e di accettarne le condizioni e i propri obblighi.

c. Di essere responsabile penalmente della non veridicità dei dati forniti, ai sensi del D.P.R. n. 445/2000 art.76.

d. Di aver preso visione ed autorizzato tramite il Portale CMD il trattamento dei propri dati personali finalizzato al rilascio del supporto e che gli stessi saranno conservati per il periodo necessario alla gestione del ciclo di vita dei certificati digitali inseriti sullo stesso.

e. Di essere a conoscenza che la propria chiave privata di Firma Digitale viene immagazzinata su un dispositivo crittografico (*smart card*) sicuro e certificato secondo la normativa vigente.

f. Di mantenere il controllo esclusivo delle credenziali (PIN/PUK) per l'utilizzo della chiave privata e del codice di emergenza e di non cederle a soggetti terzi.

g. Di consentire al mantenimento presso il *Qualified Trust Service Provider* (QTSP) delle informazioni usate durante la registrazione e delle informazioni riguardo la propria identità. Dichiara inoltre di consentire che queste informazioni siano passate a un altro soggetto solo nel caso il QTSP attuale termini i propri servizi.

h. Di autorizzare il trattamento dei propri dati personali, ai sensi del Reg. (UE) 2016/679 (GDPR).

i. Di essere a conoscenza che il proprio certificato viene pubblicato sui servizi di *directory online* interni al QTSP a norma di legge.

j. Di attivarsi tempestivamente entro 24 ore nel caso di sospetta compromissione della propria chiave privata e/o delle credenziali di utilizzo, (smarrimento o furto del supporto) al fine di sospendere il certificato corrispondente, per poi finalizzare la revoca.

_____ , lì ___/___/_____ _____

(LUOGO) (DATA) (FIRMA DEL DICHIARANTE)

SEGUE ANNESSO 1

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI AI SENSI DELL'ART.13 DEL REG. 8UE9 2016/679 GDPR E DEL D.LGS 101/2018

a. Il Titolare del trattamento dei dati è lo Stato Maggiore della Difesa, con sede in Via XX Settembre, 8 -00100 Roma raggiungibile al seguente indirizzo di posta certificata: stamadifesa@postacert.difesa.it come reso noto sul sito istituzionale www.difesa.it .

b. Il coordinatore delle attività di trattamento è il Comandante del Comando per le Operazioni in Rete, con sede in Via Stresa, 31 B - 00135 Roma.

c. Ai sensi dell'Art. 13 del Regolamento europeo (UE) 2016/679 (di seguito Regolamento), si informa la S.V., in qualità di Interessato, che il trattamento dei dati personali da lei forniti o, comunque, acquisiti nel corso dello svolgimento delle attività di competenza, è finalizzato esclusivamente all'espletamento delle attività istituzionali del Dicastero. Il trattamento dei dati personali avviene a cura del personale a ciò appositamente autorizzato, ai sensi delle vigenti disposizioni impartite dal Titolare del trattamento, con l'utilizzo di procedure anche informatizzate e con l'ausilio di apposite banche-dati automatizzate, nei modi e nei limiti necessari per il perseguimento delle finalità per cui gli stessi sono raccolti e/o successivamente trattati; ciò anche nel caso di eventuale comunicazione a terzi che si renda necessaria, ai sensi della normativa vigente.

d. Il Responsabile della protezione dei dati per il Ministro della Difesa può essere contattato ai seguenti recapiti e-mail: rpd@difesa.it; indirizzo di posta elettronica certificata: rdp@postacert.difesa.it, come reso noto sul sito istituzionale www.difesa.it.

e. I dati personali in argomento **sono rilevati esclusivamente per consentire al Ministero della Difesa di rilasciare un supporto** secondo le specifiche previste dal D.P.C. 24 maggio 2010 "Regole tecniche delle Tessere di riconoscimento (mod. AT) di cui al D.P.R. n. 851 del 1967 rilasciate con modalità elettronica dalle Amministrazioni dello Stato, ai sensi dell'articolo 66, comma 8, del D.Lg. n. 82 del 2005 e per i seguenti impieghi autorizzati dal Ministero della Difesa, secondo le specifiche previste dalla SMD_I_024 "Procedure sulla gestione in sicurezza dei servizi informatici non classificati dell'A.D", dall'art. 7 Legge 244/2007 e dal DCPM 22 febbraio 2013 "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche":

- identificazione in rete dell'intestatario del supporto ai servizi informatici del Ministero;
- rilevamento elettronico delle presenze lavorative;
- firma digitale dei documenti con limitazione all'attività di servizio.

f. I dati personali sono trattati dal Titolare del trattamento nell'esecuzione dei rispettivi compiti istituzionali, di interesse pubblico o, comunque, connessi all'esercizio dei pubblici poteri

conferiti loro dall'Ordinamento, ai sensi dell'articolo 6, paragrafo 1, lettera e) del Regolamento.

g. La base giuridica del trattamento, ai sensi del citato articolo 6, paragrafo 1, lettera e) del Regolamento, è costituita dal D.Lgs. n. 165/2001, dal C.C.N.L. del Comparto Funzioni Centrali, dal D.Lgs. n. 66/2010, concernente "Codice dell'ordinamento militare" e s.m.i. e dal D.P.R. n. 90/2010, recante "Testo Unico delle disposizioni regolamentari in materia di Ordinamento Militare" e s.m.i.. Il trattamento dei dati personali, è finalizzato esclusivamente all'espletamento delle attività istituzionali del Titolare del trattamento, a cura dei soggetti autorizzati e con utilizzo di documentazione e archivi analogici/digitali, di procedure anche informatizzate e di banche-dati, nei modi e nei limiti necessari per il perseguimento delle finalità per cui i dati stessi sono stati trattati.

h. I dati personali potranno essere comunicati alle Amministrazioni pubbliche interessate allo svolgimento dei compiti previsti dalla normativa vigente, anche connessi con la sicurezza sui luoghi di lavoro e verranno conservati sino a quando la S.V. avrà rapporti con l'Amministrazione Difesa.

i. Alla S.V. sono riconosciuti i diritti dagli art. da 15 a 21 del Regolamento, tra i quali il diritto di accedere ai dati che la riguardano, il diritto di rettificare, di aggiornare, di completare, di cancellare i dati erronei, incompleti o raccolti in termini non conformi alla legge, nonché il diritto di opporsi per motivi legittimi al loro trattamento. Tali diritti possono essere fatti nei confronti dei Titolari del trattamento, per gli aspetti di rispettiva competenza.

Il sottoscritto per le finalità di cui alla presente informativa, **autorizza** il trattamento dei suoi dati personali (compresi quelli sensibili e giudiziari):

_____, lì _____/_____/_____ _____

(LUOGO) (DATA) (FIRMA)

ANNESSO 2

MEMORANDUM DI SICUREZZA PER IL PERSONALE TITOLARE DI TESSERA RIALSCIATA DALL'A.D.

Destinatari: tutto il personale che presta una attività lavorativa presso l'Amministrazione della Difesa.

Obiettivo: detto *memorandum* si prefigge di fornire indicazioni utili al fine di porre l'interessato in grado di operare in sicurezza, evitare di subire falsificazioni o abusi, in particolar modo per quanto concerne:

- **autenticazione** dell'interessato, che permette di usare il certificato di autenticazione contenuto nel chip del supporto per l'accesso a sistemi informatici della Difesa, sia a livello di rete/sistema operativo, sia a livello di applicativo, in sostituzione delle classiche procedure di "autenticazione debole" che invece prevedono l'utilizzo di "username" e "password";
- **firma digitale** (firma a valore legale limitata all'attività di servizio): per effettuare operazioni di firma di documenti: attraverso un apposito certificato inserito nel chip, l'interessato è in grado di utilizzare il supporto come strumento di firma digitale di documenti, in conformità alle vigenti disposizioni di legge.

Modalità di pubblicazione: questo memorandum è disponibile sul portale intranet della Difesa.[1]

In caso di inosservanza ovvero cattiva gestione del supporto sono previste sanzioni in attuazione ai regolamenti, alle norme contrattuali, ai regolamentari e alle leggi in materia disciplinare.

Di seguito sono elencate alcune regole di sicurezza che l'interessato deve seguire per mantenere un buon livello di sicurezza nell'utilizzo del sistema di firma digitale e in generale del supporto hardware che lo ospita. Infatti, l'interessato è tenuto a adottare tutte le misure organizzative e tecniche idonee a evitare danno ad altri[2]. Alcune delle regole seguenti non sono strettamente collegate al sistema di firma ma sono regole di sicurezza generali nell'uso dei sistemi di elaborazione nella considerazione che la sicurezza complessiva del sistema di firma dipende anche dalla sicurezza generale della postazione di lavoro su cui viene utilizzato.

DIVIETI:

- **Non è consentito l'uso del supporto per accedere ad informazioni coperte dal Segreto di Stato**.
- E' vietata la duplicazione della chiave privata di firma e dei dispositivi che la contengono[3].
- Non è consentito l'uso di una chiave per funzioni diverse da quelle previste dalla sua tipologia[4], farne un uso illecito, nonché utilizzare la chiave privata per scopi diversi da quelli per i quali la corrispondente chiave pubblica è stata certificata.
- E' vietato utilizzare un dispositivo diverso da quello indicato/fornito dal Certificatore[5].

---

1 https://archimede.difesa.it/
2 D.Lgs. 82 del 7 marzo 2005 (Codice dell'Amministrazione Digitale)] art. 32, comma 1.
3 DPCM 13 gennaio 2004, art. 7: Conservazione delle chiavi.
4 DPCM 13 gennaio 2004, art. 4: Caratteristiche generali delle chiavi per la creazione e la verifica della firma.
5 DPCM 13 gennaio 2004, art. 6: Modalità di generazione delle chiavi.

SEGUE ANNESSO 2

DOVERI:

In considerazione della valenza legale che la firma digitale di un documento assume, l'utente deve:

- Custodire correttamente e diligentemente il supporto portandolo sempre con sé, evitandone lo smarrimento e proteggendo il supporto dal deterioramento in quanto contenente la chiave privata, al fine di garantirne l'integrità e la massima riservatezza[6].
- Non lasciare incustodito il supporto specialmente quando inserito nel lettore.
- Utilizzare il supporto per il solo tempo necessario ad apporre la firma ovvero ad accedere agli applicativi che necessitano dell'autenticazione tramite lo stesso.
- Non scrivere il PIN di abilitazione del supporto nelle vicinanze del sistema di firma o in un modo che sia facilmente riconoscibile; conservare, cioè, le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo contenente la chiave e custodire con la massima diligenza i codici riservati ricevuti dal Certificatore al fine di preservarne la riservatezza.
- Quando il PIN viene digitato fare in modo che nessuno possa dedurlo osservando il movimento delle mani.
- Cambiare periodicamente il PIN; in particolare se si ha il sospetto che il proprio PIN possa essere diventato noto a qualcuno.
- Non cedere mai il proprio supporto (ed il PIN) ad altri. **Ricordarsi che la firma digitale ha lo stesso valore legale della firma autografa.** Se sorgesse la necessità di firmare documenti in vostra assenza dovranno essere attivate le procedure amministrative di delega della firma.
- Nel caso si sospetti di avere smarrito il supporto ovvero vi sia timore che sia stato sottratto indebitamente, effettuare subito la procedura di sospensione chiamando il numero 2024444/0646914444; inviando un fax al numero 0632355396 ovvero una email all'indirizzo portalecmd@esercito.difesa.it. A tale scopo conservare con cura il codice di emergenza comunicato all'interessato tramite email in fase di emissione del supporto. In seguito, sporgere denuncia alle Autorità di Pubblica Sicurezza competenti e contattare l'Autorizzato al trattamento per le successive operazioni di revoca o riattivazione.
- Devono essere prontamente comunicati all'Ente dove si presta la propria attività lavorativa ovvero direttamente all'Autorizzato al trattamento della LRA di appartenenza i possibili malfunzionamenti riscontrati sul dispositivo di firma.
- Devono essere, altresì, prontamente comunicati all'Ente dove viene prestata l'attività lavorativa, direttamente all'Autorizzato al trattamento o, qualora non sia immediatamente contattabile (es. fuori orario di servizio), direttamente al servizio di certificazione (Call Center del Comando per le Operazioni in Rete) fatti o circostanze che determinino una possibile compromissione della chiave privata (es. furto o smarrimento del dispositivo, sospetti di avvenuta clonazione, riscontro di attacchi di pirateria informatica indirizzati al dispositivo di firma, ecc…) al fine di procedere alla sospensione immediata del corrispondente certificato.

6 DPCM 13 gennaio 2004, art. 7: Conservazione delle chiavi.

SEGUE ANNESSO 2

- A seguito di sospensione del certificato, risolta la relativa causa, è necessario presentarsi presso il proprio Autorizzato al trattamento per richiedere la revoca o la riattivazione dello stesso.
- Richiedere immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma difettosi o smarriti[7].
- Sospendere l'utilizzo dei certificati del supporto alla data della loro scadenza.
- Evitare di firmare digitalmente su stazioni di firma non sicure.
- Prestare attenzione alla configurazione del Personal Computer utilizzato per firmare digitalmente. Soprattutto, evitate di installare programmi di cui non si abbia la certezza dell'origine e dell'affidabilità. Il rischio è l'installazione involontaria di software maligno (es. *trojan, malware* o *virus*).
- I sistemi operativi della famiglia *MS Windows*® consentono di condividere risorse quali cartelle di lavoro e stampanti. La condivisione di una cartella di lavoro situata sulla propria stazione di firma ad altri utenti, li porrà nella condizione di avere accesso all'intero contenuto della cartella. Si sconsiglia di utilizzare tale procedura e di avvalersi in alternativa delle cartelle condivise predefinite sui server di rete o di utilizzare la posta elettronica per la spedizione del documento.
- I *Personal Computer* delle reti della Difesa sono protetti con anti-virus mantenuti costantemente aggiornati. Nel caso venga intercettato un *virus* o un *trojan* avvisate immediatamente l'amministratore della rete locale. E' ammesso l'uso del supporto anche su *Personal Computer* personali, pertanto è buona norma usare anche sul proprio *Personal Computer*, un buon programma *anti-virus* aggiornato, meglio se in modalità automatica.
- Non dimenticare che *Internet* è una rete insicura. Evitare di collegarsi ad *Internet* utilizzando mezzi locali diversi da quelli messi a disposizione dall'Amministrazione (soprattutto evitate l'uso di modem aggiuntivi collegati a *provider Internet*); ricordare che mentre i servizi Internet forniti attraverso la connessione ufficiale dell'Amministrazione a Internet sono controllati tramite firewall, gli stessi servizi utilizzati tramite altre vie potrebbero essere veicolo di attacchi informatici e mettere in serio pericolo il corretto funzionamento della vostra postazione di lavoro che utilizzate per firmare e di tutte le altre postazioni. Nel caso utilizziate a casa computer portatili come stazione di firma è opportuno utilizzare un *personal firewall*.
- Durante la navigazione in *Internet* evitare, se non strettamente necessario, di accettare componenti quali *ActiveX* e *applet Java* senza limitazioni sui privilegi.
- Disattivare, o fare disattivare, le funzionalità di esecuzione automatica del codice o degli allegati all'interno del vostro applicativo di posta elettronica.
- Non lanciare mai file eseguibili, (Es. con estensione .exe), ricevuti con messaggi di posta elettronica, memento da utenti fidati, dato che esistono *virus* che prendono dalla rubrica del client sul *Personal Computer* infetto indirizzi di utenti legittimi ai quali inviano file di qualsiasi tipo comprese repliche di se stessi. Deve essere prestata attenzione anche al fatto che esistono tecniche di mascheramento dei *file* potenzialmente dannosi utilizzata dai creatori di *virus*, che permettono di inviare file eseguibili come se fossero documenti, presentazioni, ecc.
- Al termine delle attività lavorative spegnere la postazione di lavoro.

7 DPCM 13 gennaio 2004, art. 7: Conservazione delle chiavi.

SEGUE ANNESSO 2

- Curare un'adeguata protezione del proprio ambiente di lavoro. Gran parte delle violazioni avviene ad opera di personale interno, accedendo, ad esempio, a documenti sensibili lasciati incustoditi su una scrivania. Evitate di visualizzare a video o lasciare incustoditi documenti sensibili se non siete soli o in presenza di personale fidato. Custodire con cura *floppy disk*, CD-ROM, chiavette USB, iPod, *hard-disk* portatili e ogni altro strumento in grado di memorizzare informazioni.

CASI PREVISTI PER LA SOSPENSIONE E LA REVOCA DELLA TESSERA A CURA DELL'INTERESSATO

Non appena si verifichi uno dei casi seguenti l'interessato dovrà richiedere la sospensione della carta.

Elenco dei casi di sospensione del supporto a cura dell'interessato

- Compromissione/perdita dei codici PIN e PUK.
- Furto/smarrimento del supporto.
- Ogni altro motivo che possa dare adito ad un uso improprio del supporto. A seguito della sospensione precauzionale del supporto, ove il problema fosse giunto a positiva conclusione, si dovrà procedere alla procedura di riattivazione. Qualora il problema permanesse, o qualora si verificasse uno dei problemi sotto riportati, si dovrà procedere alla revoca del supporto.

Elenco dei casi di revoca della carta a cura dell'interessato

- Chip o supporto difettoso per guasto o cattivo funzionamento.
- Compromissione o sospetta compromissione delle chiavi private (firma e autenticazione).
- Cambio di almeno uno dei dati pubblicati nei certificati digitali o dati errati.
- Cessazione dalla propria attività lavorativa svolta presso l'Amministrazione della Difesa (dimissioni, pensionamento, passaggio ad altra PA, ecc.).
- Furto, smarrimento o distruzione del supporto (perdita di possesso).
- Scadenza del supporto.
- Dati non mutabili errati (Es. codice fiscale, cognome, nome, data di nascita).

UTILIZZO DELLA CARTA

Modalità operative per l'utilizzo e la generazione della firma digitale

Unitamente al dispositivo di firma, nei casi previsti, viene messo a disposizione dell'interessato un lettore di smart card e il software, disponibile anche sul sito http://cmdweb.servizi.difesa.it, necessario per le operazioni di firma dei documenti.

Il software consente la selezione della coppia di chiavi di firma da utilizzare, la visualizzazione del relativo certificato e del contenuto del documento elettronico da firmare. Il software richiede all'interessato di confermare la volontà di firmare il documento elettronico visualizzato. In caso di assenso, il software procede alla produzione del documento informatico in un file con estensione "p7m" o "pdf". L'interessato per poter inviare posta elettronica firmata digitalmente dovrà obbligatoriamente avere configurato il client di posta elettronica (Outlook) in modo che la e-mail inviata riporti nel campo From (Da) l'indirizzo di posta elettronica inserito nel certificato.

SEGUE ANNESSO 2

Formato dei documenti

L'automazione delle procedure lavorative ha introdotto un largo uso di formati documentali che favoriscono l'interscambio e il riutilizzo all'interno dei processi amministrativi. Tali formati documentali arricchiscono il "contenuto" del documento con elementi di codice interpretati dal *software* applicativo (es. *Microsoft Office*), finalizzati ad incrementarne il riuso (es. modulistica, campi data, numerazione pagine, formattazione testo) o a effettuare calcoli matematici.

Tali elementi di codice possono produrre alterazioni al "contenuto" del documento dipendenti dal contesto dell'ambiente di visualizzazione in uso. Ciò avviene quando in una dichiarazione, dove normalmente a sinistra del gruppo firma viene inserita la scritta "Luogo, lì ___", al posto della linea viene inserita una macroistruzione per la visualizzazione della data corrente. Se il documento viene firmato digitalmente in data 27 marzo 2014 e viene inviato il giorno successivo, colui che lo riceverà visualizzerà che la dichiarazione è stata fatta il 28 marzo 2014 mentre la firma è stata apposta il giorno precedente.

Quanto sopra è da tenere in debita considerazione quando deve essere firmato un documento di particolare "delicatezza/importanza".

Ed infatti l'art. 4 para 3 del DPCM 22 febbraio 2014 statuisce che *"il documento informatico, sottoscritto con firma elettronica qualificata o firma digitale, non soddisfa il requisito di immodificabilità del documento previsto dall'art. 21, comma 2, del Codice, se contiene macroistruzioni, codici eseguibili o altri elementi, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati"*.
Pertanto, soprattutto per i documenti di particolare importanza, si suggerisce l'adozione di formati documentali statici quali ad esempio:

- Puro testo -".txt";
- Immagine -".tif";
- *Portable Document Format* (pdf) in formato PDF/A.

Obblighi dei destinatari

I destinatari dei messaggi elettronici e/o delle evidenze informatiche firmate digitalmente dall'interessato devono verificare:

- che il certificato contenente la chiave pubblica dell'interessato firmatario del messaggio e/o evidenza informatica non sia temporalmente scaduto;
- che il certificato dell'interessato sia stato firmato con le chiavi di certificazione della Autorità di Certificazione presenti nell'Elenco Pubblico mantenuto dall'Amministrazione;
- l'assenza del certificato nelle Liste di Revoca (CRL) che coincidono con le Liste di Sospensione (CSL) dei certificati;
- l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dall'interessato;
- che la tipologia di uso della chiave del certificato sia "Non Ripudio".

SEGUE ANNESSO 2

Modalità operative per l'utilizzo del sistema di verifica delle firme

La corretta verifica della firma richiede che l'utente utilizzi il sistema con una connessione attiva e preventivamente proceda all'aggiornamento dei certificati dell'Elenco Pubblico dei Certificatori. Il sistema sarà così in grado di effettuare, oltre che i controlli di integrità della firma (nessuna modifica del documento elettronico firmato) e validità temporale del certificato del firmatario, anche la sua credibilità (certificato del firmatario rilasciato da uno dei certificatori accreditati). L'utente dovrà inoltre accertarsi che il certificato del firmatario non sia stato revocato o sospeso attraverso l'aggiornamento delle relative CRL. Un'ulteriore verifica che l'utente deve effettuare è il controllo della conformità con il contenuto del documento firmato di un'eventuale limitazione d'uso presente nel certificato del firmatario[8]. Infine si tenga conto delle problematiche relative alla eventuale presenza di macroistruzioni o codice eseguibile nel documento verificato.

8 D.Lgs. 82 del 7 marzo 2005: Codice dell'Amministrazione Digitale art. 30, comma 3.