STATO MAGGIORE DIFESA

VI Reparto – Sistemi C4I e Trasformazione

SMD - I - 009

NORME DI GESTIONE E D'IMPIEGO
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 NOVEMBRE 2017

Pagina intenzionalmente bianca

STATO MAGGIORE DELLA DIFESA

VI REPARTO - Sistemi C4I e Trasformazione

ATTO DI APPROVAZIONE

Approvo la presente Direttiva "*Norme di gestione e d'impiego 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* (SMD-I-009)" - Edizione novembre 2017.

Essa abroga e sostituisce la precedente edizione del 2014, pari numero.

Roma, lì 20/11/2017

IL CAPO DI STATO MAGGIORE
Generale Claudio GRAZIANO

Pagina intenzionalmente bianca

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
Diramazione Interna		
UFFICIO GENERALE DEL CAPO DI SMD		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
COMANDO C4 DIFESA		1

Pagina intenzionalmente bianca

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			

GUIDA ALLA CONSULTAZIONE

DESTINATARI DELLA DIRETTIVA

La Direttiva è rivolta a tutti gli *stakeholder*[1] coinvolti nei processi di acquisizione, validazione, emissione, consegna, utilizzo e ritiro della tessera modello ATe[2]e dei certificati digitali (firma digitale, cifra e autenticazione **Carta Nazionale dei Servizi - CNS**) collocati a bordo della carta ed emessi dalla ***Public Key Infrastructure*** **(PKI)** della Difesa, nonché alle strutture organizzative che presiedono alle attività di verifica e controllo ***(Governance)*** dei predetti processi.

Di seguito, per facilitare la ricerca e la consultazione di tali tematiche, è illustrata la "mappa" del documento contenente la disposizione degli argomenti nei capitoli e paragrafi che lo costituiscono.

Nella presente direttiva sono descritte le innovazioni architetturali intercorse nel tempo con la costituzione di un ***Card Management System*** **(CMS) Unico** e illustrati tutti i processi di servizio connessi con la tessera mod. ATe.

L'esigenza di un approccio unitario e condiviso alle problematiche afferenti sia la tessera mod. ATe che la firma digitale, a fronte di una evoluzione sempre più rapida delle pubbliche amministrazioni verso la *digital transformation*, ha evidenziato la necessità di definire una *policy* di gestione comune che tenga conto delle altre realtà tecnologiche presenti e degli aggiornamenti normativi. Il nuovo documento, pertanto, abrogherà, inglobandone i contenuti ancora in vigore, le:

- SMD-I-001 "Direttiva per l'impiego della Firma Digitale in ambito amministrazione Difesa" Edizione 2005;
- SMD-I-009 "Carta Multiservizi della Difesa – Norme di gestione e di impiego" Edizione 2014.

MODALITÀ DI DISTRIBUZIONE DELLA DIRETTIVA E PRESA VISIONE

Al fine di coordinare la struttura centrale responsabile della gestione del sistema informativo per l'emissione della tessera mod. ATe e le articolazioni periferiche **dell'Amministrazione Difesa (A.D.)**, la presente direttiva dovrà essere diramata sino ai minori livelli ordinativi e pubblicata sui portali di Forza Armata.

Inoltre, tutto il personale dovrà essere edotto in relazione all'attuazione della disciplina in materia di utilizzo dei certificati digitali e di protezione dei dati personali attraverso la firma per presa visione dell'informativa ai sensi dell'art.13 del D.Lgs. n. 196/2003 sull'attività di raccolta dei dati personali predisposta in Allegato A alla presente direttiva (pagina 5).

STRUTTURA DEL DOCUMENTO

Al fine di rendere il presente documento di facile consultazione e aggiornamento, la Direttiva è stata strutturata in due Sezioni:

- **SEZIONE 1**

  *Denominata "**Core**", contiene indicazioni dottrinali di carattere generale, di governance ed elementi imprescindibili per garantire l'operatività della tessera mod. ATe e della firma digitale. E' articolata in 7 Capitoli:*

  - ***Cap. 1:** contiene una premessa introduttiva e descrive lo scopo del presente documento.*
  - ***Cap. 2:** contiene una descrizione generale della governance definendone la struttura che la*

1 In quest'ambito, il termine "stakeholders" (letteralmente "portatore di interessi") viene utilizzato per indicare genericamente l'insieme dei Soggetti dell'Amministrazione Difesa coinvolti , a qualsiasi titolo, perché in possesso di conoscenze specifiche nella acquisizione e nell'impiego di un determinato sistema informativo

2 Decreto del Presidente della Repubblica (DPR) 28 luglio 1967, n. 851, recante "Norme in materia di tessere di riconoscimento rilasciate dalle amministrazioni dello Stato, che individua i modelli di tessera rilasciati su supporto cartaceo" rilasciate con modalità elettronica dalle Amministrazioni dello Stato, ai sensi dell'articolo 66, comma 8, del D. Lgs. 82/2005 e ss.mm..

caratterizza.

- ***Cap. 3:*** *descrive le strutture organizzative che presiedono i processi di servizio illustrati, indicando ruoli e responsabilità di ciascun Attore.*
- ***Cap.*** *Errore. L'origine riferimento non è stata trovata.**:** contiene una descrizione generale della tessera mod. ATe (struttura, funzioni e informazioni) e una elencazione dei certificati essenziali installati.*
- ***Cap. 5:*** *contiene una descrizione generale della PKI riportando informazioni circa la struttura, la validità, i requisiti normativi e tecnici che la caratterizzano.*
- ***Cap. 6:*** *descrive i processi di servizio necessari per la realizzazione, la gestione e l'impiego della tessera mod. ATe e dei Certificati Digitali.*
- ***Cap. 7****: descrive le finalità e le modalità del trattamento cui sono destinati i dati personali acquisiti per il rilascio della tessera mod. ATe.*

- **SEZIONE 2**

  E' costituita da diversi Annessi e Allegati, ciascuno dei quali è focalizzato su un particolare aspetto della tessera mod. ATe e/o della PKI e ne descrive le specifiche procedure applicabili, i sistemi e i servizi in vigore al momento della consultazione.

- **EVIDENZA DEGLI ACRONIMI ALL'INTERNO DELLA DIRETTIVA**

  Gli acronimi sono stati raccolti in Annesso 2 alla Direttiva. Ciascun acronimo, al momento del suo primo utilizzo, è accompagnato dalla sua ***descrizione*** *"****in chiaro****", entrambi evidenziati con carattere "****neretto****" (****bold****).*

INDICE

- ALLEGATO H: Rappresentazione grafica del processo di sospensione.
- ALLEGATO I: Elenco dei titoli autorizzati alla trascrizione nel campo NOTE della tessera mod. ATe.
- ALLEGATO L: Personale destinatario della tessera mod. ATe.
- ALLEGATO M: Matrice delle osservazioni/proposte.

1. CARATTERIZZAZIONE DELLA DIRETTIVA

1.1. PREMESSA

L'esigenza di disporre di una "carta elettronica" contenente i dati anagrafici e sanitari del personale militare nasce e si sviluppa all'interno delle **Forze Armate** (**F.A.**) anche come risposta a specifiche esigenze ravvisate nei Teatri Operativi. In tali contesti, infatti, furono avviate le prime iniziative progettuali volte alla realizzazione di una tessera elettronica (*smartcard*) in grado di archiviare e gestire le informazioni di carattere personale e sanitario[3] con adeguati requisiti di sicurezza e, nello stesso tempo, rendesse possibile l'accesso a servizi digitali, alcuni dei quali previsti per legge[4].

Nel tempo, anche il Ministro per l'Innovazione e le Tecnologie, nel delineare la politica dell'*e-Government* per il triennio 2003-2005, allo scopo di dare un nuovo impulso alla digitalizzazione della **Pubblica Amministrazione** (**P.A.**), aveva incluso tra gli obiettivi strategici del Governo l'erogazione "*on-line*" di alcuni fondamentali servizi rivolti alla collettività[5], indicando anche standard e criteri organizzativi da seguire per la loro erogazione.

In tale scenario, l'**Amministrazione della Difesa** (**A.D.**) ha avviato un significativo processo di sviluppo tecnologico della **Carta Multiservizi della Difesa** (**CMD**) che, inserita nell'ambito di programmi specifici come la ***Defence Information Infrastructure (DII)***, ha consentito di incrementarne le potenzialità implementando un numero sempre maggiore di servizi accessibili oltre ad estenderne l'utilizzo al personale civile.

Il progetto CMD s'inquadra quindi nel più ampio programma d'iniziative intraprese dalla P.A., finalizzate a dotare il proprio personale di strumenti elettronici d'identificazione, sia fisica sia logica, che consentono l'accesso a *"**servizi primari**"*, comuni a tutte le Amministrazioni, e a *"**servizi specifici**"* peculiari del Comparto Difesa.
Sono **servizi primari** [6]:

- *l'identificazione "a vista" quale tessera di riconoscimento rilasciata dall'A.D. in sostituzione del mod. AT cartaceo[7];*
- *l'identificazione "elettronica" (compatibilità estesa al circuito della **Carta d'Identità Elettronica - CIE**);*
- *l'autenticazione e l'identificazione "in rete" (compatibilità estesa al circuito della **Carta Nazionale dei Servizi - CNS**);*
- *la firma digitale.*

I **servizi specifici** sono invece connessi all'esigenza di incrementare il livello di sicurezza dei sistemi informativi e dei dati da questi trattati, attraverso l'adozione di misure di sicurezza finalizzate a preservarli da accessi non autorizzati.

Con il DPCM 24 maggio 2010 sono state unificate per tutta la Pubblica Amministrazione le regole tecniche per il rilascio, in formato elettronico, della tessera personale di riconoscimento, di cui al decreto del Presidente della Repubblica 28 luglio 1967, n. 851, ai dipendenti di ruolo delle amministrazioni pubbliche statali di cui all'art. 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nonché al personale militare in attività di servizio ovvero in posizione di ausiliaria.
Di fatto, la Difesa è stata la prima Pubblica Amministrazione ad essersi dotata di una propria

3 Decreto Legislativo 15 marzo 2010, n. 66 – Codice dell'ordinamento militare (Art. 1496).
4 Legge 24 Dicembre 2007, n. 244 - Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato. Art. 3 Comma 83: rilevazione automatica delle presenze per l'erogazione dei compensi per lavoro straordinario.
5 Carta d'Identità Elettronica – CIE, Carta Nazionale dei Servizi – CNS e firma digitale.
6 Per i dettagli normativi e regolamentari si rimanda al DPCM 24 maggio 2010 recante *"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. Lgs. 82/2005"*.
7 DPR del 28 dicembre 2000, n. 445.

infrastruttura per la produzione dei modelli ATe e l'emissione dei certificati digitali a bordo degli stessi:

- Carta Nazionale dei Servizi – CNS;
- firma digitale;
- cifratura.

1.2. SCOPO DEL DOCUMENTO

La presente Direttiva si colloca nel naturale processo di evoluzione dell'***Information Communication Technology*** (**ICT**) della Difesa e, nello specifico, è finalizzata a disciplinare tutte le fasi del ciclo di vita della tessera modello ATe e a fornire le informazioni essenziali sulla ***Public Key Infrastructure (PKI)*** e sulla firma digitale.

Il presente documento ha lo scopo di raccogliere e definire in un unico documento gli aspetti legali, procedurali e tecnici legati all'acquisizione dei dati personali necessari alla Difesa per gestire l'intero ciclo di vita della tessera personale di riconoscimento mod. ATe, di cui al decreto del Presidente della Repubblica 28 luglio 1967, n. 851, in modalità elettronica[8] e dei certificati digitali a bordo di essa.

Tali aspetti dovranno trovare puntuale riscontro nella protezione dei dati del personale, nella tecnologia che supporta l'infrastruttura ICT dedicata ed essere ben conosciuti dei possessori della tessera. Infatti, tutta l'organizzazione è coinvolta nel rispetto dei dettami legislativi, di sicurezza e tecnici che la gestione della tessera mod. ATe comporta.

Una adeguata informazione e una opportuna conoscenza della tessera mod. ATe come strumento di lavoro non possono che avere come risultato un uso consapevole e limitato alle esigenze funzionali della Difesa.

Eventuali richieste di modifica al presente documento potranno essere rappresentate utilizzando il modulo predisposto in Allegato M.

8 Decreto Legislativo 7 marzo 2005, n. 82 Codice dell'amministrazione digitale (aggiornato al decreto legislativo 26 agosto 2016, n. 179), Art. 66. Carta d'identità elettronica e carta nazionale dei servizio.

2. GOVERNANCE

2.1. OBIETTIVI DELLA GOVERNANCE

Lo **Stato Maggiore della Difesa** (**SMD**), con la presente direttiva intende disciplinare la *governance* per la gestione dell'infostruttura preposta all'emissione della tessera mod. ATe attraverso:

- la definizione di una struttura organizzativa preposta al governo, controllo e gestione operativa, con ruoli e responsabilità ben definite in merito a tutti i temi correlati con il servizio: sicurezza, processi, infrastruttura e applicazioni;
- l'assicurazione che gli investimenti sul servizio generino un valore aggiunto, in linea con la normativa di settore in vigore, per tutta l'A.D.;
- la gestione dei rischi e dei vantaggi generati dall'utilizzo di un sistema informativo unico per il rilascio della tessera mod. ATe e la generazione di certificati digitali.

Per delineare il modello di *governance* è stato adottato come standard di riferimento per i processi, le relazioni e le responsabilità quello fissato dall'***Information Technology Infrastructure Library* - ITIL®**[9], mettendolo in correlazione con processi e strutture organizzative del Comparto Difesa.

2.2. STRUTTURA ORGANIZZATIVA DELLA GOVERNANCE

La *governance* del servizio è esercitata attraverso una struttura organizzativa che si articola secondo un modello a distinti livelli di responsabilità. Per una migliore comprensione del processo di *governance*, si riepilogano di seguito gli Organi individuati:

- **Comitato di Coordinamento Informatica (CCI)**[10]. E' l'organo permanente interforze, che ha dipendenza funzionale dal **Dirigente Generale Responsabile per i Sistemi Informativi dell'Amministrazione della Difesa (D.G.Re.S.I.A.D),** che opera nell'ambito dell'organizzazione della Difesa con il compito istituzionale di esaminare, valutare e coordinare le principali problematiche a carattere comune nel campo dell'informatica. Al CCI, a cui compete l'indirizzo strategico del servizio, ha la responsabilità di indicare le linee guida d'interesse collettivo e le eventuali azioni da intraprendere per la risoluzione delle criticità che dovessero emergere nel tempo.
- ***Change Advisory Board* (CAB).** E' l'organo preposto ad analizzare le nuove esigenze legate all'impiego del servizio (es. modifiche legislative), attraverso la determinazione degli impatti e la definizione delle risorse necessarie per l'implementazione di nuove funzionalità. Ha la responsabilità e le competenze, con particolare riguardo ai processi critici di *Change* e *Configuration Management*, per la definizione dei piani d'intervento sulle istanze migliorative/di adeguamento normativo individuate sia direttamente sia attraverso il servizio di *help desk* dove vengono raccolte le segnalazioni/*incident* che sfociano in ***Request For Change* (RFC).** Tiene costantemente informato il CCI sulle criticità emerse, sulle eventuali azioni da intraprendere e sullo stato di avanzamento degli adeguamenti avviati. I rappresentati dello Stato Maggiore della Difesa, delle Forze Armate e del Segretariato Generale della Difesa che costituiscono il ***Change Advisory Board* (CAB)** sono specificati nell'Allegato E.
- ***Application Service Provider* (ASP).** E' l'organo preposto all'erogazione del servizio ed è ospitato presso il Centro di esercizio interforze individuato dalla F.A. designata per la *Lead Service*[11]. Nello specifico, il servizio di *Card Management System* (CMS) unico è assegnato alla F.A. Esercito, che ha dunque la responsabilità, per conto della A.D., della gestione operativa del

9 Information Technology Infrastructure Library - ITIL: propone un insieme di *best practice* per la gestione dei processi nell'ambito del *service management*, suddivise rispetto alle fasi del ciclo di vita di un servizio (*Service Strategy; Service Design; Service Transition; Service Operation; Continual Service Improvement*).

10 SMD - I - 020 "Direttiva per 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".

11 F.A./Organo designato per la direzione del Servizio.

servizio e del supporto tecnico-informatico per l'attuazione dei piani d'intervento stabiliti dal CAB. All'ASP è assegnato anche il compito di gestire il *deployment* del servizio.

2.3. CHANGE ADVISORY BOARD (CAB)

Il ***Change Advisory Board*** (**CAB**) è l'organo[12] che garantisce l'applicazione:
- delle norme di legge vigenti in materia tessera di riconoscimento e di firma digitale, fornendo le indicazioni per le attività evolutive del servizio, in maniera standardizzata per tutto il Comparto Difesa;
- dei processi di ***Change Management*** **(CM)** relativi al servizio.

Al fine di contemplare tutte le esigenze correlate al sistema informativo per il rilascio della tessera mod. ATe e dei certificati digitali inseriti su di essa, i principali *stakeholder* sono rappresentati all'interno del CAB da un proprio Referente Unico. Per la trattazione di tematiche specifiche, quali ad esempio aspetti di carattere tecnico e/o normativo, ogni Referente può essere coadiuvato da altri collaboratori.

Nell'ambito del CAB lo **SMD I Reparto** e il **Segretariato Generale della Difesa - Direzione Nazionale degli Armamenti (SGD-DNA)** svolgono il ruolo di organi consulenti per l'emanazione delle direttive necessarie a garantire la conformità alle norme e alle disposizioni di legge in materia di tessere di riconoscimento rilasciate dalle amministrazioni dello Stato[13].

Stante l'assegnazione della *Lead Service* all'Esercito, il ruolo di Presidente del CAB è ricoperto dal rappresentante designato dello Stato Maggiore dell'Esercito.

2.3.1. COMPITI

Il CAB ha il compito di valutare, autorizzare e definire le priorità riguardo agli interventi evolutivi sul sistema informatico armonizzando e strutturando le richieste provenienti dall'utenza (tramite RFC) al fine di migliorare la *performance* e l'usabilità dell'applicativo. Esso approva e coordina la corretta implementazione delle modifiche, minimizzando il rischio di alterare i livelli di qualità del servizio stesso.

Nell'ambito del modello organizzativo individuato, il CAB:
- propone nell'ambito del CCI le variazioni della *policy* di gestione e di sicurezza del servizio;
- rivede periodicamente la presente direttiva;
- coordina il *deployment* del servizio, fornendo le indicazioni per la relativa distribuzione agli Enti dell'applicativo e del materiale.

In particolare:
- definisce le *policy* di gestione delle diverse classi di gravità degli errori (*standard*, *normal* o *emergency change*) e RFC;
- definisce i piani di manutenzione e il rilascio delle nuove versioni del sistema informatico;
- identifica i rischi e pone in essere i processi e le contromisure volte a mitigare l'impatto negativo sul servizio;
- è preposto alla verifica della corretta realizzazione dei piani inerenti la gestione del ciclo di vita del servizio;
- autorizza eventuali deviazioni al livello di servizio (tempi, rischi, ecc.) purché compresi nelle tolleranze dei livelli di qualità concordati con il CCI;
- vaglia, registra ed effettua le *review* delle RFC autorizzate dal CCI, stimandone l'impatto, i costi e i benefici;

12 Si veda la struttura in Allegato "E".
13 Decreto del Presidente della Repubblica (DPR) 28 luglio 1967, n. 851

- coordina l'implementazione [14] delle modifiche e ne gestisce il *deployment*;
- assicura che le modifiche siano registrate, aggiornate e supervisionata su una piattaforma di gestione per la configurazione (*Configuration Management System)*;
- coordina l'attività di formazione del personale;
- verifica e garantisce la corretta applicazione degli standard e delle metodologie definite per il servizio;
- attua le strategie stabilite dal CCI, pianificando gli interventi da effettuare sul servizio, sulla base delle risorse disponibili;
- identifica i parametri di riferimento per la misura delle *performance* del servizio: affidabilità, disponibilità, scalabilità e sicurezza;
- sottopone all'attenzione del CCI eventuali criticità, rischi o proposte di modifica che abbiano un impatto significativo sul servizio e per questioni di livello direttivo/strategico, nei casi in cui è necessario un supporto decisionale di livello superiore. Tale coinvolgimento è richiesto per questioni afferenti il sistema informatico e riguarda problematiche di ordine generale che necessitano di un coordinamento/armonizzazione traversale per tutta l'A.D.. Le soluzioni eventualmente proposte al CCI, devono essere corredate d'idonea documentazione che evidenzi anche gli oneri finanziari da sostenere.

2.4. APPLICATION SERVICE PROVIDER (ASP)

L'ASP è l'organo preposto all'erogazione del servizio al bacino di utenza. I centri responsabili dell'infrastruttura tecnologica e dell'operatività del servizio sono ubicati presso:

- **PKI: Comando C4 Difesa - Via Stresa, 31 B - 00135 Roma;**
- **tessera mod. ATe: Comando C4 Esercito - Via Guido Reni, 22 - 00196 Roma.**

2.4.1. COMPITI DELL'ASP

Nell'ambito del modello organizzativo individuato, l'ASP è responsabile delle seguenti attività:

- mantiene l'operatività dell'infrastruttura *hardware* asservita al servizio (*Card Management System, Certification Authority* e *Local Registration Authority*);
- emana/aggiorna le direttive riguardanti i compiti del personale delle L.R.A;
- definisce la configurazione delle postazioni di lavoro delle *Local Registration Authority* (LRA) alla *baseline* minima di sicurezza prevista per l'accesso al servizio;
- mantiene aggiornata all'ultimo rilascio autorizzato dal CAB, la versione dell'applicazione *software* del servizio;
- garantisce i livelli di servizio e di qualità stabiliti dal CAB;
- rendiconta i costi associati all'operatività del servizio relativamente all'adeguamento *hardware* e *software*;
- informa il CAB della necessità di effettuare l'implementazione di nuove funzionalità/interventi corretti al servizio;
- recepisce le richieste, valuta le criticità e l'impatto delle soluzioni indicate dal CAB;
- in coordinazione con i gestori della rete intranet della Difesa, formula raccomandazioni e fornisce suggerimenti al CAB sulle soluzioni tecniche per rispondere alle *policy* e alle direttive di settore;
- assicura adeguato supporto informatico al processo di sviluppo e consolidamento del servizio;
- stabilisce una gestione strutturata del ciclo di vita del servizio:
  - esegue il *Change Management*;
  - gestisce il C*onfiguration Management;*
- attiva un servizio di help desk di 1° livello a favore degli utenti;
- attiva un servizio di help desk di 2° livello a favore delle LRA;

14 Il CAB non è incaricato della implementazione delle modifiche ma controlla solo che queste siano implementate efficacemente, ad un costo ragionevole con il minimo rischio.

- propone gruppi di lavoro per lo studio di specifiche soluzioni su requisiti e\o problematiche relative al servizio;
- definisce i piani di sviluppo, di *deployment* e di formazione che pone all'approvazione del CAB;
- rivede periodicamente e/o raccomanda le variazioni delle *policy* di gestione e di sicurezza stabilite per il servizio;
- promuove il miglioramento del servizio basandosi sui risultati (*lesson learned*) raccolti dalle LRA;
- fornisce al CAB le statistiche sui malfunzionamenti rilevabili dai *ticket* gestiti dal CMS;
- gestisce il sistema di configurazione del *software* e registra ogni intervento di manutenzione correttiva o evolutiva del software attraverso lo strumento di *Application Lifecycle Management* (ALM) adottato;
- risolve, in base ai diversi livelli di intervento, le anomalie inoltrate dal servizio di *service desk management*;
- propone al CAB il piano di manutenzione ordinario (*hardware, software* e strutturale) o l'implementazione di nuove soluzioni tecnologiche per il miglioramento del servizio.

2.5. PROCEDURE PER LA MANUTENZIONE DEL SERVIZIO

Durante la sua vita operativa il servizio dovrà essere mantenuto in esercizio assicurando i livelli minimi di fornitura del servizio, attraverso la definizione e implementazione delle seguenti procedure:

- ***Service Level Agreement* (SLA):** accordo sul livello del servizio. Strumento attraverso il quale si definiscono le metriche (es. qualità di servizio) che devono essere rispettate dal CMS nei confronti degli utenti. Affinché il servizio soddisfi tutte le esigenze del Comparto Difesa, in Allegato G sono richiamati gli indicatori di qualità applicabili ai principali processi di gestione della tessera mod. ATe.
- ***Application Lifecycle Management* (ALM)**: gestione del ciclo di vita (*governance*, sviluppo e manutenzione) di un'applicazione *software*. Rappresenta l'unione delle attività di gestione del servizio con le attività di ingegneria del *software*, resa possibile dall'utilizzo di strumenti che facilitano la gestione delle fasi di: analisi dei requisiti, progetto architetturale, sviluppo, *testing*, gestione delle *release*, del *change* e del *deployment*.
- ***Request For Change* (RFC):** procedura prevista da ITIL® per inviare una proposta formale di modifica al servizio. La RFC deve contenere tutte le informazioni necessarie affinché un cambiamento possa essere valutato, approvato e implementato.

3. STRUTTURA ORGANIZZATIVA DEI PROCESSI DI SERVIZIO

3.1. GENERALITÀ

Il rilascio e la gestione della tessera mod. ATe, sia come supporto fisico sia come insieme di servizi a essa associati, coinvolgono un molteplice numero di attori che intervengono a vario titolo per l'assolvimento di diverse tipologie di mansioni.

Il presente capitolo riporta la struttura organizzativa degli Organi coinvolti nel ciclo di vita della tessera mod. ATe, definendo, per ciascuno, le mansioni ricoperte:

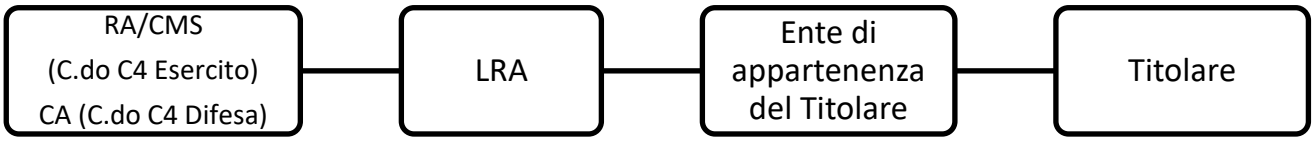


Figura 1 - Esemplificazione della struttura gerarchico-funzionale

La figura sopra riportata illustra, dal punto di vista funzionale, la gerarchia che si instaura durante il ciclo di vita della tessera mod. ATe. Il CMS, da cui ha inizio tutto il processo, è l'erogatore principale dei servizi. Le rimanenti funzioni e responsabilità sono assegnate alle *Local Registration Authority* e all'Ente di cui fa parte il personale che richiede la tessera mod. ATe.

Il ciclo di vita vede il Titolare della carta quale unico responsabile del corretto impiego della tessera mod. ATe sia per i servizi legati alla firma digitale, che per il valore legato alla sua validità in termini di documento d'identità.

3.2. CERTIFICATION AUTHORITY (CA)

Le *Certification Authority **(C.A.)*** di **Firma Digitale** e **Autenticazione CNS** sono accreditate presso l'**Agenzia per l'Italia Digitale (AgID)** e devono rispondere esattamente a tutte le specifiche tecniche/funzionali/organizzative definite dalle regole specificate nel **Codice dell'Amministrazione Digitale** (**CAD**) e nel Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio in materia di identificazione elettronica (**Regolamento eIDAS**).

La *Certification Authority* responsabile di tutta l'infrastruttura a chiave pubblica della Difesa (*Public Key Infrastructure* - PKI) è identificata nel Comando C4 Difesa. Essa è deputata all'emissione, alla gestione, alla sospensione e alla revoca dei certificati digitali a bordo della tessera mod. ATe. Quale Certificatore accreditato a livello nazionale, nell'espletamento delle proprie funzioni risponde, a norma del CAD, all'**Agenzia per l'Italia Digitale (AgID)**.

La *Certification Authority*, per l'espletamento delle proprie funzioni, si avvale:
- della *Registration Authority* (RA);
- delle *Local Registration Authority* (LRA), attraverso le quali assolve alle seguenti responsabilità :
  - riconoscimento del Titolare, dell'univocità e non ripudio dei certificati digitali;
  - emissione dei certificati digitali;
  - gestione della vita dei certificati digitali;
  - sospensione e revoca dei certificati digitali;
  - aggiornamento dello stato dei certificati.

3.3. REGISTRATION AUTHORITY (RA) E CARD MANAGEMENT SYSTEM (CMS)

Il **Comando C4 Esercito** svolge la doppia funzione di ***Registration Authority*** (**RA**) e ***Card Management System*** (**CMS**).

Come RA in ambito *Public Key Infrastructure*, su delega della *Certification Authority* (Comando C4 Difesa), gestisce tutte quelle attività propedeutiche al rilascio dei certificati digitali installati all'interno della tessera mod. ATe.

In qualità di CMS, provvede alla personalizzazione e stampa delle tessere mod. ATe, in particolare:

- alla personalizzazione grafica della tessera mod. ATe con i dati del Titolare;
- all'inserimento all'interno del chip dei certificati emessi dalla CA;
- alla validazione delle richieste di sospensione, revoca ovvero riattivazione dei certificati digitali;
- per il tramite delle LRA, alla consegna della carta al Titolare;
- al ritiro, alla verifica tecnica, alla conservazione e alla distruzione delle tessere mod. ATe scadute e revocate.

3.4. LOCAL REGISTRATION AUTHORITY

Le *Local Registration Autority*, su delega della CA e della RA, sono distribuite presso l'A.D. e sono responsabili della corretta applicazione delle procedure per la:

- distribuzione ai Titolari delle Tessere mod. ATe ricevute dal CMS;
- conservazione per 20 anni della documentazione necessaria per la richiesta di emissione/rinnovo della tessera mod. ATe;
- raccolta e inoltro al CMS delle richieste di sospensione e/o revoca;
- raccolta delle Tessere mod. ATe scadute e/o revocate, da consegnare al CMS;
- "nodo informativo" per i Titolari appartenenti alla LRA in diritto di richiedere e/o usufruire della tessera mod. ATe e dei servizi a essa associati.

3.5. TITOLARE DELLA CARTA

Il Titolare della tessera mod. ATe ha la responsabilità di:

- prendere visione della documentazione relativa all'attuazione della disciplina in materia di utilizzo dei certificati digitali e di protezione dei dati;
- prendere visione dell'informativa ai sensi dell'art.13 del D.Lgs n. 196/2003 sull'attività di raccolta dei dati personali predisposta in Allegato A alla presente direttiva (pagina 5);
- custodire il codice di emergenza della carta, valido per 10 anni, necessario per il recupero dei segreti della carta e le comunicazioni di smarrimento e furto;
- conservare la tessera mod. ATe in modo conforme al fine di non comprometterne gli utilizzi previsti dalla presente Direttiva;
- 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 della tessera mod. ATe, segnalando immediatamente l'evento all'Ufficio preposto dell'Ente di appartenenza.

In caso di recidività o grave inosservanza da parte del Titolare nella gestione e nell'utilizzo della tessera mod. ATe dovranno essere adottate le misure disciplinari previste dai regolamenti, dalle norme contrattuali e dalla legge in materia disciplinare[15]. Nel caso in cui i danni alla carta evidenzino dolo o colpa grave da parte del Titolare, potranno essere applicate le sanzioni di cui al capo 7° del Regio Decreto del 18 novembre 1923 n. 2440.

15 Es. Decreto Legislativo 15 marzo 2010, n. 66 Codice dell'ordinamento militare e del Codice di comportamento (DPCM 28 novembre 2000) per il personale civile.

4. TESSERA MODELLO ATE

4.1. GENERALITÀ

La tessera mod. ATe risponde ai requisiti del DPCM 24 maggio 2010 (modificato con DPCM 18 gennaio 2016) recante le "Regole tecniche delle Tessere di riconoscimento rilasciate con modalità elettronica dalle Amministrazioni dello Stato"[16] ed è costituita da una tessera in policarbonato contenente varie tipologie d'informazioni utilizzabili nell'ambito della Pubblica Amministrazione e, più specificamente, della Difesa.

4.2. CARATTERIZZAZIONE DEL MOD. ATE

La tessera mod. ATe costituisce la tessera personale di riconoscimento in formato elettronico rilasciato al personale militare e civile in servizio della Difesa. Viene **inizializzata** presso **l'Istituto Poligrafico della Zecca dello Stato (IPZS)** e consegnata all'Amministrazione Difesa che provvede alla sua personalizzazione presso il CMS.

Nella fase d'inizializzazione della carta sono opportunamente predisposti gli spazi dedicati ai certificati digitali, agli elementi biometrici e di sicurezza.

Figura 1 – *Layout* Carta

Alla ricezione dei dati acquisiti e validati dalle ***Local Registration Authority (LRA)***, il CMS provvede:

- alla **personalizzazione** dei certificati digitali da inserire nella tessera mod. ATe necessari all'autenticazione in rete e alla firma digitale con i dati del Titolare;
- alla **consegna** della carta alla ***Local Registration Authority (LRA)*** richiedente (spedizione a mezzo posta ovvero ritiro a mano presso il Comando C4 Esercito in Via Guido Reni, 22 Roma).

Sul lato frontale, la tessera mod. ATe riporta i dati anagrafici e la foto del Titolare: le informazioni riportate conferiscono alla tessera mod. ATe la possibilità di essere impiegata come *documento di riconoscimento a vista* del Titolare stesso.

Sul lato posteriore sono riportati i dati fisici, il comune di residenza, il codice fiscale, il codice a barre per la cattura ottica dei dati e il campo NOTE dove, nel caso sia previsto, è riportata in sede di acquisizione:

- l'eventuale dicitura "non valido per l'espatrio";
- l'eventuale codice alfanumerico (Es. registro del personale della Difesa in possesso di titoli aeronautici gestito dall'Aeronautica Militare) relativo al titolo posseduto dal Titolare presente tra quelli autorizzati ed elencati in all'Allegato I alla presente direttiva.

16 DPCM 24 maggio 2010 recante *"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. Lgs. 82/2005"*.

All'interno della carta, inoltre, è inserito un chip costituente il "cuore" tecnologico della tessera mod. ATe che contiene le chiavi private e i corrispondenti certificati di:

- firma digitale;
- autenticazione **CNS** (**Carta Nazionale dei Servizi**).

Inoltre, per far fronte a ulteriori esigenze ravvisate in ambito Difesa, all'interno del chip è stato inserito un terzo certificato per la cifratura dei documenti e delle email.

Così come strutturata, la tessera mod. ATe consente quindi di svolgere **tre principali funzioni**:

1) *documento di identificazione a vista del Titolare;*
2) *identificazione e autenticazione personale per l'uso dei servizi informatici abilitati alle funzioni CNS;*
3) *apposizione della firma digitale.*

4.3. DESTINATARI DEL MOD. ATE

L'emissione della tessera mod. ATe avviene:

- nel momento in cui nuove risorse umane entrano a far parte dell'Amministrazione Difesa;
- nei casi in cui sussiste la necessità di dotare il personale di una nuova carta perché scaduta o revocata.

In particolare, la carta dovrà essere rilasciata (Allegato L):

- a tutto il personale militare e civile in servizio presso l'Amministrazione Difesa, compreso il personale militare VFP1 e Allievo delle Scuole Militari [17]. Per queste ultime due tipologie di personale militare è auspicabile che il rilascio della tessera mod. ATe avvenga nelle fasi iniziali dell'incorporamento senza attendere l'assegnazione ai Reparti d'impiego;
- al personale della **Magistratura Militare**, dell'**Agenzia Industrie Difesa** (**AID**), del **Corpo Militare della Croce Rossa Italiana** (**CRI**) e del **Sovrano militare Ordine di Malta** (**SMOM**).

Per esigenze particolari (Es. impiego fuori area) la tessera mod. ATe potrà essere rilasciata anche a personale in servizio momentaneo presso l'Amministrazione della Difesa.

La tessera mod. ATe dovrà essere revocata e/o ritirata a cura dell'Ufficio/Sezione Personale dell'EDRC dove il personale presta servizio e consegnata alla LRA di competenza per la successiva restituzione al CMS:

- al personale civile posto in pensione;
- al personale in servizio temporaneo al momento del collocamento in congedo illimitato;
- al personale militare in quiescenza, in ausiliaria o in riserva al momento del collocamento in congedo assoluto[18];
- al personale militare rimosso dal grado o degradato;
- al personale militare e civile a carico del quale è stato adottato un provvedimento di sospensione cautelare obbligatoria a norma delle disposizioni vigenti.

Per la gestione del personale militare al momento del collocamento in congedo assoluto le **Forze Armate** dovranno predisporre delle direttive interne comprensive della procedure di riconsegna della tessera ATe prevedendo, se necessario, il rilascio di una diversa tipologia di tessera (es. iscrizione Associazione d'Arma).

17 Sono esclusi i frequentatori delle Scuole di formazione militare.
18 Art. 1009 del Decreto Legislativo 15 marzo 2010, n. 66 – Codice dell'ordinamento militare. Al raggiungimento del congedo assoluto il Titolare della Tessera mod. ATe deve restituire la carta ad una delle *Local Registration Authority* dislocate sul territorio nazionale.

Al fine di ridurre le emissioni dei modelli ATe al personale in argomento, in caso di richiami vicini nel tempo, al termine del periodo di servizio attivo si potrà prevedere la "sospensione" della carta e la riconsegna alle Segreterie Generali di Reparto in alternativa alla "revoca", mentre le credenziali per l'utilizzo dei certificati digitali a bordo della stessa (PIN/PUK carta/firma) dovranno rimanere ad uso esclusivo del Titolare della carta al fine di prevenire eventuali usi illeciti attraverso la dissociazione del dispositivo fisico (modello ATe) e degli elementi di sicurezza (codice di emergenza e PIN/PUK carta e firma). Tale procedura dovrà prevedere la compilazione di un apposito verbale di consegna della carta nel quale dovrà essere indicato l'esatto periodo di sospensione e il nominativo del personale responsabile della custodia del modello ATe.

4.4. DURATA

La tessera mod. ATe, svolgendo anche il ruolo di documento d'identità, ha un limite temporale di validità non superiore ai 10 anni, come previsto dalle norme in vigore[19]. È tuttavia necessario considerare che la carta possa essere sostituita prima del normale termine, anche per motivi riconducibili a una perdita parziale o totale di una delle funzioni assolte (Es. *illeggibilità dei dati stampigliati sulla carta, malfunzionamenti dei certificati, danni strutturali al supporto, danni al chip, ecc.)*, secondo procedure dettagliato all'interno dei capitoli successivi. Il cambio di residenza non costituisce motivo di rinnovo della carta mentre costituisce motivo di rinnovo della carta il cambio di categoria. Per il personale non in servizio attivo, la scadenza della carta non potrà essere superiore alla data prevista per il collocamento in congedo assoluto.

4.5. PRIORITÀ NELLA PROCEDURA DI EMISSIONE DELLA CARTA

La procedura ordinaria di emissione delle carte, segue la naturale cronologia delle richieste inoltrate al CMS. **È tuttavia possibile che si verifichino eventi che stabiliscano un regime di priorità straordinaria.** Sono considerate di priorità straordinaria, tutte quelle richieste che, se non soddisfatte in un tempo inferiore a quello ordinario, rendono impossibile il normale operato del Titolare (Es. è possibile che il Titolare di una tessera mod. ATe prossima alla scadenza, debba essere impiegato in un teatro operativo fuori dal territorio nazionale: per evitare che la tessera mod. ATe perda la sua validità durante il periodo di missione, verrà eseguita una nuova emissione che, necessariamente, dovrà essere soddisfatta prima della sua partenza).

La scelta dell'attribuzione del regime di priorità straordinaria è demandata al Responsabile del trattamento[20] in fase di acquisizione presso la LRA e, sarà gestita in maniera automatizzata dal sistema. In presenza di code di stampa, qualora il criterio cronologico non sia applicabile in funzione dell'elevata richiesta di applicazione della procedura di priorità straordinaria, il CMS potrà stabilire in maniera manuale quale delle richieste con priorità straordinaria debba essere processata prima delle altre.

19 Decreto-Legge 9 febbraio 2012 , n. 5 (Art. 7, comma 3) "*Le tessere di riconoscimento rilasciate dalle amministrazioni dello Stato ai sensi del decreto del Presidente della Repubblica 28 luglio 1967, n. 851, hanno durata decennale"*

20 Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", art. 29.

Pagina intenzionalmente bianca

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

5.1. GENERALITÀ

L'Infrastruttura a chiave Pubblica della Difesa (PKI) del Comando C4 Difesa - Ente di Certificazione accreditato presso l'Ag.ID - fornisce alla tessera mod. ATe tre certificati digitali di:

- firma digitale;
- autenticazione CNS;
- cifratura per particolari esigenze della Difesa.

Il certificato di Firma Digitale, garantisce l'autenticità della sottoscrizione, l'integrità del documento e la non ripudiabilità da parte del Titolare. Un documento firmato con firma digitale, ai sensi dell'art. 24 del CAD, ha l'efficacia prevista dall'art. 2702 del Codice Civile.

Il certificato di Autenticazione CNS consente al Titolare di essere "riconosciuto in rete" con assoluta certezza e, quindi, permettergli di accedere ai servizi resi disponibili *on-line* dalle 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).

Il certificato di cifratura consente al Titolare della carta di criptare documenti ed email con il certificato di cifratura del personale che deve ricevere le informazioni. Le modalità di configurazione dei sistemi e le procedure di utilizzo del certificato di cifratura sono disponibili sul sito del Comando C4 Difesa.

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

STATO MAGGIORE DIFESA - Comando C4 Difesa - 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 Titolare di tessera mod. ATe è tenuto a prendere visione e approfondire gli aspetti inerenti la firma digitale e l'autenticazione CNS attraverso la consultazione dei Manuali Operativi e degli avvisi agli utenti resi disponibili dal Certificatore all'indirizzo:

http://c4d.difesa.it/Sistemi/CertificazioneConservazione/Pagine/default.aspx

https://pki.difesa.it/tsp

o, in alternativa, sul sito dell'AgID:

http://www.agid.gov.it/identita-digitali/firme-elettroniche/certificatori-attivi.

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*);
- 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.

Pagina intenzionalmente bianca

6. PROCESSI DI SERVIZIO DELLA CMD/MODELLO ATE

6.1. GENERALITÀ

Il termine "**processo di servizio**" indica l'insieme di attività che, a partire da "**risorse in ingresso**" *(risorse tecnologiche, umane, informative, ecc.)* realizzano un "**prodotto finale**" destinato a potenziali utenti. A corredo di tale definizione, si aggiunge che:

- ***ogni processo di servizio:***
  - *deve risultare replicabile ed essere caratterizzato da parametri misurabili e monitorabili nel tempo mediante indicatori di prestazione chiave (**Key Performance Indicator** – **KPI**);*
  - *deve essere orientato al raggiungimento di uno o più obiettivi dell'Organizzazione nella quale il processo stesso si sviluppa e attua;*
  - *in quanto insieme di attività volte a trasformare le risorse in ingresso nel prodotto finale, può essere eseguito da personale, da macchine o sistemi specializzati, ovvero ancora da una combinazione di tali elementi.*
- ***il prodotto finale**, a sua volta, può essere costituito da beni, servizi, informazioni o da una qualsiasi combinazione di tali elementi.*

La tessera mod. ATe **contiene al suo interno certificati** digitali e, pertanto, i processi di servizio di seguito illustrati, sono strettamente correlati con i criteri e le procedure di rilascio, consegna, sospensione ed eventuale revoca dei certificati digitali.

6.2. CICLO DI VITA DELLA TESSERA MODELLO ATE

Di seguito sono indicate le fasi del ciclo di vita della carta:

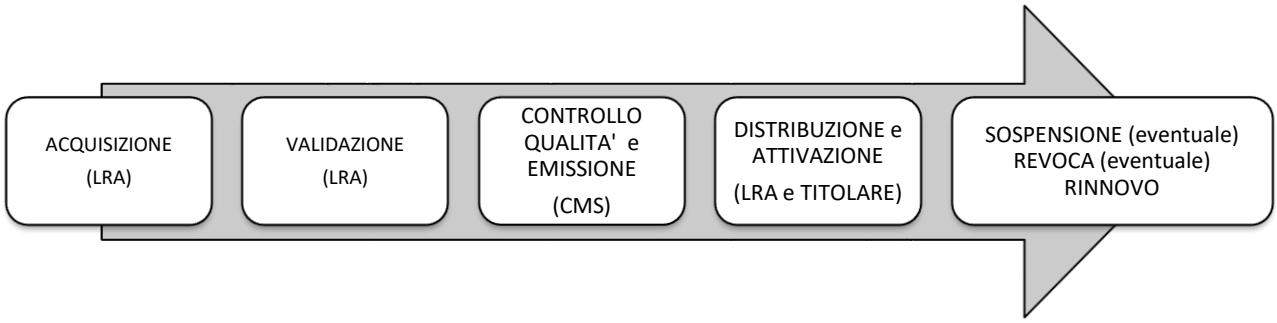


Figura 2 - Fasi del ciclo di vita del mod. ATe

- **Acquisizione.** Il processo di acquisizione è effettuato presso una qualsiasi ***Local Registration Authority*** **(LRA)**[21], in linea con i regolamenti interni delle F.A., presentando il modulo in Allegato A[22] debitamente compilato, che dovrà essere conservato agli atti per 20 anni. La pratica di acquisizione per il rilascio della tessera mod. ATe può avere inizio solo dopo la presentazione della richiesta cartacea (Allegato A – DPR 445/2000) provvista delle firme autografe del Titolare, del Comandante di Corpo/Delegato, se con figli minori dell'altro genitore e timbro a secco dell'EDRC responsabile. In fase di inserimento, il servizio provvede a interrogare la Banca Dati del CMS per avviare il processo di pre-caricamento dei dati del Titolare. In caso di difformità dei soli dati modificabili (Es. residenza) farà fede quanto dichiarato dal richiedente e certificato dal predetto Allegato A. Nel caso in cui i dati anagrafici del richiedente non siano presenti nella Banca Dati del CMS e sussiste la necessità di richiedere la tessera mod. ATe per esigenze di

21 Il personale non più in servizio attivo può recarsi ~~solo~~ presso una LRA della F.A. di provenienza.
22 L'Allegato A deve essere conservato presso le LRA per almeno 20 anni.

servizio urgenti, le LRA possono comunque procedere all'acquisizione dando comunicazione dell'assenza del richiedente nella banca dati agli organi responsabili dell'inserimento del personale nei Data Base di F.A./Persomil.

- **Validazione.** La validazione dei dati acquisiti è di competenza del Responsabile del trattamento (Allegato C). Il processo attiva la procedura di trasmissione dei dati al CMS per l'avvio delle fasi successive della produzione.
- **Emissione.** Il processo di emissione presiede al rilascio[23] della tessera mod. ATe e include tutte le attività necessarie per finalizzare la consegna della carta al "Titolare"[24]. Tutte le attività di emissione sono gestite dal personale del CMS.
- **Attivazione e Consegna.** La tessera mod. ATe viene distribuita all'interno dell'A.D. attraverso la consegna a cura del CMS alla LRA che provvede a consegnarla esclusivamente al Titolare, contestualmente alla fase di attivazione.
- **Rinnovo tramite sostituzione del supporto.** Questo processo si attiva alla naturale scadenza della carta e ogni volta che si verifica un deterioramento o un danneggiamento del supporto fisico. Il rinnovo prevede la sostituzione completa della tessera mod. ATe e dei relativi certificati.

Di seguito, invece, si elencano le attività da attuare in occasione di eventi negativi (es. smarrimento, sospensione dal servizio):

- **Sospensione.** Il processo di sospensione dei certificati porta la tessera mod. ATe in uno stato "temporaneo", che precede quello di revoca. In particolare, questo processo viene istanziato in tutti quei casi in cui sia necessario "sospendere" momentaneamente i servizi erogati dalla carta per procedere ad attività urgenti volte a verificare la persistenza di tutti i requisiti necessari per la sua validità. Al periodo di sospensione segue inevitabilmente o la riattivazione della carta o la sua revoca. In caso di riattivazione, la carta e i certificati vengono considerati "mai sospesi"; in caso di revoca la carta e i certificati vengono considerati revocati dal primo giorno di sospensione.
- **Revoca.** Il processo di revoca invalida i certificati digitali della tessera mod. ATe e li annulla definitivamente: si tratta pertanto di un processo irreversibile.

Con riferimento ai processi di "**Sospensione**" e di "**Revoca**" dei certificati digitali, si evidenzia quanto segue:

1. il **DPCM 22 febbraio 2013** *(recante "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali…<omissis>")* e successive modifiche prescrive:
   - l'obbligo, per il Certificatore, di fornire al Titolare almeno un *"**Codice di emergenza**"*, da utilizzare per richiedere la sospensione del certificato nei casi di emergenza;
   - le modalità operative per procedere alla *"**richiesta di revoca**"* su iniziativa del Certificatore, del Titolare e del Terzo interessato. Sia il Titolare che il Terzo interessato inviano la richiesta di revoca al Certificatore che è tenuto ad accertare l'autenticità della richiesta attivando, ove necessario, il processo di sospensione;
   - le modalità operative per procedere alla *"**richiesta di sospensione**"* su iniziativa del Certificatore, del Titolare e del Terzo interessato. Sia il Titolare che il Terzo interessato

23 Di fatto il processo di "**Emissione**" viene istanziato in occasione del primo rilascio ma anche degli eventuali rilasci successivi, a loro volta attivati in concomitanza con gli "eventi" più avanti descritti.

24 Nella Direttiva il termine "**Titolare**" viene utilizzato per indicare la persona fisica alla quale viene consegnata (ed affidata, ai fini della cura nel suo mantenimento) la Tessera mod. ATe e l'eventuale certificato di Firma Digitale posto a bordo della stessa. In alcuni casi, viene anche usato il termine "**Destinatario**" (coincidente con il "Titolare"), per enfatizzare il concetto di persona fisica che fruisce dei servizi erogati dalla Tessera mod. ATe.

inviano la richiesta di sospensione al Certificatore che è tenuto ad accertare l'autenticità della richiesta;
- il contenuto minimo del *"**Manuale Operativo**"*, redatto, pubblicato e aggiornato dal Certificatore *(in modo da consentirne l'accesso e la consultazione anche per via telematica)*, nel quale sono definite le procedure applicate dal Certificatore stesso nello svolgimento della sua attività;

2. **la durata temporale del "periodo di sospensione"** non è regolamentata ma viene definita di volta in volta dal Certificatore, in relazione alla specifica richiesta o in funzione delle cause che l'hanno generata ovvero, ancora, in funzione delle motivazioni addotte dal Titolare o dal Terzo interessato;
3. **il processo di "Revoca"** può essere attivato:
   - **direttamente**, tramite esplicita richiesta;
   - da una precedente "**Sospensione**", poi commutata in revoca definitiva.
4. **per chiarezza espositiva**, nel prosieguo della Direttiva **si presume che la revoca sia sempre preceduta da una sospensione**, prevedendo (come caso limite) la revoca diretta ottenuta ipotizzando un periodo di sospensione nullo *(quindi con tempo di sospensione pari a "**0**")*.

6.3. PROCEDURE DI ACQUISIZIONE DATI E RILASCIO TESSERA MODELLO ATE E CERTIFICATI DIGITALI

6.3.1. ACQUISIZIONE DEI DATI

La procedura acquisizione dei dati (*enrollment*), avviene presso i Locali Centri di Registrazione[25] (***Local Registration Authority*** - LRA) predisposti dalle F.A. e autorizzati dal Comando C4 Difesa[26] previa nomina del Responsabile del trattamento e degli Incaricati del trattamento[27] dei dati (Allegato F) e ha inizio solo dopo presentazione della richiesta cartacea (Allegato A) debitamente compilata dal richiedente e certificata dalla firma del Comandante di Corpo/Delegato.

Non è possibile rilasciare tessere di riconoscimento valide per l'espatrio a personale con figli minori senza l'assenso di chi ha la responsabilità genitoriale[28], allegando copie fotostatiche dei relativi documenti di riconoscimento, ovvero l'eventuale sentenza da cui si evinca a chi rimanga attestata tale responsabilità[29].

Il Responsabile del trattamento (Allegato C), effettuata l'identificazione del richiedente a vista o con 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 firma dell'Allegato A, dell'informativa specifica relativa all'utilizzo dei dati personali che dovrà essere firmata dal richiedente pena l'impossibilità di procedere con la procedura di emissione della tessera mod. ATe;
- all'acquisizione dei dati anagrafici, militari, amministrativi e della fotografia (formato in Allegato D), attraverso specifiche procedure, oltre ad una eventuale ulteriore e_mail e numero telefonico per l'invio di comunicazioni;
- alla conferma da parte del richiedente, con firma grafometrica (nome e cognome) leggibile, dei dati raccolti;

25 La soppressione/creazione di una LRA deve essere preventivamente formalizzata al Certificatore (C.do C4 Difesa).
26 Elenco LRA attive: http://portalecmd.difesa.it/
27 Decreto legislativo 30 giugno 200, n. 196 "Codice in materia di protezione dei dati personali", art. 30.
28 Che potrebbe essere anche di un soggetto diverso dal genitore.
29 Art. 330 del codice civile "decadenza dalla responsabilità genitoriale sui figli".

- a convalidare i dati raccolti controfirmandoli con la propria firma digitale.

Nella fase di pre-caricamento dei dati, il sistema prevede l'interrogazione e la restituzione dei dati dei titolari dalla Banca Dati Unica del CMS secondo il processo riepilogato in Figura 3.

In fase di acquisizione, in linea con i regolamenti interni delle F.A., è possibile apportare modifiche ai dati contenuti nei campi abilitati all'inserimento, pre-inizializzati in fase di acquisizione con le informazioni relative al richiedente già presenti nella banca dati del CMS (es. Comune e indirizzo di residenza, religione, grado/area di appartenenza, Status, ecc.). In tale circostanza faranno fede i dati rilasciati dal richiedente e certificati dal Comandante di Corpo/Delegato dell'Ente nell'Allegato A. Analogamente, per il personale non presente nella banca dati del CMS che necessita del rilascio della tessera mod. ATe per urgenti e improcrastinabili esigenze di servizio, sarà comunque possibile attivare una procedura di emissione della carta che dovrà essere comunque preceduta da una segnalazione a cura dei Comandi/Enti di appartenenza del richiedente di inserimento nella banca dati di F.A./Persociv .

Relativamente alla fotografia, per l'acquisizione dovrà essere utilizzato un fondo bianco e si dovranno rispettare tutte le caratteristiche ICAO riepilogate in Allegato D. Il personale militare dovrà indossare l'uniforme.
Terminata la procedura d'inserimento, il Responsabile del trattamento della LRA convalida i dati attraverso un'apposita procedura di approvazione apponendo la propria firma digitale attraverso la quale provvede all'invio dei dati al CMS.

Per tutti i casi non esplicitati nella presente direttiva, si rimanda alle normative vigenti per il rilascio dei documenti d'identità e dei documenti validi per l'espatrio.

6.3.2. ACQUISIZIONE DEI DATI PRESSO ALTRO ENTE

Considerata la varietà e la frammentazione sul territorio degli Enti/Uffici della Difesa, non in tutti sarà costituto un Centro di Registrazione Locale (LRA). Il personale effettivo a tali Enti dovrà compilare l'Allegato A, farlo firmare al proprio Comandante di Corpo/Delegato e recarsi presso una LRA viciniore anche di altra F.A./Persociv, che si farà carico dell'acquisizione dei dati. Sul portale CMD è inserito l'elenco delle LRA attive dislocate sul territorio nazionale. Il personale non più in servizio attivo dovrà recarsi presso una LRA della F.A. di provenienza.

6.3.3. EMISSIONE E RILASCIO DELLA TESSERA MOD. ATE

Allo scopo di delineare sommariamente il processo di emissione della tessera mod. ATe, in gran parte automatizzato, si elencano di seguito i passi logici fondamentali compresi in tale procedura.

Il CMS ricevuta la richiesta di emissione della carta dalla LRA, esegue una verifica dei dati pervenuti e, se validi, richiede l'emissione dei certificati alla C.A. che vengono caricati a bordo della carta nella fase che precede la personalizzazione della stampa della tessera mod. ATe. Dopo aver verificato il corretto funzionamento della carta, avvia il processo di emissione:

- genera all'interno della carta la prima coppia di chiavi e inoltra alla C.A. una richiesta di certificato di autenticazione. La C.A. rilascia il certificato di autenticazione CNS. Al termine della procedura il certificato CNS viene installato a bordo della tessera mod. ATe;
- genera all'interno della carta la seconda coppia di chiavi e inoltra alla C.A. di firma una richiesta di certificato di firma digitale. La C.A. rilascia il certificato di firma digitale. Il certificato di firma digitale viene quindi installato a bordo della tessera mod. ATe;
- genera all'interno della carta la terza coppia di chiavi e inoltra alla C.A. di Cifra una richiesta di certificato di cifratura. La C.A. rilascia il certificato di cifra e lo pubblica sul proprio sito (LDAP). Memorizza in un proprio database la chiave privata corrispondente (procedura di *escrew*). Il certificato di Cifra viene quindi installato a bordo della tessera mod. ATe;

- inserisce i dati personali del Titolare nel chip;
- personalizza graficamente la carta e la invia alla stampa;
- a operazione ultimata con successo, il CMS pone la carta in stato di "prodotta" e invia, con procedura automatizzata, un avviso alla LRA che può provvedere al ritiro;
- a carta ritirata a cura della LRA, al Titolare, all'indirizzo di posta elettronica di F.A./PERSOCIV (Es. nome.cognome@<*forzaarmata*>.difesa.it), viene inviata una email contenente le informazioni di avviso di "CARTA DISTRIBUITA" comprensiva del codice necessario per il ritiro della propria carta e il memorandum di sicurezza per l'utilizzo della carta (stralcio in Allegato B);
- alla consegna da parte della LRA della tessera mod. ATe prodotta, il CMS invia, con procedura automatizzata, al Titolare della carta una seconda email di "CARTA ATTIVATA". L'email conterrà:
  - il CODICE DI EMERGENZA, da conservare per tutto il periodo di validità della carta (10 anni);
  - il codice necessario per accedere al portale tessera mod. ATe, utilizzabile una sola volta, e visualizzare i codici PIN e PUK relativi alla carta e alla firma digitale.

La consegna al Titolare della nuova tessera mod. ATe, è effettuata dall'Incaricato del trattamento dei dati della LRA da dove è stata inviata la richiesta di emissione. Il Titolare, collegandosi al *link* indicato nella email di "CARTA ATTIVATA", raggiungibile dalla sola rete INTRANET, utilizzando la nuova tessera mod. ATe con un lettore di smartcard, potrà accedere alla propria Area Riservata e visionare i codici PIN/PUK associati ai certificati presenti nel chip.

Con il ritiro della tessera mod. ATe, il Titolare si obbliga ad osservare tutte prescrizioni presenti nel memorandum di utilizzo della tessera mod. ATe ricevuto all'indirizzo di posta elettronica di F.A./PERSOCIV (Es. nome.cognome@<*forzaarmata*>.difesa.it).

La consegna delle tessere mod. ATe emesse dal CMS avviene alla LRA mediante due procedure:

- consegna a mano al rappresentante della LRA in possesso di delega da parte del Responsabile del trattamento accompagnata dall'elenco delle carte da ritirare;
- posta assicurata subordinatamente alla disponibilità di fondi.

In fase di ritiro delle nuove carte, i rappresentanti della LRA dovranno consegnare al CMS le tessere mod. ATe ritirate e disattivate, per la successiva distruzione.

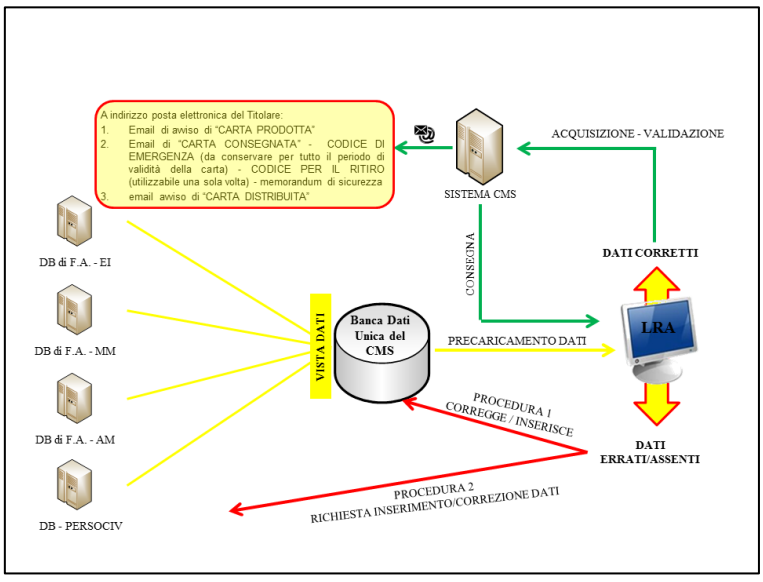


Figura 3 - Schema architetturale dell'infrastruttura dati mod. ATe

6.4. RINNOVO DELLA TESSERA MOD. ATE

6.4.1. GENERALITÀ

Al termine della sua durata di 10 anni, è necessario procedere alla sostituzione della carta riattivando il ciclo di vita della tessera mod. ATe già descritto in precedenza. Con l'emissione di una nuova carta, saranno generati nuovi certificati digitali con i relativi codici PIN e PUK, diversi da quelli preesistenti sulla carta scaduta. Il cambio di residenza non costituisce motivo di rinnovo della carta.

6.4.2. DESCRIZIONE DELLE FASI

Circa 90 giorni prima della scadenza della tessera mod. ATe il CMS, con procedura automatizzata, invia un'email di avviso al Titolare della carta. Dalla ricezione della stessa, il personale può recarsi presso la LRA competente per effettuare la nuova acquisizione dei dati.

Il Responsabile del trattamento della LRA di riferimento può validare l'acquisizione dei dati fino a un massimo di 30 giorni prima e comunque non meno di 7 giorni dalla data di scadenza.

Alla ricezione della nuova tessera mod. ATe, l'Incaricato del trattamento della LRA deve:

- convocare il Titolare della nuova carta;
- consegnare al Titolare la nuova carta ritirando contestuale la tessera mod. ATe oggetto di rinnovo;
- restituire al CMS la carta ritirata.

La LRA deve garantire la restituzione delle tessere mod. ATe revocate, non ancora riconsegnate, entro il primo trimestre dell'anno successivo perché aventi natura di carte-valori e di materiale a stretta rendicontazione.

6.5. SOSPENSIONE DELLA TESSERA MODELLO ATE E CERTIFICATI DIGITALI

6.5.1. TESSERA MODELLO ATE

I possibili eventi che possono portare alla sospensione della tessera mod. ATe 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 della tessera mod. ATe: ad es. impossibilità di accedere alle funzioni di firma digitale e/o errore nell'accesso ai servizi/sistemi informativi della P.A., con relativa mancata operatività della carta, ecc.);*
- ***sospetto smarrimento del documento****. A riguardo, entro il termine massimo di 10 giorni il Titolare della carta 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*** *(Es. sospensione disciplinare temporanea dal servizio)****;***
- ***uso improprio della carta da parte del Titolare****.*

6.5.2. CERTIFICATI DIGITALI

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.

6.5.3. FORMALIZZAZIONE DELLA RICHIESTA

Il processo di sospensione, le cui fasi sono dettagliate in Allegato H, è attivato attraverso la formalizzazione di una richiesta che deve sempre contenere la descrizione dettagliata delle motivazioni della sospensione:

- **su iniziativa del Certificatore** [28] *(DPCM 22 febbraio 2013 – art. 27):*
  - *"…salvo casi d'urgenza …<omissis>… il Certificatore che intende sospendere un certificato qualificato ne dà preventiva comunicazione al Titolare e all'eventuale terzo interessato specificando i motivi della sospensione e la sua durata…";*
  - *"…se la sospensione è causata da una richiesta di revoca motivata dalla possibile compromissione della chiave privata, il Certificatore procede tempestivamente alla pubblicazione della sospensione…";*
- **su richiesta del Titolare** *(DPCM 22 febbraio 2013 – art. 28):*
  - *"…la richiesta di sospensione del certificato qualificato, con la specificazione della sua durata, è inoltrata al Certificatore* [29]*, secondo le modalità indicate nel manuale operativo…"*
  - *"…il Certificatore verifica l'autenticità della richiesta e procede alla sospensione entro il termine richiesto…";*
- **su richiesta del Terzo interessato**[30] *(DPCM 22 febbraio 2013 – art. 29):*
  - *"…la richiesta di sospensione del certificato qualificato da parte del Terzo interessato, da cui derivano i poteri di firma del Titolare, è inoltrata al Certificatore munita di sottoscrizione e con la specificazione della sua durata…".*

La durata dello stato di sospensione, ove non esplicitamente richiesto dal Titolare o dal Terzo interessato, è definita dal Certificatore in relazione alle motivazioni che hanno generato la sospensione stessa. Al termine del periodo, la carta dovrà essere:

- nuovamente abilitata, se sono decaduti i motivi che hanno portato alla sospensione (Es. ritrovamento del documento);
- ovvero revocata.

6.5.4. VALUTAZIONE DELLA RICHIESTA

Il Certificatore è l'unica Autorità preposta alla valutazione della richiesta. Tra i suoi compiti, rientra la verifica della corretta applicazione degli aspetti formali e l'eventuale attuazione della sospensione. La valutazione può avere due possibili stati:

- esito negativo: il Certificatore richiede al Titolare o al Terzo interessato l'aggiornamento o l'integrazione della documentazione fornita ("Adeguamento della documentazione");
- esito positivo: il Certificatore istruisce la pratica di sospensione che, a sua volta, avvia il periodo di sospensione ("Istruzione della pratica di sospensione").

---

28 Il "**Certificatore**" rappresenta l'autorità che assevera la corrispondenza *(associazione biunivoca)* del Titolare alla sua chiave pubblica. Il Certificatore rende disponibile una lista aggiornata delle chiavi pubbliche in uso e di quelle revocate o sospese.

29 Comando C4 Difesa.

30 Il "**Terzo interessato**" dispone della sola facoltà di richiedere al Certificatore la "Sospensione" o la "Revoca" della carta ovvero dei certificati digitali *(Artt. 23, 24, 25, 27, 28 e 29, DPCM 22 febbraio 2013).*

6.5.5. AVVIO DEL PERIODO DI SOSPENSIONE

Quale conseguenza dell'avvio del periodo di sospensione, il Certificatore provvede a:

- *aggiornare gli elenchi dei certificati, registrando ogni cambio di stato dei certificati del Titolare, annotandone tutti i dettagli previsti dalla legge;*
- *predisporre e inviare (al Titolare e al Terzo interessato) le comunicazioni di inizio e di fine del periodo di sospensione, ovvero di revoca (nel caso la sospensione sfoci in tale stato definitivo).*

Il periodo di sospensione può essere interrotto al ripristino della corretta funzionalità della tessera mod. ATe.

In caso contrario, la sospensione evolverà con l'avvio del **processo di Revoca**.

6.6. REVOCA DELLA TESSERA MOD. ATE E DEI CERTIFICATI DIGITALI

Il processo di revoca è avviato per perdita del grado, smarrimento, furto o compromissione della tessera mod. ATe, o quando vi è un utilizzo della carta non conforme agli scopi e ai metodi di utilizzo previsti dalla presente Direttiva e/o dalle leggi in vigore. La compromissione, in modo particolare, prevede la revoca 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 nella tessera mod. ATe ovvero della carta stessa. 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 di appartenenza del Titolare. In caso di revoca della tessera mod. ATe anche come documento di riconoscimento la carta deve essere ritirata a cura della LRA e consegnata per la distruzione al CMS.

6.6.1. FORMALIZZAZIONE DELLA RICHIESTA

Il processo di revoca della tessera mod. ATe o di un suo certificato (a seguito di un precedente periodo di sospensione ovvero attraverso la formalizzazione di una specifica richiesta) può essere avviato:

- **su iniziativa del Certificatore** *(DPCM 22 febbraio 2013 – art. 23):*
  - *"…salvo i casi di motivata urgenza, il Certificatore che intende revocare un certificato qualificato ne dà preventiva comunicazione al Titolare, specificando i motivi della revoca nonché la data e l'ora a partire dalla quale la revoca è efficace …";*
- **su richiesta del Titolare** *(DPCM 22 febbraio 2013 – art. 24):*
  - *"…la richiesta di revoca è inoltrata al Certificatore munita della sottoscrizione del Titolare e con la specificazione della sua decorrenza.*
  - *..<omissis>…*
  - *il Certificatore verifica l'autenticità della richiesta e procede alla Revoca entro il termine richiesto …<omissis>…*
  - *se il Certificatore non ha la possibilità di accertare in tempo utile l'autenticità della richiesta, procede alla sospensione del Certificato…";*
- **su richiesta del Terzo interessato** *(DPCM 22 febbraio 2013 – art. 25):*
  - *"…la richiesta di revoca da parte del Terzo interessato da cui derivano i poteri di firma del Titolare è inoltrata al Certificatore munita di sottoscrizione e con la specificazione della sua decorrenza;*
  - *in caso di cessazione o modifica delle qualifiche o del titolo inserite nel certificato su richiesta*

del Terzo interessato, la richiesta di revoca è inoltrata non appena il Terzo venga a conoscenza della variazione di stato;

- *se il Certificatore non ha la possibilità di accertare in tempo utile l'autenticità della richiesta, procede alla sospensione del certificato…"*

La richiesta deve comunque contenere una descrizione dettagliata delle motivazioni che hanno portato alla sospensione.

6.6.2. REVOCA PER FURTO/SMARRIMENTO

In caso di furto/smarrimento, il Titolare deve dare immediata comunicazione all'Ente di appartenenza. Qualora ciò non sia possibile, l'interessato deve contattare il n. 0646914444 (Comando C4 Difesa) attivando così la **sospensione** immediata della tessera mod. ATe. Inoltre il Titolare 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 di appartenenza del Titolare che avrà comunque l'obbligo di trasmettere al CMS i riferimenti della pratica di smarrimento. Qualora non ci siano ulteriori comunicazioni, trascorsi 15 giorni la tessera mod. ATe verrà revocata".

6.6.3. REVOCA PER CAMBIO DELLO STATUS GIURIDICO

Il processo di revoca per cambio di status si verifica, ad esempio, quando un civile, impiegato presso l'Amministrazione Difesa, cambia amministrazione di appartenenza (*Es.: da Ministero della Difesa al Ministero di Giustizia*), ovvero quando il proprietario della tessera mod. ATe, da militare transita nello stato civile. Il cambio di status, difatti, segna il termine di possesso e uso della tessera mod. ATe che viene revocata perdendo tutte le sue funzionalità.

6.6.4. AGGIORNAMENTO DEGLI ELENCHI DEI CERTIFICATI

Quale conseguenza dell'avvenuta revoca dei certificati la *Certification Authority* provvede all'aggiornamento degli elenchi pubblici dei certificati nonché a tutti i compiti e le attività di dettaglio inerenti allo svolgimento dell'attività di Certificatore accreditato.

Pagina intenzionalmente bianca

7. DATI PERSONALI CONTENUTI NELLA TESSERA MODELLO ATE.

7.1. GENERALITÀ

Il trattamento dei dati personali, riepilogati nell'Allegato A alla presente direttiva, avviene unicamente per consentire l'emissione della tessera di riconoscimento rilasciate dalle amministrazioni dello Stato ai sensi del D.P.R. 28 luglio 1967, n. 851, anche con modalità elettroniche affinché contengano le funzionalità per consentire l'accesso per via telematica ai servizi erogati in rete. Tutti i dati acquisiti non vengono utilizzati in altre operazioni di trattamento che siano con questo incompatibili.

Per la funzionalità di cui sopra, la tessera mod. ATe può contenere dati personali, nel rispetto delle disposizioni contenute nel codice in materia di protezione dei dati personali.

7.2. MODALITÀ DI FUNZIONAMENTO DELLA PROCEDURA INFORMATIZZATA PER IL RILASCIO E IL RINNOVO DELLA TESSERA MOD. ATE.

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

   - che i dati personali in argomento sono rilevati esclusivamente per consentire al Ministero della Difesa di rilasciare la tessera mod. ATe secondo le specifiche previste dal DPCM 24 mag. 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 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 modello ATe con conseguente limitazione all'identificazione ed all'autenticazione nelle reti della Difesa, necessario a garantire l'accesso sicuro ai sistemi informativi;
   - non verrà richiesto il conferimento di altri dati personali oltre l'immagine del titolare, l'immagine della firma autografa, il gruppo sanguigno e, per particolari esigenze di sicurezza fisica e logica, in base ad espresse disposizioni di legge che li prevedano specificatamente e secondo quanto previsto dalle norme vigenti sulla protezione dei dati personali, il *template* dell'impronta digitale del dito indice di entrambe le mani (qualora non disponibile di altro dito: medio, anulare o pollice);
   - se acquisito, il *template* dell'impronta digitale sarà trascritto nel microchip della tessera mod. ATe del dipendente e non saranno diffuse né saranno conservate in banche dati di alcun tipo. Al momento dell'emissione della tessera mod. ATe, tramite una procedura di sicurezza interna al sistema, il *template* dell'impronta digitale è cancellato dal sistema in maniera sicura;
   - il richiedente è titolare dei diritti di cui all'articolo 7 del Codice in materia di trattamento dei dati personali;
   - il titolare del trattamento dei dati è il Ministero della Difesa, con sede in Via XX Settembre, 8 – 00100 Roma, ed è effettuato esclusivamente da personale incaricato.

b. Il sistema di acquisizione dei dati per il rilascio della tessera mod. ATe (militari, anagrafici e biometrici) 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* (CMS) unico, preposto all'emissione (stampa) della tessera mod. ATe, espone via web il servizio di acquisizione, attraverso il quale vengono raccolti i dati (militari, anagrafici ed eventualmente biometrici) del personale e scritti all'interno del filesystem della tessera mod. ATe. Durante il processo di emissione della carta, il CMS si interfaccia con le *Certification Authority* (C.A.) della Difesa, per il rilascio del certificato di autenticazione CNS, di firma digitale e di cifratura.
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'AgID.

7.3. ACQUISIZIONE DI ULTERIORI DATI PER PARTICOLARI ESIGENZE DI SICUREZZA FISICA O LOGICA.

Nel rispetto delle disposizioni del D.Lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali, in base a quanto ulteriormente specificato nel DPCM 24 maggio 2010 (modificato con DPCM 18 gennaio 2016), nell'ambito delle finalità proprie delle Tessere mod. ATe, la Difesa può utilizzare per particolari esigenze di sicurezza fisica o logica, informazioni biometriche come le impronte digitali del titolare della tessera mod. ATe. L'utilizzo di tali informazioni potrà avvenire solo nel rispetto della normativa in materia di protezione dei dati personali. A riguardo, prima del trattamento di dati biometrici che si intendono eventualmente effettuare nella tessera mod. ATe, le F.A. dovranno:

- circostanziare le particolari esigenze di sicurezza fisica o logica, che rendono necessario il ricorso al trattamento dei dati biometrici del personale per il raggiungimento di specifici scopi di sicurezza;
- interessare lo Stato Maggiore della Difesa VI Reparto – Sistemi C4I e Trasformazione affinché avvii il procedimento di verifica preliminare davanti al Garante per la protezione dei dati personali;
- selezionare il personale che, in relazione alle mansioni svolte ed agli incarichi ricoperti, dovrà essere sottoposto alla procedura di autenticazione tramite l'utilizzo del *template* delle impronte digitali;

In merito all'immagine dell'impronta digitale del personale, questa viene trasformata nel modello di riferimento da essa ricavato (c.d. *template*) già in fase di acquisizione dei dati raccolti in occasione del rilascio e del rinnovo della tessera mod. ATe. Il *template* non viene mai archiviato in banche dati centrali e nei sistemi informativi dell'Amministrazione della Difesa, ma viene salvato solo nella tessera mod. ATe, che rimane nell'esclusiva disponibilità dell'interessato per tutto il ciclo di vita della carta (presso l'Amministrazione della Difesa non esistono banche dati contenenti dei dati biometrici).

8. ELENCO DEGLI ANNESSI E DEGLI ALLEGATI ALLA DIRETTIVA

Elenco degli Annessi alla presente Direttiva:

- **ANNESSO 1**: Elenco delle definizioni.
- **ANNESSO 2**: Elenco degli acronimi.
- **ANNESSO 3**: Normativa di riferimento applicabile suddivisa in Leggi e Decreti, Direttive dell'A.D., Direttive della NATO, Direttive e standard nazionali e internazionali e Altri documenti.

Elenco degli allegati alla presente Direttiva:

- **ALLEGATO A**: Modulo di richiesta tessera mod. ATe.
- **ALLEGATO B**: Memorandum di Sicurezza per Titolari della tessera mod. ATe.
- **ALLEGATO C**: Compiti del Responsabile del trattamento e dell'Incaricato del trattamento dei dati.
- **ALLEGATO D**: Istruzioni sul formato ICAO della foto.
- **ALLEGATO E:** Membri del *Change Advisory Board.*
- **ALLEGATO F**: Facsimile atto di nomina del Responsabile e degli Incaricati del trattamento dei dati.
- **ALLEGATO G:** Livelli di servizio.
- **ALLEGATO H:** Rappresentazione grafica del processo di sospensione.
- **ALLEGATO I:** Elenco dei titoli autorizzati alla trascrizione nel campo NOTE della tessera mod. ATe.
- **ALLEGATO L:** Personale destinatario della tessera mod. ATe.
- **ALLEGATO M:** Matrice delle osservazioni/proposte.

Pagina intenzionalmente bianca

ANNESSO 1

ELENCO DELLE DEFINIZIONI

Ai fini della presente Direttiva, si applicano le definizioni contenute nel:

- **DPCM 22 febbraio 2013;**
- **Codice dell'Amministrazione Digitale (CAD).**

TERMINE	DEFINIZIONE
ACQ	Modulo logico di acquisizione dati.
Algoritmo di hashing	Una funzione di hash è un algoritmo che trasforma un numero qualsiasi di caratteri in un codice univoco di lunghezza fissa.
Autenticazione	Il processo che attraverso un certificato digitale e l'impiego della corrispettiva chiave privata garantisce l'autenticità del possessore.
Autorità di Certificazione/Certification Authority	L'autorità, legalmente riconosciuta, che rilascia e gestisce la vita dei certificati digitali.
Autorità di Registrazione	*Registration Authority* - entità che, su delega dalla *Certification Authority*, svolge tutte quelle azioni propedeutiche al rilascio dei certificati digitali in capo ad un Titolare. E' responsabile di tutto il processo di identificazione, validazione, consegna e ritiro dei supporti (smart-card) contenenti i certificati digitali e dei relativi segreti (Codici firma e autenticazione).
CA	Vedi Autorità di Certificazione.
Card / Carta / Tessera mod. ATe	La tessera mod. ATe (il supporto fisico) sulla quale sono stampigliati gli elementi identificativi del Titolare.
Tessera mod. ATe	La tessera rilasciata al personale della Difesa.
Centro di Certificazione	Il luogo scelto dal Certificatore dove operano le persone, le macchine e le procedure necessarie alla conduzione dei servizi di certificazione.
Certificati elettronici	Gli attestati elettronici che collegano all'identità del Titolare i dati utilizzati per verificare le firme elettroniche
Certificato qualificato	Il certificato elettronico contenuto nella tessera mod. ATe, conforme ai requisiti di cui all'Allegato I della direttiva 1999/93/CE, rilasciati da Certificatori che rispondono ai requisiti di cui all'Allegato II della medesima direttiva.
Certificatore/QTSP	Il soggetto (Prestatore di Servizi Fiduciari Qualificato eIDAS) che presta servizi di certificazione qualificati delle firme elettroniche o che fornisce altri servizi fiduciari qualificati connessi con queste ultime.

TERMINE	DEFINIZIONE
Certificazione	Il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto Titolare, si identifica quest'ultimo, si attesta il periodo di validità della predetta chiave e il termine di scadenza del relativo certificato.
Chiave	Sequenza di dati (stringa) di lunghezza arbitraria impiegata come parametro dall'algoritmo di cifratura/decifratura. La lunghezza della chiave determina la difficoltà di decodifica del messaggio non conoscendo la chiave di decodifica.
Chiave di sessione	Chiave che ha validità limitata alla durata di una sessione di lavoro.
Chiave privata	Elemento della coppia di chiavi asimmetriche, destinato a essere conosciuto dal soggetto Titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica.
Chiave pubblica	Elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal Titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al Titolare delle predette chiavi.
Chiavi asimmetriche	Coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici.
Cifratura di un file	La cifratura di un file è l'operazione mediante la quale applicando un algoritmo di cifratura con l'impiego di una chiave, si ottiene un file non intelligibile.
CIE	Carta d'Identità Elettronica del Ministero dell'Interno.
Cifratura	Processo di trasformazione dell'informazione (testo in chiaro o plaintext) in testo cifrato (o ciphertext), guidato da una chiave.
Ciphertext	Il risultato della cifratura. Il ciphertext o testo cifrato contiene le stesse informazioni del testo originale (plaintext) però nasconde l'informazione originale, generalmente con l'ausilio di una chiave e di un algoritmo di cifratura.
CMS	Card Management System - Struttura preposta alla emissione e gestione della tessera mod. ATe.
CNS	Carta Nazionale dei Servizi.
Compromissione (della carta / dei certificati / ecc.):	La sopravvenuta assenza di affidabilità nelle caratteristiche di sicurezza connesse con il supporto fisico o con le componenti tecnologiche della tessera mod. ATe, ovvero ancora con i certificati contenuti nella carta stessa.

TERMINE	DEFINIZIONE
Crittanalisi	Aspetto della crittologia, si occupa di analisi della robustezza dei sistemi crittografici e di ricerca di metodi per forzare i sistemi crittografici.
Crittografia	Disciplina che studia l'utilizzo e la creazione di crittosistemi. L'arte (la scienza) di trasformare le informazioni in una forma intermedia sicura. A differenza della steganografia, che cerca di nascondere l'esistenza di qualunque messaggio, la crittografia si occupa di rendere il messaggio illeggibile benché completamente accessibile. La crittografia comprende necessariamente la segretezza (confidenzialità) e l'integrità (autenticazione del messaggio). Può comprendere il non disconoscimento (l'impossibilità di negare l'avvenuto invio di un messaggio) ed il controllo d'accesso (autenticazione dell'utente).
Disponibilità	La possibilità di accedere ai dati contenuti nella tessera mod. ATe senza restrizioni non riconducibili a esplicite norme di legge.
Firma Elettronica	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica.
Firma Elettronica Avanzata	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.
Firma Elettronica Qualificata	Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma.
Firma Digitale	Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al Titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.
Local Registration Authority	Ente delegato dalla C.A. a svolgere le operazioni di acquisizione dei dati, consegna e ritiro delle Tessere mod. ATe.
Marca Temporale	Il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo.
Riferimento temporale	Evidenza informatica, contenente la data e l'ora, che viene associata ad uno o più documenti informatici.

TERMINE	DEFINIZIONE
Terzo interessato	La persona o il soggetto interessato da cui derivano i poteri di firma attribuiti al Titolare.
Titolare	La persona fisica cui è attribuita la tessera mod. ATe e la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica.

ANNESSO 2

ELENCO DEGLI ACRONIMI

SIGLA	ACRONIMO
A.D.	*Amministrazione Difesa*
Ag.ID	*Agenzia per l'Italia Digitale*
AIPA	*Associazione per l'Informatica nella Pubblica Amministrazione*
ALM	*Application Lifecycle Management*
ASP	*Application Service Provider*
CA	*Certification Authority*
CAB	*Change Advisory Board*
CAD	*Codice dell'Amministrazione Digitale*
CCI	*Comitato Coordinamento Informatica*
CIE	*Carta d'Identità Elettronica*
CM	*Change Management*
CMD	*Carta Multiservizi Difesa*
CMS	*Card Management System*
CNS	*Carta Nazionale dei Servizi*
CRL	*Certificate Revocation List*
DII	*Defence Information Infrastructure*
DPCM	*Decreto del Presidente del Consiglio dei Ministri*
EDRC	*Ente Distaccamento Reparto Comando*
F.A.	*Forze Armate*
KPI	*Key Performance Indicator*
ICAO	*International Civil Aviation Organization*
ICT	*Information and Communication Technology*
ITIL	*Information Technology Infrastructure Library*
LDAP	*Lightweight Directory Access Protocol*
LS	*Lead Service*
LRA	*Local Registration Authority*
OCSP	*Online certificate status protocol*
QTSP	*Qualified Trust Service Provider*
P.A.	*Pubblica Amministrazione*

SIGLA	ACRONIMO
PIN	*Personal Identification Number*
PKI	*Public Key Infrastructure*
PUK	*Personal Unblocking Key*
RA	*Registration Authority*
RFC	*Request For Change*
SIPAD	*Sistema Informativo del Personale Difesa*
SLA	*Service Level Agreement*
SMD	*Stato Maggiore della Difesa*

ANNESSO 3

NORMATIVA DI RIFERIMENTO

Per la realizzazione del presente documento si è fatto riferimento alle seguenti norme e direttive, per quanto applicabili:

- **NORME NAZIONALI**
  1. L. 21 novembre 1967, n. 1185 "*Norme sui passaporti*";
  2. L. 21 giugno 1986, n. 317 "*Procedura d'informazione nel settore delle norme e regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione in attuazione della direttiva 98/34/CE del Parlamento europeo e del Consiglio del 22 giugno 1998, modificata dalla direttiva 98/48/CE del Parlamento europeo e del Consiglio del 20 luglio 1998*";
  3. D.Lgs. 23 novembre 2000, n. 427 "*Modifiche ed integrazioni alla L. 21 giugno 1986, n. 317, concernenti la procedura di informazione nel settore delle norme e regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione, in attuazione delle direttive 98/34/CE e 98/48/CE*";
  4. D.Lgs. 30 giugno 2003, n. 196 "*Codice in materia di protezione dei dati personali*";
  5. D.Lgs. 7 marzo 2005, n. 82 "*Codice dell'amministrazione digitale*", e in part. l'art. 66, ottavo comma, che sancisce che "*le tessere di riconoscimento rilasciate dalle amministrazioni dello Stato ... possono essere realizzate anche con modalità elettroniche ... e contenere le funzionalità della carta nazionale dei servizi per consentire l'accesso per via telematica ai servizi erogati in rete dalle pubbliche amministrazioni*";
  6. L. 24 dicembre 2007, n. 244 "*Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato (legge finanziaria 2008)*", solamente art. 3, c. 83 (sistemi di rilevazione automatica delle presenze);
  7. D.Lgs. 15 marzo 2010, n. 66 "*Codice dell'ordinamento militare*", art. 1496;
  8. D.P.R. 28 luglio 1967, n. 851 "*Norme in materia di tessere di riconoscimento rilasciate dalle Amministrazioni dello Stato*";
  9. D.P.R. 6 agosto 1974, n. 649 "*Disciplina dell'uso della carta d'identità e degli altri documenti equipollenti al passaporto ai fini dell'espatrio*";
  10. D.P.R. 28 dicembre 2000, n. 445 "*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*", in particolare l'art. 35, secondo comma;
  11. D.M. (MEF) 4 agosto 2003 "*Istruzioni per la disciplina dei servizi di vigilanza e controllo sulla produzione delle carte valori, degli stampati a rigoroso rendiconto, degli stampati comuni e delle pubblicazioni ufficiali, nonché delle ordinazioni, consegne, distribuzione e dei rapporti con l'Istituto Poligrafico e Zecca dello Stato S.p.A.*";
  12. D.P.R. 2 marzo 2004, n. 117 "*Regolamento concernente la diffusione della carta nazionale dei servizi, a norma dell'articolo 27, comma 8, lettera b), della L. 16 gennaio 2003, n. 3*";
  13. D.L. 31 gennaio 2005, n. 7 "*Disposizioni urgenti per l'università e la ricerca, per i beni e le attività culturali, per il completamento di grandi opere strategiche, per la mobilità dei pubblici dipendenti, e per semplificare gli adempimenti relativi a imposte di bollo e tasse di concessione, nonché altre misure urgenti*", i soli artt. 7-vicies ter e 7-vicies quater;

SEGUITO ANNESSO 3

14. D.M.(I) 8 novembre 2007 "*Regole tecniche della Carta d'identità elettronica*";
15. D.P.C.M. 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 decreto legislativo n. 82 del 2005*";
16. D.P.C.M. 22 febbraio 2013 "*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*";
17. D.P.C.M. 24 ottobre 2014 "*Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese*";
18. D.P.C.M. 13 novembre 2014 "*Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni ai sensi degli articoli 20, 22, 23-bis, 23-ter, 40, comma 1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005*";
19. D.P.C.M. 18 gennaio 2016 "*Modifiche al decreto del Presidente del Consiglio dei ministri del 24 maggio 2010, recante: «Regole tecniche delle Tessere di riconoscimento (mod. AT) di cui al decreto del Presidente della Repubblica 28 luglio 1967, n. 851, rilasciate con modalità elettronica dalle Amministrazioni dello Stato, ai sensi dell'articolo 66, comma 8, del decreto legislativo 7 marzo 2005, n. 82*".

- **NORMATIVE, DIRETTIVE E STANDARD NAZIONALI E INTERNAZIONALI**

1. Direttiva CEE 22 giugno 1998, n. 98/34/CE "*Direttiva del Parlamento europeo e del Consiglio che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione*";
2. Direttiva CEE 13 dicembre 1999, n. 1999/93/CE "*Direttiva del Parlamento europeo e del Consiglio relativa ad un quadro comunitario per le firme elettroniche*";
3. Regolamento CE 23 luglio 2014, n. 910/2014 "*Regolamento del parlamento europeo e del consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE*".

- **DIRETTIVE DELLA NATO**

1. AC/322-D(2007)0048 "*NATO Architecture Framework*" version 3;

- **ALTRI DOCUMENTI**

1. F.n. M_D SSMD 0078014 datato 28 settembre 2010, resoconto di riunione del Comitato di Coordinamento Informatica del 21 settembre 2010;
2. F.n. 0052165 datato 29 ottobre 2010 con il quale SME esprime la propria disponibilità a svolgere il ruolo di *lead service* per il progetto CMD;
3. *Defence information infrastructure* (DII) requisito operativo definitivo:
   a) annesso 5-E, "*Adeguamento ed ammodernamento funzionale PKI*";
   b) annesso 5-L, "*Accesso ai servizi, applicazioni e dati attraverso la CMD*";

SEGUITO ANNESSO 3

4. Linee guida per l'utilizzo della firma digitale del CNIPA, ed. maggio 2004;
5. Circolare AIPA n. 24 datata 19 giugno 2000 per l'interoperabilità della firma digitale;
6. *Public Key Infrastructure* Firma Digitale Difesa -Autenticazione CNS - Manuale Operativo v. 1.0 – 1.3.6.1.4.1.14031.2.1.

Pagina intenzionalmente bianca

ALLEGATO A

MODULO RICHIESTA TESSERA MOD. ATE

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 DELLA ATe ☐ ATe MEDICO ☐ .

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

Grado/area di appartenenza[2] _____ Codice fiscale _____

In attività di servizio presso _____ Tel. Uff. _____

Data assunzione in servizio ___/___/____ scadenza vincolo ___/___/____ (se non in serv.perm).

DICHIARO/A QUANTO SEGUE:

DATI ANAGRAFICI

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

Sesso M - F Cittadinanza _____ Religione[3] _____

Stato civile: (celibe, coniugato, vedovo o stato libero ai sensi dell'art. 46 di cui al D.P.R. n 445/2000)
_____

Senza prole minore/con prole minore estremi atto di nascita[4] _____
(cancellare la casella **non** di interesse)

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

Via/piazza _____ nr. _____

Tessera che si verserà all'atto della consegna del nuovo modello ATe:

mod. ATe nr. _____ rilasciata da _____ in data ___/___/____

DATI AMMINISTRATIVI

Matricola _____ Categoria[5] _____
Ruolo[6] _____ Status[7] _____
Account email[8] _____@_____

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 …

2 Per il personale civile della A.D.

3 Dato non obbligatorio.

4 Dato non obbligatorio. Dato presente sulla carta d'identità cartacea o reperibile presso l'anagrafe di appartenenza.

5 Civile – Truppa – Graduato – Sottufficiale – Ufficiale.

6 Legge 196/95: Ruolo Marescialli – Ruolo Sergente

7 Servizio Permanente – Ferma prefissata – Riserva – Ausiliaria.

8 L'account email dovrà obbligatoriamente essere quello rilasciato dalla propria amministrazione (Es. nome.cognome@persociv.difesa.it). Se il dipendente non è in possesso di tale account, dovrà necessariamente chiederne il rilascio alla propria amministrazione prima di eseguire con l'acquisizione elettronica dei dati.

SEGUE ALLEGATO A

Eventuale altro account mail _____@_____n. Tel_____

Anzianità assoluta ___/___/____ Anzianità di grado/di livello ___/___/____ .

Incarico principale _____

Reparto di appartenenza/Ente di servizio _____

Titolare di pensione SI - NO

DATI PERSONALI

Gruppo Sanguigno[9] _____ Statura (cm) _____ Colore capelli _____

Colore occhi _____ Segni particolari _____

PROFILO DI FIRMA

Chiede l'emissione di un certificato personale di firma digitale[10]:

Senza limitazioni ☐ Solo per attività di servizio ☐

Inoltre, chiede che la tessera sia resa valida per l'espatrio e dichiara che non ricorrono le condizioni ostative al rilascio del documento.

_____, lì ___/___/____ _____ _____

(LUOGO) (DATA) (FIRMA DEL RICHIEDENTE) (FIRMA DELL'ALTRO GENITORE – Avvertenza .1)

Documento/tessera del richiedente e del/dei genitore/i del/dei figlio/i minore/i (allegare copia/e):

- richiedente: mod. ____ nr. _____ rilasciato da _____ data scadenza ___/___/____
- altro genitore: mod. ____ nr. _____ rilasciato da _____ data scadenza ___/___/____

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

9 Colui che richiede il nuovo modello ATe, durante la fase di acquisizione, dovrà mostrare all'Incaricato del trattamento dei dati un documento che attesti il proprio gruppo sanguigno per la stampa sulla carta. Sono documenti validi: la cartella sanitaria, il foglio matricolare, la piastrina di riconoscimento e qualsiasi altro documento certificato da personale medico/di laboratorio.

10 Decreto del Presidente della Repubblica 7 aprile 2003, n. 137.

SEGUE ALLEGATO A

AVVERTENZE

1. Per verificare che non ricorrano le condizioni ostative al rilascio della tessera mod. ATe valido per l'espatrio fare riferimento all'art. 3[11] lettera a., b., d. ed e. della Legge 21 nov. 1967 nr. 1185 e Legge n. 3/2003 art. 24[12]. Nel caso vi fossero condizioni ostative, verrà apposta la dizione "NON VALIDO PER L'ESPATRIO" nel campo NOTE della tessera mod. ATe. Non occorre l'autorizzazione del giudice tutelare per il rilascio della tessera valida per l'espatrio, a favore del genitore con prole minore quando questi sia vedovo o unico genitore naturale, ovvero abbia l'assenso dell'altro genitore legittimo da cui non sia legalmente separato e che dimori nel territorio della Repubblica Italiana.
2. La presente richiesta deve essere consegnata a mano dal richiedente all'Incaricato del trattamento dei dati per l'acquisizione. Potranno essere effettuati controlli volti ad accertare la veridicità delle dichiarazioni rese dagli interessati, ai sensi del codice penale e delle leggi speciali in materia (art. 71 DPR 445/2000[13]).
3. I Responsabili del Trattamento curano la restituzione delle carte dei propri dipendenti scadute ovvero revocate, per il successivo inoltro al *Card Management System* (CMS) Unico che le rilascia, oltre che nei casi previsti dall'art. 4[14] del D.P.R. n. 851/67, nel caso di collocamento a riposo con diritto a pensione, per le prescritte variazioni.
4. Analogamente a quanto stabilito per l'espatrio dei titolari di passaporto ordinario, il soggiorno per turismo nei paesi consentiti non può superare il periodo di tre mesi. Il soggiorno superiore a tre mesi, anche per motivi di servizio, deve essere autorizzato dai locali organi di polizia.
5. Le dichiarazioni mendaci, la falsità negli atti e l'uso di atti falsi sono puniti ai sensi del codice penale e delle leggi speciali in materia (art. 76 DPR 445/2000[15]).

---

11 Art. 3 : … omissis…
3. Non possono ottenere il passaporto:
a) coloro che, essendo a norma di legge sottoposti alla patria potestà o alla potestà tutoria, siano privi dell'assenso della persona che la esercita e, nel caso di affidamento a persona diversa, dell'assenso anche di questa; o, in difetto, della autorizzazione del giudice tutelare;
b) i genitori che, avendo prole minore, non ottengano l'autorizzazione del giudice tutelare; l'autorizzazione non è necessaria quando il richiedente abbia l'assenso dell'altro genitore legittimo da cui non sia legalmente separato e che dimori nel territorio della Repubblica (1/b);
c) [coloro contro i quali esista mandato o ordine di cattura o di arresto, ovvero nei cui confronti penda procedimento penale per un reato per il quale la legge consente l'emissione del mandato di cattura, salvo il nulla osta dell'autorità giudiziaria competente ed eccettuati i casi in cui vi sia impugnazione del solo imputato avverso sentenza di proscioglimento o di condanna ad una pena interamente espiata, o condonata] (1/c);
d) coloro che debbano espiare una pena restrittiva della libertà personale o soddisfare una multa o ammenda, salvo per questi ultimi il nulla osta dell'autorità che deve curare l'esecuzione della sentenza, sempreché la multa o l'ammenda non siano già state convertite in pena restrittiva della libertà personale, o la loro conversione non importi una pena superiore a mesi 1 di reclusione o 2 di arresto;
e) coloro che siano sottoposti ad una misura di sicurezza detentiva ovvero ad una misura di prevenzione prevista dagli articoli 3 e seguenti della legge 27 dicembre 1956, n. 1423 (2);
f) [coloro che, trovandosi in Italia, siano obbligati al servizio militare di leva o risultino vincolati da speciali obblighi militari previsti dalle vigenti disposizioni legislative, quando il Ministro per la difesa o l'autorità da lui delegata non assenta al rilascio del passaporto] (2/a).

12 Art. 24: Modifiche alla legge 21 novembre 1967, n. 1185, in materia di rilascio dei passaporti:
"b) i genitori che, avendo prole minore, non ottengano l'autorizzazione del giudice tutelare; l'autorizzazione non è necessaria quando il richiedente abbia l'assenso dell'altro genitore, o quando sia Titolare esclusivo della potestà sul figlio;".

13 Art. 71 (L-R) - Modalità dei controlli:
1. Le amministrazioni procedenti sono tenute ad effettuare idonei controlli, anche a campione, e in tutti i casi in cui sorgono fondati dubbi, sulla veridicità delle dichiarazioni sostitutive di cui agli articoli 46 e 47. (R)
3. Qualora le dichiarazioni di cui agli articoli 46 e 47 presentino delle irregolarità o delle omissioni rilevabili d'ufficio, non costituenti falsità, il funzionario competente a ricevere la documentazione dà notizia all'interessato di tale irregolarità. Questi è tenuto alla regolarizzazione o al completamento della dichiarazione; in mancanza il procedimento non ha seguito. (R)

14 Art. 4. : la tessera personale di riconoscimento è ritirata al dipendente destituito dall'impiego, nonché al dipendente cessato dal servizio senza diritto a pensione. La tessera personale di riconoscimento è altresì ritirata al dipendente a carico del quale è stato adottato provvedimento di sospensione cautelare obbligatoria a norma delle disposizioni vigenti.

15 Art. 76 (L) - Norme penali:
1. Chiunque rilascia dichiarazioni mendaci, forma atti falsi o ne fa uso nei casi previsti dal presente testo unico è punito ai sensi del codice penale e delle leggi speciali in materia.
2. L'esibizione di un atto contenente dati non più rispondenti a verità equivale ad uso di atto falso.
3. Le dichiarazioni sostitutive rese ai sensi degli articoli 46 e 47 e le dichiarazioni rese per conto delle persone indicate nell'articolo 4, comma 2, sono considerate come fatte a pubblico ufficiale.

4. Se i reati indicati nei commi 1, 2 e 3 sono commessi per ottenere la nomina ad un pubblico ufficio o l'autorizzazione all'esercizio di una professione o arte, il giudice, nei casi più gravi, può applicare l'interdizione temporanea dai pubblici uffici o dalla professione e arte.

SEGUE ALLEGATO A

Il sottoscritto dichiara inoltre:

a. Di aver preso visione e conoscere il contenuto della Direttiva SMD-I-009 "Norme di gestione e d'impiego 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.

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 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;

e. 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;

f. Di consentire al mantenimento presso il *Trust Service Provider* (TSP) 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 TSP attuale termini i propri servizi;

g. Di autorizzare il trattamento dei propri dati personali, ai sensi del D.Lgs. 196 del 30 giu. 2003;

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

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

_____ , lì ___/___/_____ _____

(LUOGO) (DATA) (FIRMA DEL DICHIARANTE)

SEGUE ALLEGATO A

INFORMATIVA AI SENSI DELL'ART.13 DEL D.LGS N. 196/2003 SULL'ATTIVITÀ DI RACCOLTA DEI DATI PERSONALI

In relazione all'acquisizione dei dati personali, la informiamo di quanto segue:

a. I dati personali in argomento **sono rilevati esclusivamente per consentire al Ministero della Difesa di rilasciare un Modello ATe** secondo le specifiche previste dal Decreto del Presidente del Consiglio dei Ministri 24 mag. 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 decreto legislativo n. 82 del 2005.

b. Non verrà richiesto il conferimento di altri dati anche di tipo biometrico oltre l'immagine del titolare, l'immagine della firma autografa, il gruppo sanguigno e, per particolari esigenze di sicurezza fisica e logica, in base ad espresse disposizioni di legge che li prevedano specificatamente, il *template* dell'impronta digitale del dito indice di entrambe le mani (qualora non disponibile di altro dito: medio, anulare o pollice).

c. Limitatamente al gruppo sanguigno, il conferimento di tale dato è obbligatorio per il personale militare e opzionale per il personale civile.

d. In caso di un suo eventuale rifiuto al trattamento di tali dati, il Ministero della Difesa non potrà emettere il modello ATe con conseguente limitazione all'identificazione ed all'autenticazione nelle reti della Difesa, necessario a garantire l'accesso sicuro ai sistemi informativi.

e. Se acquisito, il *template* dell'impronta digitale sarà trascritto nel microchip del modello ATe del dipendente e **non saranno diffuse né saranno conservate in banche dati di alcun tipo**. Al momento dell'emissione del modello ATe, tramite una procedura di sicurezza interna al sistema, il *template* dell'impronta digitale **sarà cancellato dal sistema in maniera sicura.**

f. La SV è titolare dei diritti di cui all'articolo 7 del *Codice in materia di trattamento dei dati personali.*

g. Il titolare del trattamento dei dati è il Ministero della Difesa, con sede in Via XX Settembre, 8 – 00100 Roma, ed è effettuato esclusivamente da personale incaricato.

Il sottoscritto_____ dichiara di aver preso visione della presente informativa.

Luogo, _____Data _____, Firma _____

Pagina intenzionalmente bianca

ALLEGATO B

MEMORANDUM DI SICUREZZA PER I TITOLARI DELLA TESSERA MODELLO ATE

Destinatari: tutto il personale dell'Amministrazione della Difesa.

Obiettivo: detto memorandum si prefigge di fornire indicazioni utili al fine di porre il Titolare della tessera mod. ATe in grado di operare in sicurezza, evitare di subire falsificazioni o abusi, in particolar modo per quanto concerne:

- **autenticazione** del Titolare, che permette di usare il certificato di autenticazione CNS contenuto nel chip della carta per l'accesso a sistemi informatici, 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): è un supporto per effettuare operazioni di firma di documenti: attraverso un apposito certificato inserito nel chip, il Titolare è in grado di utilizzare la tessera mod. ATe come strumento di firma digitale di documenti, in conformità alle vigenti disposizioni di legge;
- **cifra** per cifrare i documenti, in modo che possano essere accessibili solo al destinatario. Le finalità sono di natura operativa e di rispetto di *security*, *privacy* e leggi penali.

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

In caso di inosservanza ovvero cattiva gestione della tessera mod. ATe sono previste sanzioni in attuazione ai regolamenti , alle norme contrattuali, ai regolamentari e alle leggi in materia disciplinare sia per il personale militare sia per il personale civile[46]

Di seguito sono elencate alcune regole di sicurezza che il Titolare deve seguire per raggiungere e mantenere un buon livello di sicurezza nell'utilizzo del sistema di firma digitale e in generale del supporto hardware che lo ospita. Infatti, il Titolare è tenuto a adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri [47]. 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 macchina su cui viene utilizzato.

DIVIETI:

- **Non è consentito l'uso della tessera mod. ATe per accedere ad informazioni coperte dal Segreto di Stato**.
- E' vietata la duplicazione della chiave privata di firma e dei dispositivi che la contengono [48].
- Non è consentito l'uso di una chiave per funzioni diverse da quelle previste dalla sua tipologia [49], 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[50].

46 Es. Decreto Legislativo 15 marzo 2010, n. 66 Codice dell'ordinamento militare e del Codice di comportamento (DPCM 28 novembre 2000).
47 D.Lgs. 82 del 7 marzo 2005 (Codice dell'Amministrazione Digitale)] art. 32, comma 1.
48 DPCM 13 gennaio 2004, art. 7: Conservazione delle chiavi.
49 DPCM 13 gennaio 2004, art. 4: Caratteristiche generali delle chiavi per la creazione e la verifica della firma.
50 DPCM 13 gennaio 2004, art. 6: Modalità di generazione delle chiavi.

SEGUE ALLEGATO B

DOVERI:

In considerazione della valenza legale che la firma digitale di un documento assume, nonché del fatto che tramite la tessera mod. ATe è possibile cifrare informazioni sensibili in termini di *privacy* ovvero informazioni d'ufficio di carattere "delicato", l'utente deve:

- Custodire correttamente e diligentemente la carta portandola sempre con se, evitandone lo smarrimento e proteggendo la tessera mod. ATe dal deterioramento in quanto contenente la chiave privata, al fine di garantirne l'integrità e la massima riservatezza[51].
- Non lasciare incustodita la carta di firma specialmente quando inserita nel lettore.
- Utilizzare la carta per il solo tempo necessario ad apporre la firma ovvero ad accedere agli applicativi che necessitano dell'autenticazione tramite tessera mod. ATe.
- Non scrivere il PIN di abilitazione della carta 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 la propria carta (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 la smart card di firma o vi sia timore che sia stata sottratta indebitamente, effettuare subito la procedura di sospensione immediata 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 al Titolare tramite email. In seguito sporgere denuncia alle Autorità di Pubblica Sicurezza competenti e contattare l'Incaricato del trattamento per le successive operazioni di revoca o riattivazione.
- Devono essere prontamente comunicati al proprio Comando o direttamente all'Incaricato del trattamento della LRA di appartenenza i possibili malfunzionamenti riscontrati sul dispositivo di firma.
- Devono essere, altresì, prontamente comunicati al proprio Comando, direttamente all'Incaricato del trattamento o, qualora non sia immediatamente contattabile (es. fuori orario di servizio), direttamente al servizio di certificazione (Call Center) 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.

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

SEGUE ALLEGATO B

- A seguito di sospensione del certificato, risolta la relativa causa, è necessario presentarsi presso il proprio Incaricato del 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[52].
- Sospendere l'utilizzo dei certificati della tessera mod. ATe 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 della tessera mod. ATe 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 stazione di lavoro.

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

SEGUE ALLEGATO B

- 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 DEL TITOLARE

Non appena si verifichi uno dei casi seguenti il Titolare della carta dovrà richiedere la sospensione della carta.

Elenco dei casi di sospensione della carta a cura del Titolare

- Compromissione/perdita dei codici PIN e PUK;
- Furto/smarrimento della carta;
- Ogni altro motivo che possa dare adito ad un uso improprio della carta. A seguito della sospensione precauzionale della carta, 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 della carta.

Elenco dei casi di revoca della carta a cura del Titolare

- Chip o carta difettosa 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 dal servizio nell'Amministrazione della Difesa (dimissioni, pensionamento, passaggio ad altra PA, ecc.);
- Furto, smarrimento o distruzione della carta (perdita di possesso);
- Scadenza della tessera mod. ATe;
- 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 del Titolare della carta un lettore di carta e il software, disponibile anche sul sito http://cmdweb.servizi.difesa.it, necessario per le operazioni di firma e cifra 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 al Titolare 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". Il Titolare 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 ALLEGATO B

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 da Titolare della tessera mod. ATe devono verificare:

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

SEGUE ALLEGATO B

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 ai 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[53]. Infine si tenga conto delle problematiche relative alla eventuale presenza di macroistruzioni o codice eseguibile nel documento verificato.

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

ALLEGATO C

COMPITI DEL RESPONSABILE DEL TRATTAMENTO

In merito al "Responsabile del trattamento", il DLGS 196/2003 prevede quanto segue:

Art. 29

1) Il responsabile è designato dal Titolare[54] *facoltativamente.*

2) Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

3) Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

4) I compiti affidati al responsabile sono analiticamente specificati per iscritto dal Titolare.

5) Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni."

Il Responsabile del trattamento della LRA è responsabile della richiesta di emissione della tessera mod. ATe per il militare /dipendente dagli ECDR che compongono la LRA, di militari/personale civile dell'A.D. in transito o effettivi ad ECDR viciniore non in possesso di postazione di acquisizione o con postazione di acquisizione temporaneamente inefficiente.

In località dove più Enti/Distaccamenti/Reparti utilizzano una sola LRA, il "Responsabile del trattamento" sarà il Comandante dell'Ente che la gestisce a cui è devoluta anche la responsabilità di firmare la tessera mod. ATe quale "Autorità Rilasciante".

È normalmente il Comandante/Direttore dell'ECDR in cui è realizzata la postazione di acquisizione dati (LRA) ed è normalmente descritto nel documento annuale del proprio ECDR (Atto dispositivo n. 1 o su AA.VV. o documento paritetico), come indicato in Allegato F.

Potrà essere prevista anche la possibilità, per il Comandante dell'Ente, di delegare, con atto di nomina formale, le funzioni di "Responsabile del trattamento" ad altra persona (preferibilmente Ufficiale/Dirigente).

Per ogni LRA potrà essere attiva una sola tessera mod. ATe abilitata al portale CMS con profilo "Responsabile del trattamento".

Nell'ambito della propria LRA il Responsabile del trattamento dovrà:
- indicare i compiti e le responsabilità del personale designato quale "Responsabile del Trattamento" che dovrà essere investito con atto di nomina formale;
- indicare in maniera chiara e inequivocabile il personale a cui rilasciare la tessera mod. ATe.
- approvare i dati rilevati per il rilascio della tessera mod. ATe;
- approvare ed inviare le pratiche di cambio stato;
- gestire i Responsabili del trattamento della LRA;
- custodire la *Key Recovery;*
- è responsabile della Reportistica e delle rilevazioni Statistiche legate all'operato della LRA.

---

[54] ***DLGS 196/2003 - Art.28:*** *"Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, Titolare del trattamento è l'entità nel suo complesso o l'unità od organismo del trattamento che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza."*

SEGUE ALLEGATO C

COMPITI DELL'INCARICATO DEL TRATTAMENTO DEI DATI

In merito all' "Incaricato del trattamento", il DLGS 196/2003 prevede quanto segue:

Art.30

1) Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Titolare o del responsabile, attenendosi alle istruzioni impartite.

2) La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima."

E' il responsabile dell'acquisizione dei dati ai fini dell'emissione della tessera mod. ATe e della raccolta dati per il Passaporto elettronico di servizio (ePass). Viene nominato dal Comandante/Direttore dell'Ente ed è registrato nel documento annuale del proprio ECRD (Atto dispositivo n.1 o sue AAVV) ai sensi dell'art. 4, comma 1 , lett g) del decreto legislativo del 30 giugno 2003, n. 196 e s.m. noto come Codice della privacy.
Nell'ambito del modello organizzativo individuato, l'Incaricato del trattamento esegue le seguenti attività:

- prima dell'inizio del trattamento (cioè antecedente alla fase di *enrollment*), deve far prendere visione al richiedente, in modalità certa attraverso la firma dell'Allegato A, dell'informativa specifica relativa all'utilizzo dei dati personali;
- mantiene l'operatività dell'infrastruttura hardware e software relativa al servizio e impiego presso la LRA;
- è responsabile della completezza della pratica per acquisizione dei dati per la tessera mod. ATe e della conservazione della pratica cartacea per almeno 10 anni;
- è responsabile della completezza dei dati richiesti ma non della corrispondenza al vero la cui responsabilità è del Titolare che ne sottoscrive la veridicità;
- è responsabile della conformità allo standard internazionale ICAO della fotografia del Titolare verificando che quest'ultima non sia più vecchia di sei mesi (Allegato D);
- tra i dati sanitari, inserisce il dato gruppo sanguigno e relativo fattore RH solo se il Titolare presenta copia di un documento che ne attesti la veridicità (stralcio del libretto personale, referto di analisi di laboratorio, tessera donatore di sangue, piastrina di riconoscimento). In caso contrario dovrà inserire il dato ND (non disponibile);
- è responsabile dell'identificazione del Titolare della futura tessera mod. ATe, accertandone l'identità tramite documento di riconoscimento in corso di validità (mod. AT, mod. ATe, carta d'identità, patente di guida, passaporto[55]). Se il Titolare ha figli minori è obbligatoria la presenza della firma autografa dell'altro genitore che deve essere verificata dal RTD tramite copia di un documento di riconoscimento provvisto di firma autografa. In caso di assenza della predetta firma, dovrà essere inserito nel campo note della tessera mod. ATe la dicitura: NON VALIDA PER L'ESPATRIO;
- acquisisce i dati previsti per l'emissione della tessera mod. ATe;
- acquisisce i dati previsti per il rilascio del Passaporto Elettronico di Servizio;
- gestisce le pratiche di restituzioni delle tessere mod. ATe revocate/scadute;
- distribuisce la nuova tessera mod. ATe ai titolari;

55 Riferimento DPR 445/2000.

SEGUE ALLEGATO C

- è responsabile della Reportistica e delle rilevazioni Statistiche legate all'operato della LRA;
- predispone le pratiche di cambio stato per la successiva approvazione e invio a cura del Responsabile del trattamento ;
- verifica eventuali inefficienze del chip delle tessere mod. ATe i cui titolari richiedono la sostituzione per inefficienza del chip prima di preparare la pratica di cambio stato.

COMPITI E RESPONSABILITÀ DELLE SEGRETERIE/UFFICI PREPOSTI ALLA GESTIONE DELLA RICHIESTA DI EMISSIONE DEL MODELLO ATe

- Distribuire al personale militare in servizio e civile, per la successiva compilazione, la richiesta per l'emissione della tessera mod. ATe (Allegato A alla Direttiva SMD-I-009);
- ritirare la richiesta di emissione tessera mod. ATe, debitamente compilata e firmata dal personale, per sottoporla alla firma del Comandante di Corpo/Dirigente o suo delegato e riconsegnarla agli interessati. Si raccomanda la massima attenzione nella compilazione del Gruppo Sanguigno che deve essere basata su idonea certificazione;
- inviare l'elenco nominativo del personale, a cui dovrà essere emessa la tessera mod. ATe ai responsabili delle postazioni di acquisizioni dati ;
- raccomandare al personale interessato di recarsi alle postazioni di acquisizioni dati munito di copia di documento di identità valido, oltre alla richiesta di emissione tessera mod. ATe da consegnare agli incaricati delle citate postazioni .
- Fornire al personale richiedente la tessera mod. ATe il supporto necessario in caso di dati non presenti in fase di precaricamento e/o incongruenti.

Pagina intenzionalmente bianca

ALLEGATO D

FORMATO DELLA FOTOGRAFIA

Il formato della fotografia è 320 x 240 punti ed eredita tutte le caratteristiche stabilite per la CIE. La fotografia da acquisire deve essere fatta in modo che le condizioni di luminosità e contrasto dell'immagine siano sufficienti per un riconoscimento a vista. L'inquadratura deve mostrare in modo evidente le caratteristiche del volto.
Lo sfondo che deve essere predisposto per l'inquadratura della foto è bianco.
Per la tipologia di luminosità e caratteristiche generali si rimanda alla normativa ICAO.

MODULO ICAO DI RIFERIMENTO PER IL RILASCIO DELLA FOTO

Qualità della foto

Le foto devono essere:

- Non anteriori a 6 mesi
- 35-40 mm di altezza
- racchiudere il volto in modo tale che esso occupi il 70-80 % della foto
- perfettamente a fuoco
- di alta qualità senza macchie o graffi

Le foto devono :

- mostrare lo sguardo diretto sull'obiettivo
- mostrare il tono naturale della pelle
- avere la giusta luminosità e contrasto
- essere stampate su carta di ottima qualità e ad alta risoluzione

SEGUE ALLEGATO D

Stile ed illuminazione

La fotografia deve:

- non avere dominanti
- mostrare gli occhi aperti e chiaramente visibili senza capelli davanti
- mostrare l'immagine frontalmente e non di 3/4 (stile ritratto) con chiaramente visibili entrambi i lati del viso
- avere uno sfondo di colore chiaro ed omogeneo
- avere un'illuminazione uniforme senza ombre, senza riflessi di flash e senza occhi rossi

SEGUE ALLEGATO D

Occhiali e copricapi

Se indossate occhiali:

- la fotografia deve mostrare gli occhi chiaramente senza riflessi di flash sulle lenti che non devono essere scure e che possibilmente devono avere una montatura leggera.
- La montatura non deve coprire alcuna parte degli occhi

Copricapi:

- non sono permessi ad eccezione di motivi religiosi, ma il viso deve essere chiaramente visibile dalla fronte al mento e per entrambi i lati,

Espressione ed immagine

La fotografia deve:

- inquadrare il soggetto frontalmente, senza oggetti vari o altre persone, con espressione neutra e bocca chiusa

Pagina intenzionalmente bianca

ALLEGATO E

MEMBRI DEL CHANGE ADVISORY BOARD (CAB)

SMD I Reparto	Rappresentante nominato dallo **SMD** *I Reparto*
SMD VI Reparto	Capo Ufficio Sistemi Informativi di Supporto o suo rappresentante Capo Sezione Servizi e Sistemi Infrastrutturali di base (CORE)
Comando C4 Difesa	Capo Ufficio Servizi ICT o suo rappresentante Capo Sezione Certificazione e conservazione
SME - VI Reparto	Capo Ufficio Sistemi di Supporto C2 o suo rappresentante Capo Sezione Produzione Tessere mod. ATe del Comando C4 Esercito.
SMM– Reparto C4S	Capo Ufficio Informatica Gestionale o suo rappresentante
SMA	Capo Ufficio Informatica o suo rappresentante
SGD	Capo del 1° Ufficio "Informatica e Statistica" o suo rappresentante

Stante l'assegnazione della *Lead Service* all'Esercito, il ruolo di Presidente del CAB è ricoperto dal rappresentante designato dello Stato Maggiore dell'Esercito.

Il CAB può coinvolgere ulteriori membri di supporto, rappresentativi delle seguenti categorie di soggetti:

- rappresentanti di gruppi di utenti;
- specialisti e consulenti tecnici;
- personale coinvolto nella gestione operativa del servizio (es. *service desk operator*).

Pagina intenzionalmente bianca

ALLEGATO F

FACSIMILE ATTO DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO E DEGLI INCARICATI DEL TRATTAMENTO DEI DATI

TIMBRO DELL'ENTE

Roma,

OGGETTO: Nomina del Responsabile del trattamento e degli Incaricati del trattamento dei dati personali ai sensi del D.l.vo 196/2003 della *Local Registration Authority* attivata presso _____ preposti alle operazioni di rilascio della tessera mod. ATe.

Il sottoscritto, _____ Comandante/Direttore/Responsabile del

_____,

in qualità di Responsabile del trattamento dei dati ai sensi del D.Lgs. 196/2003

PREMESSO CHE:

- il Dlgs 30 giugno 2003 n° 196, "Codice in materia di protezione dei dati personali", fissa le modalità da adottare per detto trattamento ed individua i soggetti che, in relazione all'attività svolta, sono tenuti agli adempimento previsti dalla stessa legge;
- l'art.30 del Dlgs 196/2003 prevede che il Responsabile del trattamento possa procedere alla nomina di uno o più Incaricati del trattamento medesimo, i quali devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni del Titolare o del Responsabile;
- è interesse dell'A.D. che il trattamento dei dati contenuti nelle proprie banche dati debba avvenire sotto il suo stretto controllo ed in conformità con le istruzioni contenute nella Direttiva SMD-I-009 "Norme di gestione e d'impiego 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";
- si intende, pertanto, procedere alla nomina degli incaricati dei trattamenti sopraindicati.

SEGUE ALLEGATO F

D I S P O N G O

la nomina del seguente personale abilitato ad operare presso la *Local Registration Authority* attivata presso _____:

- **Responsabile del trattamento: _____** .
- **Incaricato del trattamento dei dati:** _____ ;

  _____.

La nomina del personale sopra indicato dovrà essere pubblicata sull'Ordine del giorno di questo Ente.

IL COMANDANTE DI CORPO/DELEGATO DELL'ENTE

_____

(copia dell'atto di nomina dovrà essere trasmessa al Comando C4 Difesa ed al CMS presso il Comando C4 Esercito).

ALLEGATO G

LIVELLI DI SERVIZIO

TEMPO DI EMISSIONE

Caratteristica /Sottocaratteristica	Efficienza / efficienza temporale
Indicatore/Misura	**TEC - Tempo di emissione** (percentuale)
Sistema di gestione delle misure	Le misure si basano sui file di log prodotti dai sistemi di emissione delle carte, nonché sulle evidenze di rilascio delle stesse.
Metodi e strumenti di misura	Per ogni carta, si misura il tempo che intercorre tra la data di ricezione della richiesta di emissione e la data di rilascio.
Unità di misura	Percentuale
Dati elementari da rilevare	Per ogni carta, data di ricezione della richiesta (valida) di emissione Per ogni carta, data di rilascio
Periodo di riferimento	mese
Frequenza esecuzione misure	mensile
Regole di campionamento	Nessuna (parametro applicato sull'intera produzione)
Formula di calcolo	**TC_RI** = numero totale di carte richieste nel periodo **TC_OK** = numero di carte emesse in tempo nel periodo Il parametro viene calcolato con la seguente formula: **TEC** = **TC_OK** / **TC_RI** * **100**
Regole di arrotondamento	TEC va arrotondato alla frazione di punto percentuale sulla base del primo decimale: ▪ al punto % per difetto se la parte decimale è ≤ 0,5 ▪ al punto % per eccesso se la parte decimale è > 0,5
Obiettivi, (valori soglia)	▪ Entro **7 giorni lavorativi** per un totale **TEC >= 95%**; ▪ Entro **20 giorni lavorativi** per il residuo **TEC <= 5%**

SEGUE ALLEGATO G

TEMPO DI GESTIONE SOSPENSIONE / REVOCA

Caratteristica /Sottocaratteristica	Efficienza / efficienza temporale
Indicatore/Misura	**TGC - Tempo di gestione** (percentuale) per "Sospensione" (**TGC-s**) o per "Revoca" (**TGC-r**)
Sistema di gestione delle misure	Le misure si basano sui file di log prodotti dai sistemi di emissione delle carte, nonché sulle evidenze di rilascio delle stesse.
Metodi e strumenti di misura	Per ogni carta, si misura il tempo che intercorre tra la data/ora di ricezione della richiesta di gestione *(es.: attivazione, sospensione o revoca)* e la data/ora di attuazione della richiesta. La richiesta si considera attuata quando viene emessa la notifica di avvenuta esecuzione dell'operazione, in conformità con le modalità prestabilite.
Unità di misura	Percentuale
Dati elementari da rilevare	Per ogni carta, la data/ora di ricezione della richiesta (valida) di gestione Per ogni carta, la data/ora di attuazione della richiesta
Periodo di riferimento	mese
Frequenza esecuzione misure	mensile
Regole di campionamento	Nessuna (parametro applicato sull'intera produzione)
Formula di calcolo	**Per sospensione:** **TRS** = numero totale di richieste di sospensione carta nel periodo **TS_OK** = totale sospensioni attuate entro il tempo-limite stabilito Il parametro viene calcolato con la seguente formula: **TGC-s = TS_OK / TRS * 100** **Per Revoca:** **TRR** = numero totale di richieste di revoca carta nel periodo **TR_OK** = totale sospensioni attuate entro il tempo-limite stabilito Il parametro viene calcolato con la seguente formula: **TGC-r = TR_OK / TRR * 100**
Regole di arrotondamento	TGC va arrotondato alla frazione di punto percentuale sulla base del primo decimale: ▪ al punto % per difetto se la parte decimale è ≤ 0,5 ▪ al punto % per eccesso se la parte decimale è > 0,5
Obiettivi, (valori soglia)	**Per sospensione:** ▪ Entro **10 minuti** per un totale **TRS >= 98%**; ▪ Entro **30 minuti** per il residuo **TRS <= 2%** **Per revoca:** ▪ Entro **48 ore** per un totale **TRR >= 98%**; ▪ Entro **96 ore** per il residuo **TRR <= 2%**

SEGUE ALLEGATO G

TEMPO DI GESTIONE DIFETTOSITÀ

Caratteristica /Sottocaratteristica	Affidabilità / Maturità
Indicatore/Misura	**DFA** - Difettosità delle carte ed eventuali accessori
Sistema di gestione delle misure	Messaggi di posta elettronica od altra modalità prestabilita per la segnalazione di prodotti difettosi.
Metodi e strumenti di misura	Si conta il numero di prodotti segnalati come difettosi, con le modalità prestabilite, entro 10 giorni dalla relativa data di rilascio.
Unità di misura	Percentuale
Dati elementari da rilevare	Segnalazione di prodotto difettoso pervenuta, con le modalità prestabilite, entro 10 giorni dalla data di consegna.
Periodo di riferimento	mese
Frequenza esecuzione misure	mensile
Regole di campionamento	Nessuna (parametro applicato sull'intera produzione)
Formula di calcolo	**TCA** = numero totale di carte ed accessori emessi nel periodo **TCA_KO** = totale prodotti segnalati come difettosi (entro 10 giorni dalla data di rilascio) Il parametro viene calcolato con la seguente formula: **DFA = TCA_KO / TCA * 100**
Regole di arrotondamento	DFA va arrotondato alla frazione di punto percentuale sulla base del primo decimale: ▪ al punto % per difetto se la parte decimale è ≤ 0,5 ▪ al punto % per eccesso se la parte decimale è > 0,5
Obiettivi, (valori soglia)	▪ **DFA <= 3%**

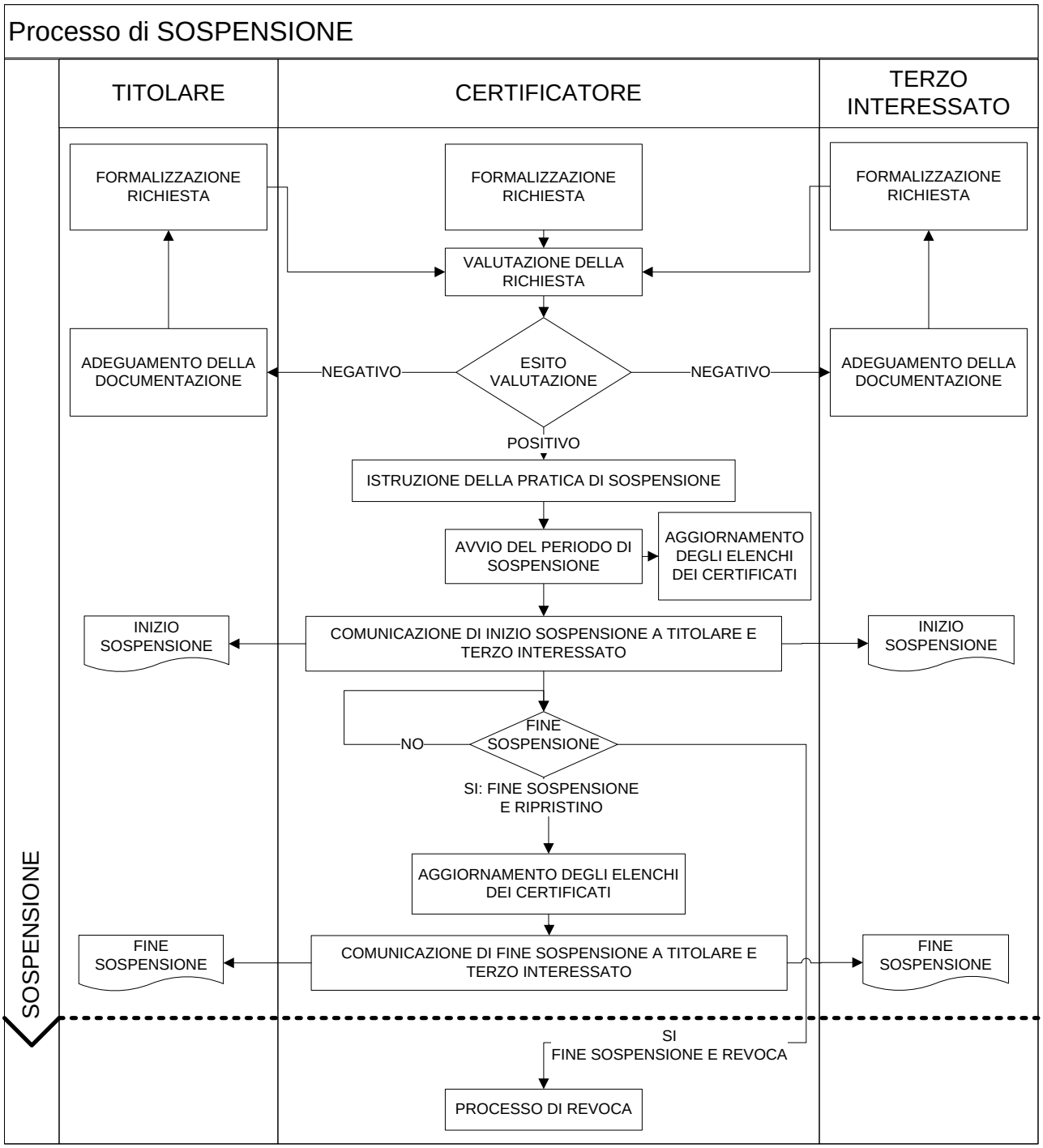
SEGUE ALLEGATO G

QUALITÀ DELLA REPORTISTICA

Caratteristica /Sottocaratteristica	Funzionalità / Accuratezza
Indicatore/Misura	**QRP** - qualità della reportistica (completezza e correttezza)
Sistema di gestione delle misure	Reportistica generata dal sistema di gestione
Metodi e strumenti di misura	Analisi della reportistica
Unità di misura	Percentuale
Dati elementari da rilevare	▪ numero di dati errati ▪ numero di dati incompleti ▪ numero totale dei dati dove con "dati" si intendono i singoli indicatori inclusi nella reportistica.
Periodo di riferimento	mese
Frequenza esecuzione misure	mensile
Regole di campionamento	Nessuna (parametro applicato sull'intera produzione)
Formula di calcolo	**TDE** = numero totale di dati errati **TDI** = numero totale di dati incompleti **TD** = numero totale di dati inclusi nella reportistica Il parametro viene calcolato con la seguente formula: **QRP = ((TDE + TDI) / TD) * 100**
Regole di arrotondamento	QRP va arrotondato alla frazione di punto percentuale sulla base del primo decimale: ▪ al punto % per difetto se la parte decimale è ≤ 0,5 ▪ al punto % per eccesso se la parte decimale è > 0,5
Obiettivi, (valori soglia)	▪ **QRP <= 5%**

ALLEGATO H

RAPPRESENTAZIONE DEL PROCESSO DI SOSPENSIONE



Pagina intenzionalmente bianca

ALLEGATO I

ELENCO DEI TITOLI AUTORIZZATI ALLA TRASCRIZIONE NEL CAMPO NOTE

TITOLO	ENTE RESPONSABILE DELL'ASSEGNAZIONE DEL CODICE ALFANUMERICO
Brevetto pilota militare	Aeronautica Militare
Brevetto navigatore militare	Aeronautica Militare
Brevetto pilota di elicottero	Aeronautica Militare
Brevetto pilota osservatore	Aeronautica Militare
Brevetto specialista aeronautico	Aeronautica Militare
Brevetto specialista di elicottero	Aeronautica Militare
Brevetto specialista velivoli leggeri	Aeronautica Militare

Pagina intenzionalmente bianca

ALLEGATO L

PERSONALE DESTINATARIO DELLA TESSERA MOD. ATE

POSIZIONE DI STATO GIURIDICO	POSIZIONE	RILASCIO MOD. ATe	LIMITAZIONI AL RILASCIO	REVOCA DELLA CARTA	NOTE
Militari in servizio permanente	In servizio attivo	SI	Senza limitazioni	Al momento del collocamento in congedo assoluto	
Personale civile della Difesa	In servizio attivo	SI	Senza limitazioni	Al momento del collocamento in pensione	
Militari in servizio temporaneo (*Se non è diversamente disposto, al personale militare in servizio temporaneo si applicano le norme previste per il personale militare in servizio permanente in materia di stato giuridico)*	Sospesi dall'impiego	NO		Al momento della sospensione dall'impiego	
	In aspettativa	SI		Al momento del collocamento in congedo assoluto	
	Volontari in ferma prefissata, in prolungamento di ferma e in rafferma	SI	Durata minima della rispettiva ferma 12 mesi	Al momento del collocamento in congedo illimitato	
	Allievi delle scuole militari	SI			Ad eccezione degli Allievi delle Scuole di Formazione militare.
	Allievi marescialli	SI			
	Allievi ufficiali	SI			

POSIZIONE DI STATO GIURIDICO	POSIZIONE	RILASCIO MOD. ATe	LIMITAZIONI AL RILASCIO	REVOCA DELLA CARTA	NOTE
Militari in servizio temporaneo (*Se non è diversamente disposto, al personale militare in servizio temporaneo si applicano le norme previste per il personale militare in servizio permanente in materia di stato giuridico)*	Marescialli in ferma	SI			
	Ufficiali di complemento in ferma e in rafferma	SI	Durata minima della rispettiva ferma 12 mesi		
	Allievi ufficiali e ufficiali in ferma prefissata	SI	Durata minima della rispettiva ferma 12 mesi		
	Ufficiali e sottufficiali piloti e navigatori di complemento	SI	Durata minima della rispettiva ferma 12 mesi		
Personale Militare in congedo	Ausiliaria	SI		Al momento del collocamento in congedo assoluto	Personale militare che ha manifestato la propria disponibilità a prestare servizio
	Complemento	NO			
	Congedo illimitato	NO			Militari di truppa che cessano dal servizio temporaneo
	Riserva	SI	Fino al collocamento in congedo assoluto	Al momento del collocamento in congedo assoluto	Militari che cessano dal servizio permanente o che vi transitano dalla categoria dell'ausiliaria
	Riserva di complemento	NO			
	Congedo assoluto	NO	Volontario al raggiungimento del 45 anno di età	Al momento del collocamento	Personale militare non più vincolato da obblighi di servizio attivo

POSIZIONE DI STATO GIURIDICO	POSIZIONE	RILASCIO MOD. ATe	LIMITAZIONI AL RILASCIO	REVOCA DELLA CARTA	NOTE
Personale Militare in congedo			Generale/Ammiraglio al raggiungimento del 73 anno di età	in congedo assoluto	
			Ufficiale superiore/inferiore al raggiungimento del 70 anno di età		
			Personale militare non direttivo e non dirigente delle Forze Armate al raggiungimento del 65 anno di età		
			Militare riconosciuto permanentemente inabile al servizio militare		
Personale Civile	Di ruolo in attività di servizio	SI		Al momento del collocamento in pensione	DPR 28 luglio 1967, n. 851
	Non di ruolo in attività di servizio	SI	Durata minima del rapporto di lavoro non inferiore ai 12 mesi continuativi	Al momento della cessazione del rapporto di lavoro	
Personale militare collocato fuori ruolo		SI		Al momento del collocamento in congedo assoluto	Transito con decreto ministeriale
Magistratura Militare		SI		Al momento della cessazione dall'impiego presso la Magistratura Militare	

POSIZIONE DI STATO GIURIDICO	POSIZIONE	RILASCIO MOD. ATe	LIMITAZIONI AL RILASCIO	REVOCA DELLA CARTA	NOTE
Sovrano Militare Ordine di Malta (SMOM)		SI	Durata minima della rispettiva ferma 12 mesi	Al momento della cessazione dell'attività di servizio	
Enti Vigilati posti sotto la vigilanza del Ministero della Difesa	Agenzia Industrie Difesa	SI	Durata minima del rapporto di lavoro non inferiore ai 12 mesi continuativi	Al momento della cessazione del rapporto di lavoro	
	Associazione italiana della Croce rossa, per le componenti ausiliarie delle Forze Armate	SI	Durata minima della rispettiva ferma 12 mesi	Al momento della cessazione dell'attività di servizio	Durata dell'arruolamento nella Croce Rossa Italiana di due anni senza soluzione di continuità

ALLEGATO M

MATRICE DELLE OSSERVAZIONI/PROPOSTE

SOSTANZIALI / EDITORIALI

(BARRARE LA VOCE NON DI INTERESSE)

N.	Ente Richiedente	Capitolo	Paragrafo	Sotto paragrafo	Pagina	Riga	Commento	Motivazione
1								
2								
3								
4								
5								
6								
7								
8								
...								