STATO MAGGIORE DIFESA

VI Reparto – Sistemi C4I e Trasformazione

SMD - I - 009

CARTA MULTISERVIZI DELLA DIFESA (CMD), PUBLIC KEY INFRASTRUCTURE (PKI) E FIRMA DIGITALE

NORME DI GESTIONE E D'IMPIEGO

EDIZIONE 2014

Pagina intenzionalmente bianca

STATO MAGGIORE DELLA DIFESA

VI REPARTO - Sistemi C4I e Trasformazione

ATTO DI APPROVAZIONE

Approvo la Direttiva SMD - I - 009 "**Carta Multiservizi della Difesa (CMD), Public Key Infrastructure (PKI) e Firma Digitale - Norme di gestione e d'impiego**".

Essa abroga e sostituisce le seguenti direttive:

- SMD-I-001 "Direttiva per l'impiego della Firma Digitale in ambito Amministrazione Difesa" - edizione 2005;
- SMD-I-009 "Carta Multiservizi della Difesa" - edizione 2005.

Roma, lì 11 NOV. 2014

IL CAPO DI STATO MAGGIORE DELLA DIFESA
Ammiraglio Luigi BINELLI MANTELLI

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			

Pagina intenzionalmente bianca

DESTINATARI DELLA DIRETTIVA E GUIDA ALLA CONSULTAZIONE

DESTINATARI DELLA DIRETTIVA

La Direttiva è rivolta a tutti gli Attori coinvolti nei processi di acquisizione, validazione, emissione, consegna e utilizzo della **Carta Multiservizi della Difesa** (**CMD**) e dei certificati digitali (firma digitale e autenticazione CNS) emessi dalla ***Public Key Infrastructure*** **(PKI)** della Difesa collocati a bordo della carta stessa, nonché alle strutture organizzative che presiedono alle attività di verifica e controllo ***(Governance)*** dei predetti processi.

Ciò premesso, ferma restando l'opportunità che il Lettore acquisisca un'adeguata conoscenza dell'intero documento, ciascuno dei destinatari della presente Direttiva potrebbe risultare maggiormente interessato a quelle specifiche tematiche che rientrano nell'ambito dei ruoli e responsabilità di sua competenza: di seguito, per facilitare la ricerca e la consultazione di tali tematiche, è illustrata la "mappa" del documento contenente la sua articolazione e 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 CMD.

L'esigenza di un approccio unitario e condiviso alle problematiche afferenti sia la CMD che la Firma Digitale, a fronte di una utenza sempre più allargata ed esigente, ha evidenziato la necessità di definire una "Politica" di gestione comune. 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 2005.

STRUTTURA DEL DOCUMENTO E GUIDA ALLA CONSULTAZIONE

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 CMD e della Firma Digitale. E' articolata in 6 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 caratterizza.*
  - ***Cap. 3:*** *descrive le strutture organizzative che presiedono i processi di servizio illustrati, indicando ruoli e responsabilità di ciascun Attore.*
  - ***Cap. 4:*** *contiene una descrizione generale della Carta Multiservizi della Difesa (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 Carta Multiservizi della Difesa e dei Certificati Digitali.*

- **SEZIONE 2**

  E' costituita da diversi Annessi e Allegati, ciascuno dei quali è focalizzato su un particolare aspetto della CMD 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

ATTO DI APPROVAZIONE ..... **III**

ELENCO DI DISTRIBUZIONE ..... **V**

REGISTRAZIONE DELLE AGGIUNTE E VARIANTI ..... **VII**

DESTINATARI DELLA DIRETTIVA E GUIDA ALLA CONSULTAZIONE ..... **IX**

1. CARATTERIZZAZIONE DELLA DIRETTIVA **1**

1.1. SCOPO DEL DOCUMENTO 1

2. GOVERNANCE **3**

2.1. OBIETTIVI 3

2.2. STRUTTURA ORGANIZZATIVA DELLA GOVERNANCE 3

2.3. CHANGE ADVISORY BOARD (CAB) 4

2.3.1. COMPITI 4

2.4. APPLICATION SERVICE PROVIDER (ASP) 5

2.4.1. COMPITI DELL'ASP 5

2.5. PROCEDURE PER LA MANUTENZIONE DEL SISTEMA 6

3. STRUTTURA ORGANIZZATIVA DEI PROCESSI DI SERVIZIO **9**

3.1. GENERALITÀ 9

3.2. CERTIFICATION AUTHORITY (CA) 9

3.3. REGISTRATION AUTHORITY (RA) E CARD MANAGEMENT SYSTEM (CMS) 10

3.4. LOCAL REGISTRATION AUTHORITY 10

3.5. TITOLARE DELLA CARTA 10

4. CARTA MULTISERVIZI DELLA DIFESA (CMD) **11**

4.1. GENERALITÀ 11

4.2. CARATTERIZZAZIONE DELLA CMD 11

4.3. DESTINATARI DELLA CMD 12

4.4. DURATA 13

4.5. PRIORITÀ NELLA PROCEDURA DI EMISSIONE DELLA CARTA 13

5. PKI - LA FUNZIONE DI FIRMA DIGITALE E DI AUTENTICAZIONE CNS **15**

5.1. GENERALITÀ 15

6. PROCESSI DI SERVIZIO DELLA CMD **17**

6.1. GENERALITÀ 17

6.2. CICLO DI VITA DELLA CMD 17

6.3. PROCEDURE DI ACQUISIZIONE DATI E RILASCIO CMD/CERTIFICATI DIGITALI 19

6.3.1. ACQUISIZIONE DEI DATI 19

6.3.2. ACQUISIZIONE DEI DATI PRESSO ALTRO ENTE 20

6.3.3. EMISSIONE E RILASCIO DELLA CMD 20

6.4. RINNOVO DELLA CMD 21
6.4.1. GENERALITÀ 21
6.4.2. DESCRIZIONE DELLE FASI 22

6.5. SOSPENSIONE DELLA CMD/CERTIFICATI DIGITALI 22
6.5.1. CARTA MULTISERVIZI DELLA DIFESA 22
6.5.2. CERTIFICATI DIGITALI 22
6.5.3. FORMALIZZAZIONE DELLA RICHIESTA 23
6.5.4. VALUTAZIONE DELLA RICHIESTA 23
6.5.5. AVVIO DEL PERIODO DI SOSPENSIONE 24

6.6. REVOCA DELLA CMD/CERTIFICATI DIGITALI 24
6.6.1. FORMALIZZAZIONE DELLA RICHIESTA 24
6.6.2. REVOCA PER FURTO/SMARRIMENTO 25
6.6.3. REVOCA PER CAMBIO DELLO STATUS GIURIDICO 25
6.6.4. AGGIORNAMENTO DEGLI ELENCHI DEI CERTIFICATI 25

7. ELENCO DEGLI ANNESSI E DEGLI ALLEGATI ALLA DIRETTIVA 27

ANNESSO 1 - ELENCO DELLE DEFINIZIONI

ANNESSO 2 - ELENCO DEGLI ACRONIMI

ANNESSO 3 - NORMATIVA DI RIFERIMENTO

ALLEGATO A - MODULO RICHIESTA CMD

ALLEGATO B - MEMORANDUM DI SICUREZZA PER TITOLARI DELLA CARTA MULTISERVIZI DELLA DIFESA (CMD)

ALLEGATO C - COMPITI DEL RESPONSABILE PERIFERICO - COMPITI DEL RESPONSABILE DEL TRATTAMENTO DEI DATI

ALLEGATO D - FORMATO DELLA FOTOGRAFIA

ALLEGATO E - MEMBRI DEL CHANGE ADVISORY BOARD

ALLEGATO F - ELENCO DELLE LOCAL REGISTRATION AUTHORITY

ALLEGATO G - LIVELLI DI SERVIZIO

ALLEGATO H - RAPPRESENTAZIONE DEL PROCESSO DI SOSPENSIONE

ALLEGATO I - ELENCO DEI TITOLI AUTORIZZATI ALLA TRASCRIZIONE NEL CAMPO NOTE

1. CARATTERIZZAZIONE DELLA DIRETTIVA

1.1. SCOPO DEL DOCUMENTO

L'esigenza di disporre di una "carta elettronica" contenente i dati anagrafici e sanitari del personale militare e civile 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 "*carta*" che, tramite un'adeguata componente *software*, fosse in grado di archiviare (sulla carta stessa rispondente ad adeguati requisiti di sicurezza) e gestire le informazioni di carattere personale e sanitario[1] e, nello stesso tempo, rendesse possibile l'accesso a servizi digitali, alcuni dei quali previsti per legge[2].

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[3], indicando anche standard e criteri organizzativi da seguire per la loro erogazione.

In questo 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.

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 considerati **servizi primari** [4]:

- *l'identificazione "a vista" quale tessera di riconoscimento rilasciata dall'A.D. in sostituzione del mod. AT cartaceo[5];*
- *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 - CNSE**);*
- *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.

---

1 Decreto Legislativo 15 marzo 2010, n. 66 – Codice dell'ordinamento militare (Art. 1496).
2 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.
3 Carta d'Identità Elettronica – CIE, Carta Nazionale dei Servizi – CNS e firma digitale.
4 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 88, del D. Lgs. 82/2005"*.
5 DPR del 28 dicembre 2000, n. 445.

La presente Direttiva si colloca nel naturale processo di evoluzione dei servizi ICT della Difesa e, nello specifico, è finalizzata a disciplinare tutte le fasi di gestione e impiego della Carta Multiservizi della Difesa e a fornire le informazioni essenziali sulla ***Public Key Infrastructure (PKI)*** e sulla firma digitale.

2. GOVERNANCE

2.1. OBIETTIVI

Lo **Stato Maggiore della Difesa** (**SMD**), con la presente direttiva intende disciplinare la *Governance* per la gestione della CMD 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'Amministrazione Difesa;
- la gestione dei rischi e dei vantaggi generati dall'utilizzo di un sistema informativo unico per il rilascio della Carta Multiservizi della Difesa 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®**[6], 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)**[7]. E' l'organo permanente interforze 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 compete il controllo strategico del servizio e ha la responsabilità di indicare le linee guida d'interesse collettivo e le eventuali azioni da intraprendere per la risoluzione delle criticità emerse.
- ***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. Costituisce il livello operativo del servizio e 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.
- ***Application Service Provider* (ASP).** E' l'organo preposto all'erogazione del servizio ed è ospitato presso il *Data Center* individuato dal designato per la *Lead Service*[8]. Ha la responsabilità, per conto della A.D., della gestione operativa del servizio, al fine di fornire il

6 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*).

7 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".

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

supporto tecnico-informatico e 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[9] che garantisce l'applicazione:

- delle norme di legge vigenti in materia di firma digitale e tessera di riconoscimento, fornendo le indicazioni per le attività evolutive del sistema, 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 CMD e firma digitale, i principali *stakeholders*[10] 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 disposizioni di legge in vigore.

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

Per le questioni di livello direttivo/strategico, nei casi in cui è necessario un supporto decisionale di livello superiore, il CAB coinvolge il CCI. 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.

2.3.1. 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 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 sistema;
- 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;
- sovraintende a tutto il processo di *Change Management* controllando e coordinando le risorse disponibili e monitorizzando lo stato di avanzamento delle attività;

9 Si veda la struttura in Allegato "E".
10 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.

- 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 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;
- coordina l'implementazione [11] 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)*;
- sottopone all'attenzione del CCI eventuali criticità, rischi o proposte di modifica che abbiano un impatto significativo sul servizio;
- 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.

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;**
- **CMD: Centro Sistemi Informatici dell'Esercito - Via Guido Reni, 22 - 00196 Roma.**

2.4.1. COMPITI DELL'ASP

Nell'ambito del modello organizzativo individuato, l'ASP esegue le seguenti attività:

- mantiene l'operatività dell'infrastruttura *hardware* asservita al servizio (*Card Management System*, *Certification Authority* e *Local Registration Authority*);
- definisce la configurazione delle postazioni di lavoro delle *Local Registration Authority* 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*;

11 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.

- informa il CAB della necessità di effettuare l'implementazione di nuove funzionalità/interventi corretti al sistema;
- recepisce le richieste, valuta le criticità e l'impatto delle soluzioni indicate dal CAB;
- formula raccomandazioni e fornisce suggerimenti al CAB sulle soluzioni di carattere informatico 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 *Local Registration Authority*;
- 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 *Local Registration Authority*;
- fornisce al CAB le statistiche sui malfunzionamenti rilevabili dai *ticket* gestiti dal *Card Management System*;
- 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* 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 sistema.

2.5. PROCEDURE PER LA MANUTENZIONE DEL SISTEMA

Durante la sua vita operativa il sistema 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 CMD.
- ***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 da adottare. La RFC deve contenere tutte le informazioni necessarie affinché un cambiamento possa essere valutato, approvato e implementato.

Pagina intenzionalmente bianca

3. STRUTTURA ORGANIZZATIVA DEI PROCESSI DI SERVIZIO

3.1. GENERALITÀ

Il rilascio e la gestione della CMD, 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 CMD, definendo, per ciascuno, le mansioni ricoperte:

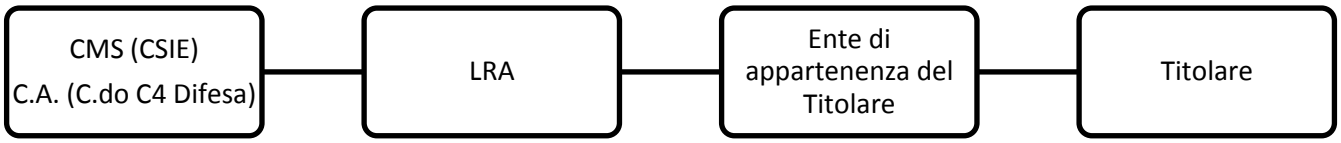


Figura 1 - Esemplificazione della struttura gerarchico-organizzativa

La figura sopra riportata illustra, dal punto di vista funzionale, la gerarchia che si stabilisce durante il ciclo di vita della CMD. 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 CMD.

Il ciclo di vita trova il confine naturale nel Titolare della carta, unico responsabile del corretto impiego della CMD 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 (Ag.ID)** e devono rispondere esattamente a tutte le specifiche tecniche/funzionali/organizzative definite dalle regole specificate nel **Codice dell'Amministrazione Digitale** (**CAD**).

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 CMD. Quale Certificatore accreditato a livello nazionale, nell'espletamento delle proprie funzioni risponde, a norma del CAD, all'**Agenzia per l'Italia Digitale (Ag.ID)**.

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 **Centro Sistemi Informatici dell'Esercito (CSIE)** 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 CMD.

In qualità di CMS, provvede alla personalizzazione e stampa delle CMD, in particolare:

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

3.4. LOCAL REGISTRATION AUTHORITY

Le *Local Registration Autority*, su delega della CA e della RA, sono responsabili della corretta applicazione delle procedure per la:

- distribuzione ai Titolari delle CMD ricevute dal CMS;
- raccolta e inoltro al CMS delle richieste di sospensione e/o revoca;
- raccolta delle CMD scadute e/o revocate, da consegnare al CMS;
- "nodo informativo" per i Titolari appartenenti alla LRA in diritto di richiedere e/o usufruire della CMD e dei servizi a essa associati.

3.5. TITOLARE DELLA CARTA

Il Titolare della CMD ha la responsabilità di:

- conservare la CMD 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 digitala dei quali è l'unico responsabile dal punto di vista legale;
- approntare le adeguate contromisure in caso di furto, smarrimento o compromissione della CMD, 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 CMD dovranno essere adottate le misure disciplinari previste dai regolamenti, dalle norme contrattuali e dalla legge in materia disciplinare [12]. 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 Regio Decreto del 18 novembre 1923 n. 2440.

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

4. CARTA MULTISERVIZI DELLA DIFESA (CMD)

4.1. GENERALITÀ

La Carta Multiservizi della Difesa risponde ai requisiti del DPCM del 24 maggio 2010 recante le "Regole tecniche delle Tessere di riconoscimento rilasciate con modalità elettronica dalle Amministrazioni dello Stato" [13] 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 DELLA CMD

La CMD 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.

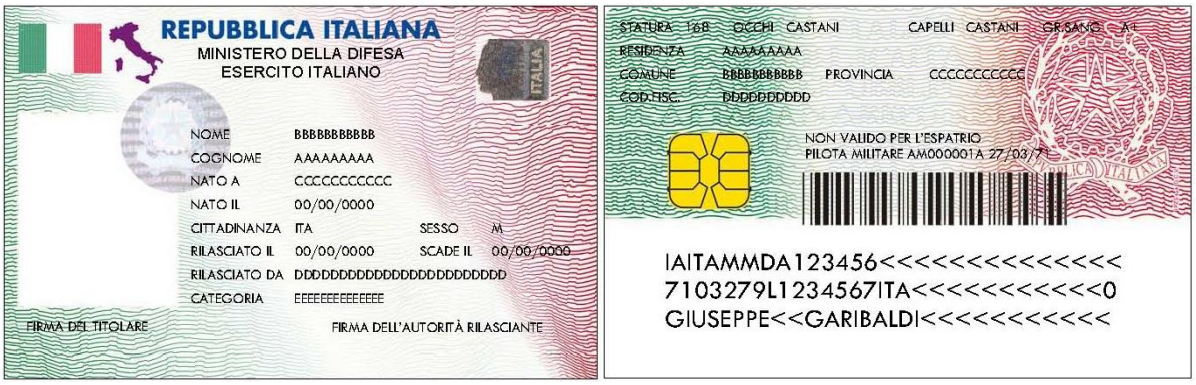


Figura 1 – *Layout* Carta

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

- alla **personalizzazione** dei certificati digitali della CMD 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 Centro Sistemi Informatici dell'Esercito –CSIE in Via Guido Reni, 22 Roma).

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

Sul lato posteriore sono riportati i dati fisici, la 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:

- la dicitura "non valido per l'espatrio";

13 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 88, del D. Lgs. 82/2005"*.

- 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 e elencati in all'Allegato I alla presente direttiva .

All'interno della carta, inoltre, è inserito un chip costituente il "cuore" tecnologico della CMD 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 certificato di cifra.

Così come strutturata, la CMD 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 DELLA CMD

La CMD costituisce la tessera personale di riconoscimento in formato elettronico (mod. ATe) rilasciato al personale militare e civile in servizio della Difesa[14]. L'emissione della carta 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:

- a tutto il personale militare e civile in servizio presso l'Amministrazione Difesa, compreso il personale militare VFP1 e Allievo delle Scuole Militari [15]. Per queste ultime due tipologie di personale militare è auspicabile che il rilascio della CMD 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 CMD potrà essere rilasciata anche a personale in servizio momentaneo presso l'Amministrazione della Difesa.

La CMD dovrà essere ritirata:

- 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[16];
- al personale militare rimosso dal grado o degradato. La CMD è altresì ritirata al militare a carico del quale è stato adottato un provvedimento di sospensione cautelare obbligatoria a norma delle disposizioni vigenti.

14 D.P.R. 28 luglio 1967, n. 851: Nome in materia di tessere di riconoscimento rilasciate dalle Amministrazioni dello Stato.
15 Sono esclusi i frequentatori delle Scuole di formazione militare.
16 Art. 1009 del Decreto Legislativo 15 marzo 2010, n. 66 – Codice dell'ordinamento militare. Al raggiungimento del congedo assoluto il Titolare della CMD dovrà restituire la carta ad una delle *Local Registration Authority* dislocate sul territorio nazionale (elenco in Allegato F).

4.4. DURATA

La CMD, 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 [17]. 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 dalla carta (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.

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 CMD prossima alla scadenza, debba essere impiegato in un teatro operativo fuori dal territorio nazionale: per evitare che la CMD 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 Periferico 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.

17 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"*

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 CMD due certificati digitali:

- un certificato di firma digitale;
- un certificato di autenticazione CNS.

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 ha l'efficacia prevista dall'art. 2702 del c.c. e fa piena prova in giudizio fino a querela di falso.

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 sui siti istituzionali di Regioni, Province, Comuni, ASL, Giustizia, ecc.).

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

STATO MAGGIORE DIFESA - Comando 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 CMD 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/Sicurezza/PKI-Firma-Digitale/Pagine/default.aspx

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

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;
- importanza della marcatura temporale incorporata nella firma e/o nel documento;
- 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

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 CMD **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 CMD

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

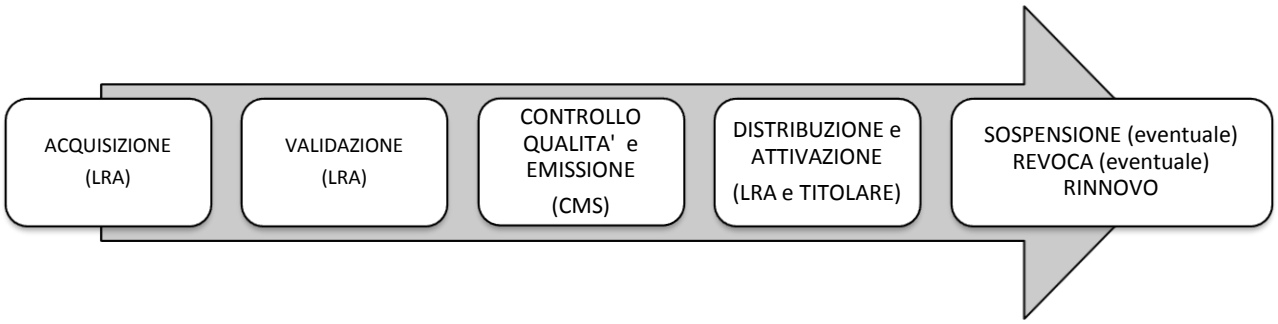


Figura 2 - Fasi del ciclo di vita della CMD

- **Acquisizione.** Il processo di acquisizione è effettuato presso una qualsiasi ***Local Registration Authority*** **(LRA)**, in linea con i regolamenti interni delle F.A., presentando il modulo in Allegato A debitamente compilato. La pratica di acquisizione per il rilascio della CMD 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'ECDR. In fase di inserimento, il sistema 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 CMD per esigenze di 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 Periferico (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[18] della CMD e include tutte le attività necessarie per finalizzare la consegna della carta al "Titolare"[19]. Tutte la attività di emissione sono gestite dal personale del CMS.
- **Attivazione e Consegna.** La CMD viene distribuita all'interno dell'Amministrazione Difesa attraverso la consegnata 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 CMD 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 CMD 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 CMD 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

[18] 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.

[19] 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 CMD 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 CMD.

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 CMD/CERTIFICATI DIGITALI

6.3.1. ACQUISIZIONE DEI DATI

La procedura acquisizione dei dati (*enrollment*), avviene presso i Locali Centri di Registrazione (***Local Registration Authority*** - LRA) inseriti in Allegato F e ha inizio solo dopo presentazione della richiesta cartacea (Allegato A) debitamente compilata dal richiedente e certificata dalla firmata dal Comandante di Corpo/Delegato.

Non è possibile rilasciare tessere di riconoscimento valide per l'espatrio al personale con figli minorenni senza l'assenso dell'altro genitore legittimo. In presenza di figli minori, qualora la CMD sia richiesta valida per l'espatrio, occorre integrare l'Allegato A con la firma dell'altro genitore allegando anche copia di un documento di riconoscimento dello stesso.

Il Responsabile del Trattamento (Allegato C), effettuata l'identificazione del richiedente a vista o con un documento di riconoscimento in corso di validità, provvede:

- all'acquisizione dei dati anagrafici, militari, amministrativi e biometrici (Allegato D), attraverso specifiche procedure;
- alla conferma da parte del richiedente, con firma grafometrica (nome e cognome) leggibile, dei dati raccolti;
- a convalidare i dati raccolti controfirmandoli con la propria firma digitale.

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 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 CMD per urgenti e improcrastinabili esigenze di servizio, sarà comunque possibile attivare una procedura di emissione della carta che dovrà essere accompagnata 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 Periferico della LRA convalida i dati attraverso un'apposita procedura di approvazione apponendo la propria firma digitale e 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 (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. In Allegato F è inserito l'elenco delle LRA dislocate sul territorio nazionale.

6.3.3. EMISSIONE E RILASCIO DELLA CMD

Allo scopo di delineare sommariamente il processo di emissione della CMD, in gran parte automatizzato, si enumerano 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 prima della personalizzazione stampa della CMD. 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 CMD;
- 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 CMD;
- genera all'interno della carta la terza coppia di chiavi e inoltra alla C.A.. di Cifra una richiesta di certificato di cifra. 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 CMD;
- inserisce i dati personali del Titolare nel chip, personalizzata 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@marina.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 CMD 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;
  - il codice necessario per accedere al portale e visualizzare i codici PIN e PUK relativi alla carta e alla firma digitale, utilizzabile una sola volta;

La consegna al Titolare della nuova CMD, è effettuata dal Responsabile del Trattamento 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 CMD con un lettore ottico, potrà accedere alla propria Area Riservata e visionare i codici PIN/PUK associati ai certificati presenti nel chip.

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

La consegna delle CMD emesse dal CMS avviene alla LRA mediante due procedure:

- consegna a mano al rappresentante della LRA in possesso di delega scritta da parte del Responsabile Periferico 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 CMD ritirate e disattivate, per la successiva distruzione.

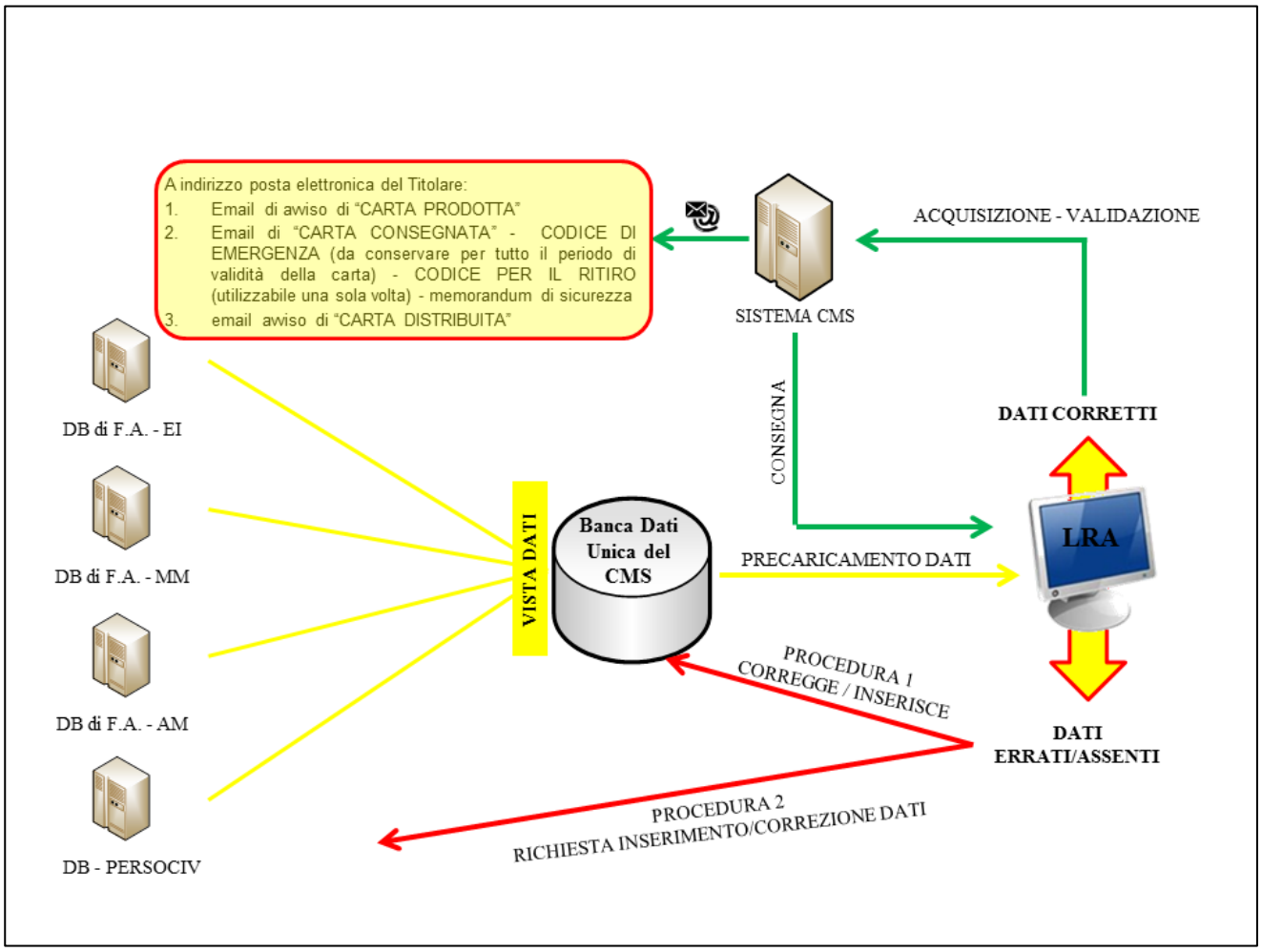


Figura 3 - Schema architetturale dell'infrastruttura dati CMD

6.4. RINNOVO DELLA CMD

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 CMD 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 CMD 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 Periferico 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 CMD, il Responsabile del Trattamento della LRA deve:

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

La LRA deve garantire la restituzione delle CMD 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 CMD/CERTIFICATI DIGITALI

6.5.1. CARTA MULTISERVIZI DELLA DIFESA

I possibili eventi che possono portare alla sospensione della CMD 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 CMD: 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****;*
- ***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** [20] *(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* [21]*, 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**[22] *(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").

20 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.

21 Comando C4 Difesa.

22 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 CMD.

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

6.6. REVOCA DELLA CMD/CERTIFICATI DIGITALI

Il processo di revoca è avviato per perdita del grado, smarrimento, furto o compromissione della CMD, 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 CMD 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 CMD 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 CMD 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, attivando così la revoca immediata della CMD. Inoltre il Titolare deve presentare formale denuncia alle autorità competenti entro le 24 ore successive alla comunicazione, consegnando copia della documentazione alla LRA necessaria anche per il rilascio di una nuova carta. 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.

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 CMD, da militare transita nello stato *civile*. Il cambio di status, difatti, segna il termine di possesso e uso della CMD 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. 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 CMD.
- **ALLEGATO B**: Memorandum di Sicurezza per Titolari della CMD.
- **ALLEGATO C**: Compiti del Responsabile Periferico e del Responsabile del Trattamento dei dati.
- **ALLEGATO D**: Istruzioni sul formato ICAO della foto.
- **ALLEGATO E:** Membri del *Change Advisory Board*.
- **ALLEGATO F**: Elenco delle *Local Registration Authority*.
- **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 CMD.

Pagina intenzionalmente bianca

ANNESSO 1

ELENCO DELLE DEFINIZIONI

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

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

TERMINE	DEFINIZIONE
ACQ	Modulo logico di acquisizione dati.
Algoritmo di hashing	Vedi *hash*.
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 / CMD	La Carta Multiservizi della Difesa (il supporto fisico) sulla quale sono stampigliati gli elementi identificativi del Titolare.
Carta Multiservizi della Difesa (CMD)	La carta 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 CMD, 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	Il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi 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 CMD.
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 CMD, 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 CMD 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 CMD.
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 CMD 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.I.D	*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*
CSIE	*Centro Sistemi Informatici dell'Esercito*
DII	*Defence Information Infrastructure*
DPCM	*Decreto del Presidente del Consiglio dei Ministri*
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*
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:

- **LEGGI E DECRETI**

1. *il 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";*
2. *la Legge (L.) 21 novembre 1967, n. 1185, e successive modificazioni, recante "Norme sui passaporti";*
3. *il DPR 6 agosto 1974, n. 649, art. 4 , recante "Disciplina dell'uso della carta d'identità e degli altri documenti equipollenti al passaporto ai fini dell'espatrio";*
4. *il DPR 28 dicembre 2000, n. 445, art. 35, comma 2, in tema di equipollenza alla carta di identità delle tessere di riconoscimento rilasciate da un'amministrazione dello Stato;*
5. *il Decreto Legislativo (D. Lgs.) 30 giugno 2003, n. 196, e successive modificazioni e integrazioni (s.m.i.), recante "Codice in materia di protezione dei dati personali";*
6. *il Decreto Ministeriale (D.M.) 4 agosto 2003 e s.m.i., recante "Istruzioni per la vigilanza ed il controllo sulla produzione delle carte valori e degli stampati a rigoroso rendiconto";*
7. *il DPR 2 marzo 2004, n. 117 e s.m.i., recante "Regolamento concernente la diffusione della carta nazionale dei servizi, a norma dell'art. 27, comma 8, lettera b), della legge 16 gennaio 2003, n. 3";*
8. *il D. Lgs. 7 marzo 2005, n. 82 e s.m.i. successive modificazioni, che all'art. 66, comma 8, stabilisce 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 (CNS) per consentire l'accesso per via telematica ai servizi erogati in rete dalle pubbliche amministrazioni;*
9. *il Decreto-Legge (D.L.) 31 gennaio 2005, n. 7 (articoli 7-vicies ter e 7-vicies quater) e s.m.i., in materia di rilascio di documentazione in formato elettronico e di carte valori;*
10. *il D.L. 4 novembre 2009, n. 152 (art. 3, comma 2), recante "Disposizioni urgenti per la proroga degli interventi di cooperazione allo sviluppo e a sostegno dei processi di pace e di stabilizzazione, nonché' delle missioni internazionali delle Forze armate e di polizia";*
11. *il DPR 2 marzo 2004, n. 117 e s.m.i., recante "Regolamento concernente la diffusione della carta nazionale dei servizi, a norma dell'art. 27, comma 8, lettera b), della legge 16 gennaio 2003, n. 3";*
12. *il Decreto del Ministro dell'interno 8 novembre 2007, pubblicato nella Gazzetta Ufficiale 9 novembre 2007, n. 261, S.O., recante "Regole tecniche della Carta d'identità elettronica";*
13. *la procedura di notifica alla Commissione europea di cui alla 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, attuata con decreto legislativo 23 novembre 2000, n. 427;*

14. *Decreto del Presidente del Consiglio dei Ministri (DPCM) 22 febbraio 2013, recante "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.*
15. *D. Lgs 82/2005 (Codice dell'Amministrazione Digitale – CAD), aggiornato con le modifiche e integrazioni introdotte dal D. Lgs. 235/2010.*
16. *Legge 24 Dicembre 2007, n. 244 - Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato. Art. 3 Comma 83.*

- **DIRETTIVE DELLA NATO**

AC/322-D(2007)0048 – "NATO Architectural Framework" (NAF) Ver.3, ed. 28 giugno 2007.

- **DIRETTIVE E STANDARD NAZIONALI E INTERNAZIONALI**

Direttiva europea 1999/93/CE "Relativa a un quadro comunitario per le firme elettroniche";

- **ALTRI DOCUMENTI**

1. *Resoconto di riunione del Comitato di Coordinamento Informatica del 21 settembre 2010 fg. prot. n. M_D SSMD 0078014 in data 28 settembre 2010;*
2. *Fg. prot. n. 0052165 del 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" (Stralcio);*
   b) *Annesso 5-L, "Accesso ai servizi, applicazioni e dati attraverso la CMD" (Stralcio);*
4. *Linee guida per l'utilizzo della firma digitale del CNIPA Ed. maggio 2004;*
5. *Circolare AIPA n. 24 del 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*

ALLEGATO A

MODULO RICHIESTA CMD

DICHIARAZIONE SOSTITUTIVA DI CERTIFICAZIONE

(resa ai sensi del DPR 445/2000 per il rilascio della CMD., art 46 [23])

VALIDA AI FINI DEL RILASCIO DELLA CMD ☐ CMD MEDICO ☐

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

Grado/area di appartenenza [24]_____ 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 [25] _____

senza prole minore/con prole minore estremi atto di nascita [26]_____
(barrare la casella **non** di interesse)

residente a _____ Prov. di (____) c.a.p. _____

via/piazza _____nr. _____

Tessera che si verserà all'atto della consegna della nuova CMD:

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

DATI AMMINISTRATIVI

Matricola _____ Categoria[27] _____

Ruolo [28] _____ Status [29] _____

Account email [30]_____ @ _____

---

23 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 …

24 Per il personale civile della A.D.

25 Dato non obbligatorio.

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

27 Civile – Truppa – Graduato – Sottufficiale – Ufficiale.

28 Legge 196/95: Ruolo Maresciallo – Ruolo Sergente.

29 Servizio Permanente – Ferma Prefissata - Riserva – Ausiliaria.

30 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 obbligatoriamente chiederne il rilascio alla propria amministrazione prima di eseguire l'acquisizione elettronica dei dati.

SEGUE ALLEGATO A

Anzianità assoluta ____ / ____ / _____ Anzianità di grado/di livello ___ / ___ /_____
Incarico principale _____

Reparto di appartenenza/Ente di servizio _____

Titolare di pensione SI - NO

DATI BIOMETRICI

Gruppo Sanguigno[31] _____ Statura (cm) _____ Colore capelli _____

Colore occhi _____ Segni particolari _____

PROFILO DI FIRMA

Chiede l'emissione di un certificato personale di firma digitale [32]:

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) (FIRMA DEL RICHIEDENTE) FIRMA DELL'ALTRO GENITORE (AVV. 1)

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

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

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

31 Colui che richiede la CMD, durante la fase di acquisizione, dovrà mostrare al responsabile del trattamento dei dati un documento che attesti il proprio gruppo sanguigno per la stampa sulla CMD. Sono documenti validi: la cartella sanitaria, il foglio matricolare, la piastrina di riconoscimento e qualsiasi altro documento certificato da personale medico / di laboratorio.

32 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 CMD valida per l'espatrio fare riferimento all'art. 3[33] lettera a., b., c., d., e., f., della Legge 21 novembre 1967 nr. 1185 e Legge n. 3/2003 art. 24[34]. Nel caso vi fossero condizioni ostative, verrà apposta la dizione "NON VALIDO PER L'ESPATRIO" nel campo NOTE della CMD. 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.
2. La presente richiesta deve essere consegnata a mano dal richiedente al Responsabile all'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[35]).
3. I Responsabili del Trattamento curano la restituzione delle carte dei propri dipendenti, per il successivo inoltro a CMS che le ha rilasciate, oltre che nei casi previsti dall'art. 4[36] 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[37]).

---

33 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);

34 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 e' necessaria quando il richiedente abbia l'assenso dell'altro genitore, o quando sia Titolare esclusivo della potestà sul figlio;".

35 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)

36 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.

37 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.

ALLEGATO B

MEMORANDUM DI SICUREZZA PER TITOLARI DELLA CARTA MULTISERVIZI DELLA DIFESA (CMD)

Destinatari: il personale dell'Amministrazione della Difesa.

Obiettivo: detto memorandum si prefigge di fornire indicazioni utili al fine di porre il Titolare della CMD 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 CMD 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 CMD sono previste sanzioni in attuazione ai regolamenti , alle norme contrattuali, ai regolamentari e alle legge in materia disciplinare sia per il personale militare sia per il personale civile[38]

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 [39]. 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 CMD per accedere ad informazioni coperte dal Segreto di Stato**.
- E' vietata la duplicazione della chiave privata di firma e dei dispositivi che la contengono [40].
- Non è consentito l'uso di una chiave per funzioni diverse da quelle previste dalla sua tipologia [41], 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[42].

38 Es. Decreto Legislativo 15 marzo 2010, n. 66 Codice dell'ordinamento militare e del Codice di comportamento (DPCM 28 novembre 2000).
39 D.Lgs. 82 del 7 marzo 2005 (Codice dell'Amministrazione Digitale)] art. 32, comma 1.
40 DPCM 13 gennaio 2004, art. 7: Conservazione delle chiavi.
41 DPCM 13 gennaio 2004, art. 4: Caratteristiche generali delle chiavi per la creazione e la verifica della firma.
42 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 CMD 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 CMD. dal deterioramento in quanto contenente la chiave privata, al fine di garantirne l'integrità e la massima riservatezza[43].
- 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 CMD.
- 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 1025040/2024444/06809925040/0646914444; 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; poi contattare il Responsabile Periferico per le successive operazioni di revoca o riattivazione.
- Devono essere prontamente comunicati al proprio Comando o direttamente al Responsabile Periferico della LRA di appartenenza i possibili malfunzionamenti riscontrati sul dispositivo di firma.
- Devono essere, altresì, prontamente comunicati al proprio Comando, direttamente al Responsabile Periferico 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.
- A seguito di sospensione del certificato, risolta la relativa causa, è necessario presentarsi presso il proprio Responsabile Periferico per richiedere la revoca o la riattivazione dello stesso.

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

SEGUE ALLEGATO B

- Richiedere immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma difettosi o smarriti[44].
- Sospendere l'utilizzo dei certificati della CMD 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 CMD 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.

44 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 CARTA 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 CMD;
- 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 CMD 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[45]. Infine si tenga conto delle problematiche relative alla eventuale presenza di macroistruzioni o codice eseguibile nel documento verificato.

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

ALLEGATO C

COMPITI DEL RESPONSABILE PERIFERICO

Il Responsabile Periferico della LRA è responsabile della richiesta di emissione della CMD per il militare /dipendente dagli ECDR che compongono la LRA, di militari/personale civile dell'AD in transito o effettivi a 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 Periferico " sarà il Comandante dell'Ente che la gestisce a cui è devoluta anche la responsabilità di firmare la CMD 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).

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

Per ogni LRA potrà essere attiva una sola CMD abilitata al portale CMS con profilo "Responsabile Periferico " .

Nell'ambito della propria LRA il Responsabile Periferico 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 CMD.
- approvare i dati rilevati per il rilascio della CMD;
- 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.

COMPITI DEL RESPONSABILE DEL TRATTAMENTO DEI DATI

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

"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 periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza." ***Art.28***

1) Il responsabile è designato dal Titolare 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.

SEGUE ALLEGATO C

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." ***Art. 29***

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." ***Art.30***

E' il responsabile dell'acquisizione dei dati ai fini dell'emissione della CMD 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, il Responsabile del Trattamento esegue le seguenti attività:

- 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 CMD 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 CMD, accertandone l'identità tramite documento di riconoscimento in corso di validità (mod. AT, mod. ATe, carta d'identità, patente di guida, passaporto[46]). 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 CMD la dicitura: NON VALIDA PER L'ESPATRIO;
- acquisisce i dati previsti per l'emissione della CMD;
- acquisisce i dati previsti per il rilascio del Passaporto Elettronico di Servizio;
- gestisce le pratiche di restituzioni delle CMD revocate/scadute;
- distribuisce la nuova CMD ai titolari;
- 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 Periferico ;

46 Riferimento DPR 445/2000.

SEGUE ALLEGATO C

- verifica eventuali inefficienze del chip delle CMD i cui titolari richiedono la sostituzione per inefficienza del chip prima di preparare la pratica di cambio stato.

COMPITI E RESPONSABILITÀ DELLE SEGRETERIE DEI REPARTI/UFFICI PER LA RICHIESTA DI EMISSIONE DELLA CARTA MULTISERVIZI DELLA DIFESA

- Distribuire al personale militare in servizio e civile, per la successiva compilazione, la richiesta per l'emissione della CMD (Allegato A alla Direttiva SMD-I-009);
- ritirare la richiesta di emissione CMD, 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 CMD 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 CMD da consegnare agli incaricati delle citate postazioni .
- Fornire al personale richiedente la CMD il supporto necessario in caso di dati non presenti in fase di precaricamento e/o incongruenti.

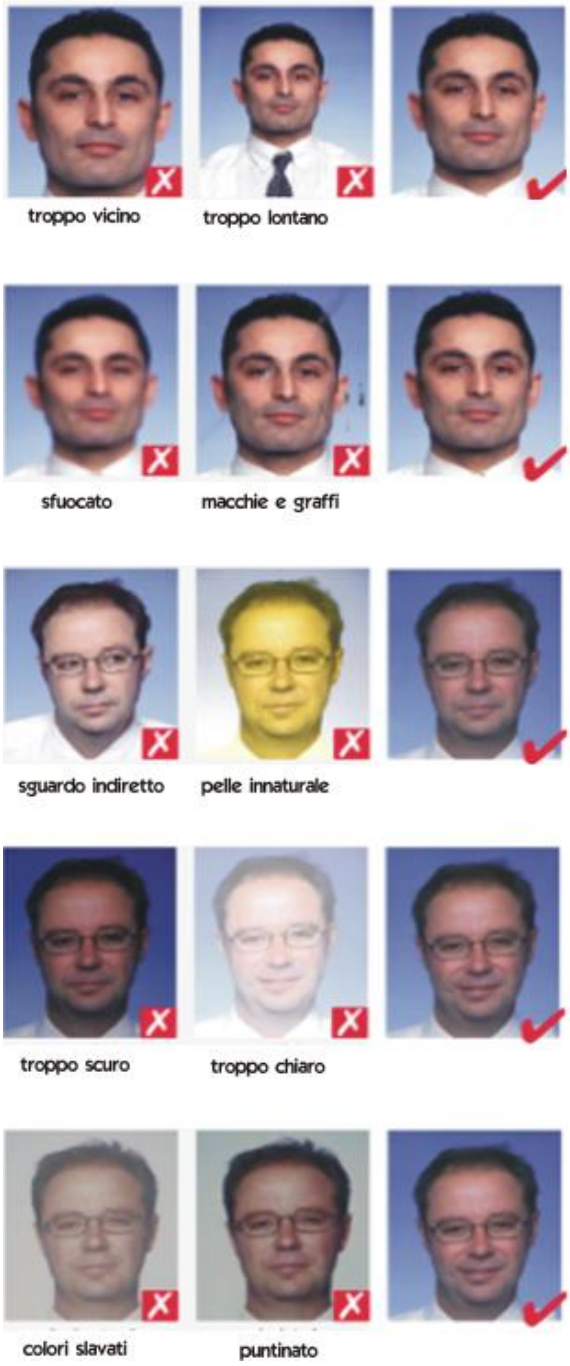
Pagina intenzionalmente bianca

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

SMD I Reparto	Rappresentante nominato dallo **SMD** *I Reparto*
SMD VI Reparto	Rappresentante Ufficio Sistemi Informatici Gestionali
Comando C4 Difesa	Capo Sezione PKI Difesa
SME - IV Reparto	Capo Sezione Certificazione e Produzione CMD. Svolge la funzione di Presidente del CAB
SMM– Reparto C4S	Rappresentante Ufficio Informatica Gestionale
SMA	Rappresentante Ufficio Informatica
SGD	Rappresentante nominato dal SGD

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

ELENCO DELLE LOCAL REGISTRATION AUTHORITY

FA	DENOMINAZIONE ENTE	INDIRIZZO	CITTA	CAP	PROV	REGIONE
AM	DISTACCAMENTO AERONAUTICA MILITARE - CAPO MELE	STRADA DELLE CATENE, 16-25	ANDORA	17051	SV	LIGURIA
AM	CENTRO LOGISTICO DI SUPPORTO AREALE/ISTITUTO U. MADDALENA	VIA DELLA MARINA, 15	CADIMARE	19131	SP	LIGURIA
AM	COMANDO AEROPORTO/QG 1^ REGIONE AEREA	VIA DELL'AVIAZIONE, 1	LINATE	20100	MI	LOMBARDIA
AM	COMANDO AEROPORTO - CAMERI	STRADA PER BELLINZAGO NOVARESE, SNC	CAMERI	28062	NO	PIEMONTE
AM	50 STORMO	VIA GODI 1/A	PIACENZA	29121	PC	EMILIA ROMAGNA
AM	51 STORMO	VIA MONTE GRAPPA, 83	ISTRANA	31036	TV	VENETO
AM	3 REPARTO MANUTENZIONE VELIVOLI	VIA CANIZZANO, 22	TREVISO	31100	VE	VENETO
AM	2 STORMO - RIVOLTO - UD	VIA UDINE, 56	CODROIPO (RIVOLTO)	33033	UD	FRIULI
AM	COMANDO AEROPORTO AVIANO	VIA PIONIERI DELL'ARIA, 1	AVIANO	33081	PN	FRIULI
AM	2 REPARTO MANUTENZIONE MISSILI	VIA SORIO, 87	PADOVA	35100	PD	VENETO
AM	3 STORMO	LOCALITÀ CALURI	VILLAFRANCA DI VERONA	37069	VR	VENETO
AM	4 REPARTO TECNICO MANUTENTIVO DIFESA AEREA ASSIST.VOLO E TLC	VIA DELLA CHIESUOLA, 78	BORGO PIAVE	40100	LT	LAZIO
AM	REPARTO SUPPORTO SERVIZI GENERALI	VIA CANTONE, 14	POGGIO RENATICO	44028	FE	EMILIA ROMAGNA
AM	15 STORMO - CERVIA	VIA CONFINE, 547	CERVIA	48015	RA	EMILIA ROMAGNA
AM	ISTITUTO DI SCIENZE MILITARI AERONAUTICHE	VIALE DELL'AERONAUTICA, 14	FIRENZE	50144	FI	TOSCANA
AM	46 BRIGATA AEREA	VIA CADUTI DI KINDU, 1	PISA	56121	PI	TOSCANA
AM	4 STORMO - GROSSETO	VIA CASTIGLIONESE, 70	GROSSETO	58100	GR	TOSCANA
AM	SCUOLA LINGUE ESTERE	VIA SAN GIOVANNI BOSCO, 31	LORETO	60025	AN	MARCHE
AM	133 SQUADRIGLIA RADAR REMOTA	VIA VALLELUNGA, 45	S.GIOVANNI TEATINO	66020	CH	ABRUZZO
AM	36 STORMO GIOIA DEL COLLE	VIA FEDERICO II DI SVEVIA, 6738	GIOIA DEL COLLE	70023	BA	PUGLIA
AM	QG COMANDO SCUOLE/3^ REGIONE AEREA	LUNGOMARE NAZARIO SAURO, 39	BARI	70121	BA	PUGLIA
AM	32 STORMO – AMENDOLA	SS. 89 PER MANFREDONIA	AMENDOLA	71040	FG	PUGLIA
AM	DISTACCAMENTO AEROPORTUALE - BRINDISI	VIA UMBERTO MADDALENA, 54	BRINDISI	72100	BR	PUGLIA
AM	61 STORMO - GALATINA	SS. 476 GALATINA C/O AEROPORTO LECCE	GALATINA	73013	LE	PUGLIA
AM	16 STORMO - PROTEZIONE DELLE FORZE	VIA MASSAFRA, 143	MARTINA FRANCA	74015	TA	PUGLIA
AM	SCUOLA VOLONTARI DI TRUPPA A.M.	VIA RONDINELLA CONTRADA PIZZONE	TARANTO	74121	TA	PUGLIA
AM	ACCADEMIA AERONAUTICA - POZZUOLI	VIA S. GENNARO AGNANO, 30	POZZUOLI	80078	NA	CAMPANIA
AM	COMANDO AEROPORTO - CAPODICHINO	VIALE COMANDANTE UMBERTO MADDALENA, 9	NAPOLI	80144	NA	CAMPANIA
AM	9 STORMO	VIA DELL'AEROPORTO, 1	GRAZZANISE	81046	CE	CAMPANIA
AM	SCUOLA SPECIALISTI A.M.	VIA NAZIONALE APPIA, 2/A C	CASERTA	81100	CE	CAMPANIA
AM	DISTACCAMENTO MONTESCURO (CS)	FORESTA DEMANIALE SILA DI TASSO MONTE SCURO –	CAMIGLIATELLO SILANO	87052	CS	CALABRIA
AM	DISTACCAMENTO AEROPORTUALE - PANTELLERIA	CONTRADA MARGANO	PANTELLERIA	91017	TP	SICILIA
AM	37 STORMO	SP. TRAPANI-MARSALA, 2	MARSALA	91025	TP	SICILIA
AM	DISTACCAMENTO AERONAUTICO - LAMPEDUSA	VIA CALAFRANCESE, S.N.C.	LAMPEDUSA	92010	AG	SICILIA
AM	41 STORMO ANTISOM	STRADA PROVINCIALE 69 PIANO D'ARCI	LENTINI	96016	SR	SICILIA

FA	DENOMINAZIONE ENTE	INDIRIZZO	CITTA	CAP	PROV	REGIONE
AM	DISTACCAMENTO AERONAUTICO - SIRACUSA	VIA ELORINA, 23	SIRACUSA	96100	SR	SICILIA
AM	11 DEPOSITO CENTRALE A.M. ORTE	VIA VOCABOLO LUCIGNANO, 1	ORTE	O1028	VT	LAZIO
AM	SCUOLA MARESCIALLI A.M./COMANDO AEROPORTO VITERBO	STRADA TUSCANESE, 71H	VITERBO	O1100	VT	LAZIO
AM	DISTACCAMENTO AERONAUTICO MONTE TERMINILLO (RI)	PIAN DE' VALLI - VIA DEI VILLINI, 169	RIETI	O2100	RI	LAZIO
AM	72 STORMO	VIA ARMANDO FABI, 192	FROSINONE	O3100	FR	LAZIO
AM	70 STORMO	VIA DELL'AEROPORTO, 1	LATINA	O4100	LT	LAZIO
AM	DISTACCAMENTO AEROPORTUALE ALGHERO (SS)	REGIONE NURAGHE BIANCHU, SNC	ALGHERO	O7041	SS	SARDEGNA
AM	POLIGONO SPERIMENTALE E DI ADDESTRAMENTO INTERFORZE - PERDAS	VIA COLOMBO, 1	PERDASDEFOGU	O8046	OG	SARDEGNA
AM	DISTACCAMENTO AEROPORTUALE ELMAS	C/O AEROPORTO DI CAGLIARI-ELMAS	ELMAS	O9030	CA	SARDEGNA
AM	REPARTO SPERIMENTALE E DI STANDARDIZZAZIONE TIRO AEREO	STRADA STATALE 196 KM 4	VILLASOR	O9034	CA	SARDEGNA
AM	COMANDO AEROPORTO / QG DEL COMAER	VIA DI CENTOCELLE, 301	ROMA	OO100	RM	LAZIO
AM	REPARTO SISTEMI INFORMATIVI AUTOMATIZZATI (RE.S.I.A.)	VIA APPIA PIGNATELLI, 123	ROMA	OO178	RM	LAZIO
AM	COMANDO AERONAUTICA MILITARE ROMA	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
AM	COMANDO LOGISTICO 2 DIVISIONE	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
AM	COMANDO LOGISTICO 3 DIVISIONE	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
AM	COMANDO LOGISTICO DELL A.M.	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
AM	DIREZIONE IMPIEGO PERSONALE MILITARE AERONAUTICA	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
AM	ISPETTORATO PER LA SICUREZZA DEL VOLO	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
AM	SERVIZIO DEI SUPPORTI - COMANDO LOGISTICO AM	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
AM	SERVIZIO DI COMMISSARIATO E AMMINISTRAZIONE - COMANDO LOGISTICO	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
AM	SERVIZIO INFRASTRUTTURE - COMANDO LOGISTICO	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
AM	SERVIZIO SANITARIO A.M. - COMANDO LOGISTICO	VIA PIERO GOBETTI, 2A	ROMA	OO185	RM	LAZIO
AM	SMA 1 REPARTO	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
AM	SMA 3 REPARTO	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
AM	SMA 4 REPARTO	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
AM	SMA 6 REPARTO	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
AM	SMA REPARTO GENERALE SICUREZZA	VIALE DELL'UNIVERSITÀ', 4	ROMA	OO185	RM	LAZIO
AM	STATO MAGGIORE AERONAUTICA - UFFICIO SOTTOCAPO	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
AM	UFFICIO GENERALE COMUNICAZIONE EX 5 REPARTO - ROMA	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
AM	COMANDO AEROPORTO/GRUPPO DI VOLO A VELA DI GUIDONIA	VIA ROMA, 26	GUIDONIA	OOO12	RM	LAZIO
AM	1 DIVISIONE COMLOG - PRATICA DI MARE	VIA PRATICA DI MARE, 45	POMEZIA	OOO40	RM	LAZIO
AM	6 REPARTO MANUTENZIONE ELICOTTERI	VIA PRATICA DI MARE, 45	POMEZIA	OOO40	RM	LAZIO
AM	COMANDO AEROPORTO PRATICA DI MARE	VIA PRATICA DI MARE, 45	POMEZIA	OOO40	RM	LAZIO
AM	31 STORMO	VIA APPIA NUOVA, 1651	CIAMPINO	OOO43	RM	LAZIO
AM	17 STORMO	FURBARA - VIA AURELIA KM 47,200	CERVETERI	OOO52	RM	LAZIO
AM	CENTRO TECNICO RIFORNIMENTI	VIA PORTUENSE, 1818	ROMA	OOO54	RM	LAZIO
AM	COMANDO AEROPORTO/CENTRO STORIOGRAFICO E SPORTIVO AM	VIA CIRCUMLACUALE, 41	VIGNA DI VALLE	OOO62	RM	LAZIO
EI	3 REGGIMENTO ALPINI	VIA STRADALE SAN SECONDO, 7	PINEROLO	10064	TO	PIEMONTE
EI	34 GRUPPO SQUADRONI AVES "TORO"	VIA CARLO GRASSI, 47	VENARIA REALE	10078	TO	PIEMONTE
EI	1 REGGIMENTO DI MANOVRA	CORSO SUSA, 189	RIVOLI	10098	TO	PIEMONTE

FA	DENOMINAZIONE ENTE	INDIRIZZO	CITTA	CAP	PROV	REGIONE
EI	COMANDO REGIONE MILITARE NORD	CORSO VINZAGLIO, 6	TORINO	10121	TO	PIEMONTE
EI	COMANDO PER LA FORMAZIONE E SCUOLA DI APPLICAZIONE DELL ESERCITO	VIA DELL'ARSENALE, 22	TORINO	10121	TO	PIEMONTE
EI	1 REPARTO INFRASTRUTTURE (TO)	PIAZZETTA ACCADEMIA MILITARE, 3	TORINO	10124	TO	PIEMONTE
EI	BATTAGLIONE T."FREJUS"	CORSO UNIONE SOVIETICA, 100	TORINO	10134	TO	PIEMONTE
EI	REPARTO COMANDO E SPT.TAT."TAURINENSE"	CORSO IV NOVEMBRE, 3	TORINO	10136	TO	PIEMONTE
EI	DIPARTIMENTO MILITARE DI MEDICINA LEGALE TIPO B (TO)	VIA BARLETTA, 14/B	TORINO	10136	TO	PIEMONTE
EI	32 REGGIMENTO GENIO GUASTATORI (FORZE LEGGERE ALP)	CORSO BRUNELLESCHI, 112	TORINO	10142	TO	PIEMONTE
EI	CENTRO ADD.ALP.-SCUOLA MILITARE	VIA SCUOLA MILITARE ALPINA, 17	AOSTA	11100	AO	VALLE D'AOSTA
EI	1 REGGIMENTO A.TER.(MON.)	VIA ANGELO PACCHIOTTI, 3	FOSSANO	12045	CN	PIEMONTE
EI	PARCO MEZZI CINGOLATI E CORAZZATI	VIA DEI CAPANNONI, 1	LENTA	13035	VC	PIEMONTE
EI	52 REGGIMENTO A.TER "TORINO"	CORSO PAPA GIOVANNI PAOLO II, 35	VERCELLI	13100	VC	PIEMONTE
EI	CDO SCUTEL	VIA PARMA, 34	CHIAVARI	16043	GE	LIGURIA
EI	COMANDO MILITARE ESERCITO LIGURIA	LARGO DELLA ZECCA, 2	GENOVA	16124	GE	LIGURIA
EI	3 CENTRO RIFORNIMENTI MANTENIMENTO	VIA TANZI, 5	MILANO	20010	MI	LOMBARDIA
EI	SCUOLA MILITARE "TEULIE'"	CORSO ITALIA, 58	MILANO	20122	MI	LOMBARDIA
EI	3 REPARTO INFRASTRUTTURE (MI)	VIA PAGANO MARIO, 22	MILANO	20145	MI	LOMBARDIA
EI	REGGIMENTO ART.CAVALLO	PIAZZALE GIUSEPPE PERRUCCHETTI, 1	MILANO	20147	MI	LOMBARDIA
EI	1 REGGIMENTO TRASMISSIONI	PIAZZALE GIUSEPPE PERRUCCHETTI, 1	MILANO	20147	MI	LOMBARDIA
EI	DIPARTIMENTO MILITARE DI MEDICINA LEGALE TIPO A (MI)	VIA SIMONE SAINT BON, 7	MILANO	20147	MI	LOMBARDIA
EI	COMANDO MILITARE ESERCITO LOMBARDIA	VIA CARACCIOLO, 29 / VIA VINCENZO MONTI, 59	MILANO	20155	MI	LOMBARDIA
EI	COMANDO BRIGATA DI SUPPORTO AL NRDC-ITA (HQ)	VIA PER BUSTO , 20	SOLBIATE OLONA	21058	VA	LOMBARDIA
EI	REGGIMENTO SPT. TATTICO E LOGISTICO (HQ)NRDC-ITA	VIA PER BUSTO , 20	SOLBIATE OLONA	21058	VA	LOMBARDIA
EI	CENTRO DOCUMENTALE COMO	PIAZZALE MONTE SANTO, 2	COMO	22100	CO	LOMBARDIA
EI	3 REGGIMENTO SOSTEGNO AVES "AQUILA"	VIA CAVOUR, 26	ORIO AL SERIO	24050	BG	LOMBARDIA
EI	CENTRO DOCUMENTALE BRESCIA	VIA CALLEGARI, 1	BRESCIA	25121	BS	LOMBARDIA
EI	10 REGGIMENTO G.GUA.	VIA BRESCIA , 189	CREMONA	26100	CR	LOMBARDIA
EI	1 REGGIMENTO TRASPORTI	VIA BORNAGO, 1	BELLINZAGO NOVARESE	28043	NO	PIEMONTE
EI	2 REGGIMENTO GENIO PONTIERI	PIAZZA ALESSANDRO CASALI, 12	PIACENZA	29121	PC	EMILIA ROMAGNA
EI	POLO MANTENIMENTO PESANTE NORD	VIALE MALTA 18	PIACENZA	29121	PC	EMILIA ROMAGNA
EI	MAGAZZINO CENTRALE RICAMBI AUTO	VIA DELLE NOVATE, 43	PIACENZA	29122	PC	EMILIA ROMAGNA
EI	5 REGGIMENTO A.TER.LRZ. "SUPERGA"	VIALE TRIESTE, 169	PORTOGRUARO	30026	VE	VENETO
EI	PRESIDIO MILITARE VENEZIA	RIVA DEGLI SCHIAVONI, 4142	VENEZIA	30122	VE	VENETO
EI	REGGIMENTO LAG."SERENISSIMA"	VIA TERRAIO , 42	MESTRE	30173	VE	VENETO
EI	MULTINATIONAL CIMIC GROUP	VIA R. SCARPA, 75	MOTTA DI LIVENZA	31045	TV	VENETO
EI	SEZIONE RIF.MANTENIMENTO (TV)	VIA ZERMANESE, 241	TREVISO	31100	TV	VENETO
EI	184 REGGIMENTO SOSTEGNO TLC. "CANSIGLIO"	VIA LUNGO IL FIUME CERCA, 10	TREVISO	31100	TV	VENETO
EI	REPARTO SVIL.INT.SIST.C4/COMANDO C4 IEW	VIA LUNGO FIUME CERCA, 10	TREVISO	31100	TV	VENETO
EI	COMANDO B.LOG.DI PROIEZIONE	VIA ZERMANESE , 178	TREVISO	31100	TV	VENETO
EI	33 REGGIMENTO EW	VIA FELTRINA, 99	TREVISO	31100	TV	VENETO
EI	7 REGGIMENTO ALPINI	VIA COL DI LANA , 5	BELLUNO	32100	BL	VENETO

FA	DENOMINAZIONE ENTE	INDIRIZZO	CITTA	CAP	PROV	REGIONE
EI	BATTAGLIONE ALP. TOLMEZZO	VIA UDINE, 3 / VIA ARMANDO DIAZ, 35	VENZONE	33010	UD	FRIULI
EI	3 REGGIMENTO A.TER.(MON.)	VIA PIO PASCHINI , 21	TOLMEZZO	33028	UD	FRIULI
EI	REGGIMENTO C.LINEA "LANC.DI NOVARA"(5)	VIA STAZIONE, 70	CODROIPO	33033	UD	FRIULI
EI	8 REGGIMENTO ALPINI	VIA UDINE, 3	CIVIDALE DEL FRIULI	33043	UD	FRIULI
EI	8 REGGIMENTO TRASPORTI	VIALE DEL SOLE, 105	REMANZACCO	33047	UD	FRIULI
EI	REGGIMENTO C.LINEA "GENOVA CAVAL."(4)	VIALE DEGLI SPERONI 2	PALMANOVA	33057	UD	FRIULI
EI	5 REGGIMENTO AVES "RIGEL"	VIALE VENEZIA, 79	CASARSA DELLA DELIZIA	33072	PN	FRIULI
EI	7 REGGIMENTO TRASMISSIONI	VICOLO MARIO DAL FABBRO, 15	SACILE	33077	PN	FRIULI
EI	11 REGGIMENTO BERSAGLIERI	VIA CASARSA N. 77	ORCENICO SUPERIORE	33080	PN	FRIULI
EI	132 REGGIMENTO CARRI	VIA MARTIRI DELLA LIBERTA', 163	CORDENONS	33084	PN	FRIULI
EI	BATTAGLIONE LOG."ARIETE"	VIA PORDENONE, 94	MANIAGO	33085	PN	FRIULI
EI	132 REGGIMENTO A.TER.(SMV)"ARIETE"	VIA PORDENONE, 94	MANIAGO	33085	PN	FRIULI
EI	32 REGGIMENTO CARRI	VIA BASALDELLA, 14	TAURIANO DI SPILIMBERGO	33097	PN	FRIULI
EI	COMANDO B.ALP."JULIA"	VIA SANT'AGOSTINO, 6-8	UDINE	33100	UD	FRIULI
EI	3 REGGIMENTO GENIO GUASTATORI	VIA SAN ROCCO , 180	UDINE	33100	UD	FRIULI
EI	REPARTO COMANDO E SPT.TAT."JULIA"	VIA FRUCH, 4	UDINE	33100	UD	FRIULI
EI	12 REPARTO INFRASTRUTTURE (UD)	VIA I° MAGGIO, 27	UDINE	33100	UD	FRIULI
EI	CENTRO DOCUMENTALE UDINE	VIA PRACCHIUSO, 16	UDINE	33100	UD	FRIULI
EI	COMANDO 132^ B.COR."ARIETE"	VIA MONTEREALE, 25	PORDENONE	33170	PN	FRIULI
EI	REPARTO COMANDO E SPT.TAT."ARIETE"	VIA MONTEREALE, 25	PORDENONE	33170	PN	FRIULI
EI	COMANDO MILITARE ESERCITO FRIULI VENEZIA GIULIA	VIA DELL'UNIVERSITA', 2	TRIESTE	34123	TS	FRIULI
EI	REGGIMENTO C.LINEA "PIEMONTE"(2)	VIA DI PROSECCO, 241	VILLA OPICINA	34151	TS	FRIULI
EI	COMANDO B.C."POZZUOLO FRIULI"	PIAZZA CESARE BATTISTI , 9	GORIZIA	34170	GO	FRIULI
EI	REPARTO COMANDO E SPT.TAT."P.DEL FRIULI"	VIA TRIESTE , 54	GORIZIA	34170	GO	FRIULI
EI	COMANDO INFRASTRUTTURE NORD (PD)	PIAZZA PRATO DELLA VALLE, 64	PADOVA	35123	PD	VENETO
EI	COMANDO LOGISTICO NORD	PIAZZA PRATO DELLA VALLE, 64	PADOVA	35123	PD	VENETO
EI	REPARTO SPT.GEN./COMANDO L.NORD.	VIA SAN MICHELE ARCANGELO , 84	PADOVA	35123	PD	VENETO
EI	32 REGGIMENTO TRASMISSIONI	VIA CHIESANUOVA, 68	PADOVA	35136	PD	VENETO
EI	15 CENTRO RIFORNIMENTI MANTENIMENTO	VIA DUE PALAZZI, 67	PADOVA	35136	PD	VENETO
EI	DIPARTIMENTO MILITARE DI MEDICINA LEGALE TIPO A (PD)	VIA SAN GIOVANNI DI VERDARA, 123	PADOVA	35137	PD	VENETO
EI	5 REPARTO INFRASTRUTTURE (PD)	VICOLO SAN BENEDETTO, 28	PADOVA	35139	PD	VENETO
EI	COMANDO MILITARE ESERCITO VENETO	VIA CRISTOFORO MORO, 7	PADOVA	35141	PD	VENETO
EI	PARCO MATERIALI MOTORIZZAZIONE E GENIO	VIA MANDELLA, 1	PESCHIERA DEL GARDA	37019	VR	VENETO
EI	8 REGGIMENTO GENIO GUASTATORI (FORZE LEGGERE PAR.)	VIA DEL PONTIERE, 16	LEGNAGO	37045	VR	VENETO
EI	CERICO (VR)	VIA GEMMETTO, 60	CA' DI DAVID	37061	VE	VENETO
EI	COMANDO FORZE OPERATIVE TERRESTRI (HQ)	VIA ROMA, 31	VERONA	37121	VR	VENETO
EI	QUARTIER GENERALE ITALIANO	PIAZZA POZZA, 1	VERONA	37123	VR	VENETO
EI	CENTRO DOCUMENTALE VERONA	VIA XX SETTEMBRE, 72	VERONA	37129	VR	VENETO
EI	85 RAV. "VERONA"	VIA SAN MICHELE, 6	MONTORIO VERONESE	37141	VE	VENETO
EI	4 REGGIMENTO ALPINI (PARACADUTISTI)	VIA SAN MICHELE, 6	MONTORIO VERONESE	37141	VR	TRENTINO ALTO ADIGE

FA	DENOMINAZIONE ENTE	INDIRIZZO	CITTA	CAP	PROV	REGIONE
EI	2 REGGIMENTO ART.TER. ALPINO "VICENZA"	VIA DELLE GHIAIE , 24	TRENTO	38122	TN	TRENTINO ALTO ADIGE
EI	COMANDO MILITARE ESERCITO TRENTINO ALTO ADIGE	VIA DELLE GHIAIE , 24	TRENTO	38122	TN	TRENTINO ALTO ADIGE
EI	2 REGGIMENTO GENIO GUASTATORI	VIA LA CLARINA, 3	TRENTO	38123	TN	TRENTINO ALTO ADIGE
EI	24 REGGIMENTO DI MANOVRA ALPINO	VIA CASERME , 8	MERANO	39012	BZ	TRENTINO ALTO ADIGE
EI	6 REGGIMENTO ALPINI (GEST.ISOLA ADD.VALP.)	VIA DANTE , 27	BRUNICO	39031	BZ	TRENTINO ALTO ADIGE
EI	5 REGGIMENTO ALPINI	VIA ALTA, 16	VIPITENO	39049	BZ	TRENTINO ALTO ADIGE
EI	COMANDO TRUPPE ALPINE	PIAZZA IV NOVEMBRE , 6	BOLZANO	39100	BZ	TRENTINO ALTO ADIGE
EI	REPARTO COMANDO E SPT.TAT.TRIDENTINA	VIALE DRUSO, 110	BOLZANO	39100	BZ	TRENTINO ALTO ADIGE
EI	4 REGGIMENTO AVES "ALTAIR"	VIA FRANCESCO BARACCA, 7	SAN GIACOMO DI LAIVES	39100	BZ	TRENTINO ALTO ADIGE
EI	2 REGGIMENTO TRASMISSIONI ALPINO	VIA VITTORIO VENETO, 82	BOLZANO	39100	BZ	TRENTINO ALTO ADIGE
EI	4 REPARTO INFRASTRUTTURE (BZ)	VIA VITTORIO VENETO, 84	BOLZANO	39100	BZ	TRENTINO ALTO ADIGE
EI	REGGIMENTO GENIO FERROVIERI	VIALE DELLE RIMEMBRANZE, 1	CASTELMAGGIORE	40013	BO	EMILIA ROMAGNA
EI	6 REGGIMENTO TRASPORTI	VIA ZENDALINO SUD, 20	BUDRIO	40054	BO	EMILIA ROMAGNA
EI	BATTAGLIONE ESERCIZIO/RGT.G.FV (OZZANO)	VIA MARCONI, 14	OZZANO DELL'EMILIA	40064	BO	EMILIA ROMAGNA
EI	REPARTO COMANDO SPT.TAT. /B.AEROMOBILE FRIULI	VIALE GIOVANNI VICINI, 32	BOLOGNA	40122	BO	EMILIA ROMAGNA
EI	6 REPARTO INFRASTRUTTURE (BO)	VIA SANTA MARGHERITA, 21	BOLOGNA	40123	BO	EMILIA ROMAGNA
EI	COMANDO MILITARE ESERCITO EMILIA ROMAGNA	VIA URBANA, 8	BOLOGNA	40123	BO	EMILIA ROMAGNA
EI	2 REGGIMENTO SOSTEGNO AVES "ORIONE"	VIA DELL'AEROPORTO	BOLOGNA	40132	BO	EMILIA ROMAGNA
EI	121 REGGIMENTO A.C/A E."RAVENNA"	VIA DUE MADONNE, 9/2	BOLOGNA	40139	BO	EMILIA ROMAGNA
EI	ACCADEMIA MILITARE ESERCITO	PIAZZA ROMA, 15	MODENA	41121	MO	EMILIA ROMAGNA
EI	4 REGGIMENTO A.C/A E."PESCHIERA"	VIA DEI TOSCANI, 28	MANTOVA	46100	MN	LOMBARDIA
EI	66 REGGIMENTO FANTERIA AEROMOBILE "TRIESTE"	VIALE ROMA, 151	FORLI'	47100	FC	EMILIA ROMAGNA
EI	7 REGGIMENTO AVES "VEGA"	VIA FLAMINIA, 407	MIRAMARE DI RIMINI	47831	RN	EMILIA ROMAGNA
EI	II GR.A.C/A/121RGT A.C/A(RIMINI)	VIA FLAMINIA, 66	RIMINI	47923	RN	EMILIA ROMAGNA
EI	ISTITUTO GEOGRAFICO MILITARE	VIA CESARE BATTISTI , 10	FIRENZE	50121	FI	TOSCANA
EI	COMANDO INFRASTRUTTURE CENTRO (FI)	VIA CAMILLO BENSO CAVOUR, 49	FIRENZE	50121	FI	TOSCANA
EI	COMANDO MILITARE ESERCITO TOSCANA	VIA CAMILLO BENSO CAVOUR, 49	FIRENZE	50121	FI	TOSCANA
EI	7 REPARTO INFRASTRUTTURE (FI)	VIA DI NOVOLI, 48	FIRENZE	50127	FI	TOSCANA
EI	COMANDO MILITARE PER IL TERRITORIO DELL ESERCITO	VIALE DEL GIGNORO, 34	FIRENZE	50135	FI	TOSCANA
EI	BATTAGLIONE T."ABETONE"/ 3 REGGIMENTO T.	VIA ARETINA, 354	FIRENZE	50136	FI	TOSCANA
EI	COMANDO DIVISIONE MANTOVA	VIA ARETINA, 356	FIRENZE	50136	FI	TOSCANA
EI	183 REGGIMENTO PAR."NEMBO"	VIALE ITALIA, 68	PISTOIA	51100	PT	TOSCANA
EI	186 REGGIMENTO PAR. "FOLGORE"	PIAZZA AMENDOLA, 27	SIENA	53100	SI	TOSCANA
EI	CENTRO ADD.PARACADUTISMO	VIA DI GELLO, 138	PISA	56123	PI	TOSCANA
EI	6 REGGIMENTO DI MANOVRA	VIA DERNA ,2	PISA	56126	PI	TOSCANA
EI	REPARTO COMANDO E SPT.TAT."FOLGORE"	VIALE G. CARDUCCI, 91	LIVORNO	57027	LI	TOSCANA
EI	COMANDO B.PAR."FOLGORE"	VIALE MARCONI	LIVORNO	57125	LI	TOSCANA
EI	185 REGGIMENTO PAR. RICOGN. ACQUISIZ. OBJ. "FOLGORE"	VIALE MARCONI, 5	LIVORNO	57125	LI	TOSCANA
EI	187 REGGIMENTO PAR. "FOLGORE"	VIA DELL'ARDENZA, 133	LIVORNO	57128	LI	TOSCANA
EI	9 REGGIMENTO ASS.PAR. "COL MOSCHIN"	VIA DELL'ARDENZA, 133	LIVORNO	57128	LI	TOSCANA

FA	DENOMINAZIONE ENTE	INDIRIZZO	CITTA	CAP	PROV	REGIONE
EI	REGGIMENTO "SAVOIA CAVALLERIA"	VIA SENESE , 191	GROSSETO	58100	GR	TOSCANA
EI	CENTRO MIL.VETERINARIO	VIA CASTIGLIONESE, 201	GROSSETO	58100	GR	TOSCANA
EI	PARCO MATERIALI ARTIGLIERIA (GR)	VIA SENESE, 163	GROSSETO	58100	GR	TOSCANA
EI	COMANDO MILITARE ESERCITO MARCHE	VIA DEI TORRIONI, 10	ANCONA	60122	AN	MARCHE
EI	28 REGGIMENTO "PAVIA"	VIA DELLA LIBERAZIONE, 7	PESARO	61121	PU	MARCHE
EI	235 RAV. PICENO	VIA XII SETTEMBRE, 2	ASCOLI PICENO	63100	AP	MARCHE
EI	SEZIONE STACCATA AUT.(PE)/COMANDO INFR.CE	PIAZZA UNIONE, 24	PESCARA	65127	PE	ABRUZZO
EI	CENTRO DOCUMENTALE CHIETI	PIAZZA GARIBALDI,16	CHIETI	66100	CH	ABRUZZO
EI	9 REGGIMENTO ALPINI	VIA PARROZZANI N. 1	L'AQUILA	67100	AQ	ABRUZZO
EI	33 REGGIMENTO A.TER. "ACQUI"	STATALE 80	L'AQUILA	67100	AQ	ABRUZZO
EI	COMANDO MILITARE ESERCITO ABRUZZO	PIAZZA SAN BERNARDINO / VIA PANFILO TEDESCHI, 6	L'AQUILA	67100	AQ	ABRUZZO
EI	COMANDO MILITARE ESERCITO PUGLIA	PIAZZA LUIGI DI SAVOIA, 4	BARI	70121	BA	PUGLIA
EI	CENTRO DOCUMENTALE BARI	PIAZZA BALENZANO, SNC / PIAZZA LUIGI DI SAVOIA, 4	BARI	70121	BA	PUGLIA
EI	REPARTO COMANDO E SPT.TAT."PINEROLO"	VIA GIUSEPPE FANELLI, 269	BARI	70125	BA	PUGLIA
EI	COMANDO BRIGATA MECCANIZZATA PINEROLO	VIA GIUSEPPE FANELLI, 269	BARI	70125	BA	PUGLIA
EI	10 REGGIMENTO TRASPORTI	VIA NAPOLI, 328	BARI	70132	BA	PUGLIA
EI	15 REPARTO INFRASTRUTTURE (BA)	VIA NAPOLI, 322 B	BARI	70132	BA	PUGLIA
EI	21 REGGIMENTO A.CAM.SMV. "TRIESTE	VIA DELLE CASERMETTE SNC	FOGGIA	71121	FG	PUGLIA
EI	11 REGGIMENTO G.GUA (FG)	VIA DELLE CASERMETTE SNC	FOGGIA	71121	FG	PUGLIA
EI	SCUOLA CAVALLERIA	VIA MASSAGLIA , 19	LECCE	73100	LE	PUGLIA
EI	CENTRO DOCUMENTALE LECCE	VIA COL COSTADURA, 1	LECCE	73100	LE	PUGLIA
EI	31 REGGIMENTO CARRI	VIA MONTERONI, 148	LECCE	73100	LE	PUGLIA
EI	82 REGGIMENTO FANTERIA "TORINO" (BARLETTA)	VIA ANDRIA, 105	BARLETTA	76121	BT	PUGLIA
EI	9 REGGIMENTO FANTERIA "BARI"	PIAZZALE SANTO ANNIBALE MARIA DI	TRANI	76125	BT	PUGLIA
EI	POLO MANTENIMENTO PESANTE SUD	VIA S. PAOLO BEL SITO, 135	NOLA	80035	NA	CAMPANIA
EI	COMANDO 2 FOD	CORSO SAN GIOVANNI A TEDUCCIO , 1062	SAN GIORGIO A CREMANO	80046	NA	CAMPANIA
EI	REPARTO COMANDO SPT.TAT. ACQUI	CORSO SAN GIOVANNI A TEDUCCIO, 1062	SAN GIORGIO A CREMANO	80046	NA	CAMPANIA
EI	STABILIMENTO BALNEO-TERMALE ELIO.(ISCHIA)	VIA ROMA, 94	ISCHIA	80077	NA	CAMPANIA
EI	NATO - SOUTH RC	VIALE DELLA LIBERAZIONE, 124	BAGNOLI	80124	NA	CAMPANIA
EI	10 REPARTO INFRASTRUTTURE (NA)	VIA PIETRO METASTASIO, 99	NAPOLI	80125	NA	CAMPANIA
EI	SCUOLA MILITARE "NUNZIATELLA"	VIA GENERALE PARISI, 16	NAPOLI	80132	NA	CAMPANIA
EI	COMANDO LOGISTICO SUD	PIAZZA DEL PLEBISCITO, 33	NAPOLI	80132	NA	CAMPANIA
EI	10 CENTRO RIFORNIMENTI MANTENIMENTO	CORSO MALTA, 110	NAPOLI	80141	NA	CAMPANIA
EI	COMANDO INFRASTRUTTURE SUD (NA)	CORSO MALTA, 91	NAPOLI	80141	NA	CAMPANIA
EI	UFFICIO REV.CONT.MAT.DECENTRATA (NA)	VIA COLONNELLO LA HALLE, 55	NAPOLI	80141	NA	CAMPANIA
EI	COMANDO MILITARE ESERCITO CAMPANIA	VIA COLONNELLO LA HALLE, 55	NAPOLI	80141	NA	CAMPANIA
EI	CENTRO DOCUMENTALE NAPOLI	VIA COLONNELLO LA HALLE, 55	NAPOLI	80141	NA	CAMPANIA
EI	CENTRO SELEZIONE VFP-1 NAPOLI	VIA COLONNELLO LA HALLE, 55 / CORSO MALTA,	NAPOLI	80141	NA	CAMPANIA
EI	REPARTO SPT.GEN./COMANDO L.SUD.	CORSO MALTA, 110	NAPOLI	80141	NA	CAMPANIA
EI	CERICO (NA)	VIA MILANO, 189	NAPOLI	80145	NA	CAMPANIA

FA	DENOMINAZIONE ENTE	INDIRIZZO	CITTA	CAP	PROV	REGIONE
EI	SCUOLA AMMINISTRAZIONE E COMMISSARIATO	VIA CAUDINA, 147	MADDALONI	81024	CE	CAMPANIA
EI	47 RAV "FERRARA" (CAPUA)	VIA BREZZA, 8	CAPUA	81043	CE	CAMPANIA
EI	RAGGRUPPAMENTO UNITA ADD.(RUA)	VIA BREZZA	CAPUA	81043	CE	CAMPANIA
EI	17 RAV. ACQUI (CAPUA)	VIA BREZZA	CAPUA	81043	CE	CAMPANIA
EI	COMANDO ORGANIZZAZIONE PENITENZIARIA MILITARE	VIA DEL LAVORO, 202	SANTA MARIA CAPUA VETERE	81055	CE	CAMPANIA
EI	REPARTO COMANDO E SPT.TAT."GARIBALDI"	VIA LAVIANO, 4	CASERTA	81100	CE	CAMPANIA
EI	8 REGGIMENTO BERSAGLIERI	VIA LAVIANO, 8	CASERTA	81100	CE	CAMPANIA
EI	COMANDO B.BERS. GARIBALDI	VIA LAVIANO, 4	CASERTA	81100	CE	CAMPANIA
EI	21 REGGIMENTO GENIO GUASTATORI	VIA ELEUTERIO RUGGIERO, 49	CASERTA	81100	CE	CAMPANIA
EI	DIPARTIMENTO MILITARE DI MEDICINA LEGALE TIPO B (CE)	VIA TORRINO, 1	CASERTA	81100	CE	CAMPANIA
EI	CENTRO DOCUMENTALE CASERTA	VIA DOHUET, 1	CASERTA	81100	CE	CAMPANIA
EI	232 REGGIMENTO TRASMISSIONI	VIALE ITALIA	AVELLINO	83100	AV	CAMPANIA
EI	BATTAGLIONE T."VULTURE"	VIALE SAN FRANCESCO, 1	NOCERA INFERIORE	84014	SA	CAMPANIA
EI	10 REGGIMENTO DI MANOVRA	VIA BORGO S.LAZZARO - SERRE PERSANO SELE	PERSANO	84023	SA	CAMPANIA
EI	8 REGGIMENTO ART. "PASUBIO"	VIA BORGO S.LAZZARO	PERSANO	84023	SA	CAMPANIA
EI	4 REGGIMENTO CARRI (EX 131 RGT CARRI)	VIALE GIOACCHINO MURAT, SNC	PERSANO	84023	SA	CAMPANIA
EI	COMANDO COMPRENSORIO PERSANO	VIA BORGO SAN LAZZARO	PERSANO	84023	SA	CAMPANIA
EI	CENTRO DOCUMENTALE SALERNO	VIA POSIDONIA, 98	SALERNO	84128	SA	CAMPANIA
EI	REGGIMENTO "CVG.GUIDE" (19)	VIA PIETRO DEL PEZZO, 79	SALERNO	84133	SA	CAMPANIA
EI	COMANDO MILITARE ESERCITO BASILICATA	VIA CICCOTTI, 32 A	POTENZA	85100	PZ	BASILICATA
EI	COMANDO MILITARE ESERCITO MOLISE	VIA VERDONE, 1	CAMPOBASSO	86100	CB	MOLISE
EI	1 REGGIMENTO BERSAGLIERI	VIA PANEBIANCO, 184	COSENZA	87100	CS	CALABRIA
EI	2 REGGIMENTO AVES "SIRIO"	VIA G. CUGLIETTA C/O AEREOPORTO, 5	LAMEZIA TERME	88046	CZ	CALABRIA
EI	COMANDO MILITARE ESERCITO CALABRIA	VIA L. PASCALI, 40	CATANZARO	88100	CZ	CALABRIA
EI	46 REGGIMENTO TRASMISSIONI	PIAZZA GENERALE TURBA, 200	PALERMO	90129	PA	SICILIA
EI	11 REPARTO INFRASTRUTTURE (PA)	VIA EMANUELA LOI, 6	PALERMO	90129	PA	SICILIA
EI	CENTRO DOCUMENTALE PALERMO	PIAZZA INDIPENDENZA, 7	PALERMO	90129	PA	SICILIA
EI	4 REGGIMENTO GENIO GUASTATORI	CORSO CALATAFIMI 1000/A	PALERMO	90131	PA	SICILIA
EI	COMANDO REGIONE MILITARE SUD	PIAZZA DELLA VITTORIA, 14	PALERMO	90134	PA	SICILIA
EI	SEZIONE RIFORNIMENTI E MANTENIMENTO (PA)	VIA GENERALE CANTORE, 35/A	PALERMO	90141	PA	SICILIA
EI	REGGIMENTO C.LINEA PE."LANC.DI AOSTA"(6)	VIA ISAAC RABIN, 47	PALERMO	90142	PA	SICILIA
EI	SERICO (PA)	VIA ALBERT AHRENS SNC	PALERMO	90146	PA	SICILIA
EI	6 REGGIMENTO BERSAGLIERI	CORSO PIERSANTI MATTARELLA, 127	TRAPANI	91100	TP	SICILIA
EI	62 REGGIMENTO FANTERIA "SICILIA"	VIA VAL DI SAVOIA, 1	CATANIA	95123	CT	SICILIA
EI	CENTRO DOCUMENTALE CATANIA	VIA GUGLIELMO OBERDAN, 33	CATANIA	95131	CT	SICILIA
EI	24 REGGIMENTO A.TER.(SMV)"PELORITANI"	VIA TAORMINA , 63	MESSINA	98050	ME	SICILIA
EI	REPARTO COMANDO E SPT.TAT."AOSTA"	VIA COMUNALE VISCONTE	MESSINA	98100	ME	SICILIA
EI	COMANDO B.MEC."AOSTA"	VIA DEL VESPRO, 74 - ISOLATO N 285	MESSINA	98122	ME	SICILIA
EI	5 REGGIMENTO FANTERIA "AOSTA"	VIALE EUROPA, 150	MESSINA	98123	ME	SICILIA
EI	ITALSTAFF-RAP.MIL.IT.C/O NATO	BOULEVARD (BRUXELLES)	BRUXELLES	---	--	BELGIO

FA	DENOMINAZIONE ENTE	INDIRIZZO	CITTA	CAP	PROV	REGIONE
EI	REPARTO SPT.L. - POL. MONTEROMANO	VIA DELLA MADONNELLA, 25	MONTEROMANO	O1010	VT	LAZIO
EI	SCUOLA SOTTUFFICIALI EI	STRADA CIMINA, 4	VITERBO	O1100	VT	LAZIO
EI	COMANDO AVES	PIAZZA SAN FRANCESCO, 5	VITERBO	O1100	VT	LAZIO
EI	1 REGGIMENTO AVES"ANTARES"	VIA TUSCANESE, 14	VITERBO	O1100	VT	LAZIO
EI	4 REGGIMENTO SOSTEGNO AVES "SCORPIONE"	STRADA TUSCANESE , 71 R	VITERBO	O1100	VT	LAZIO
EI	CENTRO ADDESTRATIVO AVIAZIONE DELL'ESERCITO	STRADA TUSCANESE, 14	VITERBO	O1100	VT	LAZIO
EI	SCUOLA INTERFORZE DI NBC	VIALE DEI FLAVI, 4	RIETI	O2100	RI	LAZIO
EI	41 REGGIMENTO "CORDENONS"	VIA DIVISIONE "ACQUI", N. 1	SORA	O3039	FR	LAZIO
EI	80 RAV. "ROMA"	VIA VAGLIE, SNC	CASSINO	O3043	FR	LAZIO
EI	17 REGGIMENTO A.C/A "SFORZESCA"SABAUDIA	VIA CAPORALE ARMANDO TORTINI, 9	SABAUDIA	O4016	LT	LAZIO
EI	REPARTO COMANDO /COMANDO A.C/A	VIA CAPORALE ARMANDO TORTINI, 9	SABAUDIA	O4016	LT	LAZIO
EI	STABILIMENTO GRAFICO MILITARE	VIA L. MUNANZIO PLANCO	GAETA	O4024	LT	LAZIO
EI	POLO MANTENIMENTO ARMI LEGGERE	VIALE BENEDETTO BRIN, 149	TERNI	O5100	TR	UMBRIA
EI	CENTRO SEL.RECL.NAZ.ESERCITO (CSRNE)	VIA MEZZETTI, 2	FOLIGNO	O6034	PG	UMBRIA
EI	SCUOLA LINGUE ESTERE EI	VIA BALDASSARRE ORSINI, 3	PERUGIA	O6121	PG	UMBRIA
EI	COMANDO MILITARE ESERCITO UMBRIA	VIA LUPATELLI, 1	PERUGIA	O6123	PG	UMBRIA
EI	CENTRO DOCUMENTALE PERUGIA	VIA LUPATELLI, 1	PERUGIA	O6123	PG	UMBRIA
EI	COMANDO B.MEC."SASSARI"	PIAZZA CASTELLO , 9	SASSARI	O7100	SS	SARDEGNA
EI	152 REGGIMENTO MEC."SASSARI"	VIA CARLO FELICE, 7	SASSARI	O7100	SS	SARDEGNA
EI	REPARTO COMANDO E SPT.TAT."SASSARI"	PIAZZA CASTELLO, 9	SASSARI	O7100	SS	SARDEGNA
EI	5 REGGIMENTO GENIO GUASTATORI (MACOMER)	VIALE GRAMSCI SNC	MACOMER	O8015	NU	SARDEGNA
EI	BASE LOGISTICA ADD. (NU)	VIA SARDEGNA, 3	NUORO	O8100	NU	SARDEGNA
EI	1 REGGIMENTO CORAZZATO	LOCALITA' SA PORTEDDA SNC	TEULADA	O9019	CA	SARDEGNA
EI	21 GRUPPO SQUADRONI AVES "ORSA MAGGIORE"	VIA DEI TRASVOLATORI SNC	ELMAS	O9030	CA	SARDEGNA
EI	COMANDO MILITARE AUTONOMO DELLA SARDEGNA	VIA TORINO, 21	CAGLIARI	O9047	CA	SARDEGNA
EI	DIPARTIMENTO MILITARE DI MEDICINA LEGALE TIPO A (CA)	VIA OSPEDALE, 2	CAGLIARI	O9124	CA	SARDEGNA
EI	151 REGGIMENTO MEC."SASSARI"	VIALE DEL POETTO, 17	CAGLIARI	O9126	CA	SARDEGNA
EI	BATTAGLIONE T."GENNARGENTU"	VIALE DEL POETTO, 21	CAGLIARI	O9126	CA	SARDEGNA
EI	SERICO (CA)	VIA DEL POETTO, 21	CAGLIARI	O9126	CA	SARDEGNA
EI	SEZIONE RIFORNIMENTI E MANTENIMENTO (CA)	VIALE SAN BARTOLOMEO, 14/16	CAGLIARI	O9126	CA	SARDEGNA
EI	14 REPARTO INFRASTRUTTURE (CA)	VIALE DEL POETTO, 21	CAGLIARI	O9126	CA	SARDEGNA
EI	CENTRO DOCUMENTALE CAGLIARI	VIALE CALAMOSCA, 29	CAGLIARI	O9126	CA	SARDEGNA
EI	CENTRO AMM.E.I.	VIA SFORZA, 17	ROMA	OO100	RM	LAZIO
EI	BANDA ESERCITO	CECCHIGNOLA - VIA GIORGIO PELOSI, 22	ROMA	OO143	RM	LAZIO
EI	6 REGGIMENTO GENIO PIONIERI	CECCHIGNOLA - VIA GIOVANNI LUCENTE, 1	ROMA	OO143	RM	LAZIO
EI	3 REGGIMENTO TRASMISSIONI	CECCHIGNOLA - VIA DEI GENIERI, 287	ROMA	OO143	RM	LAZIO
EI	CERICO (RM)	VIA G. PELOSI, 81	ROMA	OO143	RM	LAZIO
EI	8 REGGIMENTO TRASPORTI "CASILINA"	CECCHIGNOLA, VIA DELLA CHIESA DEL PRESIDIO, 140	ROMA	OO143	RM	LAZIO
EI	SCUOLA SANITA/VETERINARIA MILITARE	CECCHIGNOLA - VIA GIORGIO PELOSI, 41	ROMA	OO143	RM	LAZIO
EI	44 REGGIMENTO SOSTEGNO TLC. "PENNE"	CECCHIGNOLA – VIA VINCENZO PANDOLFO, 125	ROMA	OO143	RM	LAZIO

FA	DENOMINAZIONE ENTE	INDIRIZZO	CITTA	CAP	PROV	REGIONE
EI	REGGIMENTO SPT. CECCHIGNOLA	CECCHIGNOLA – VIALE DELL'ESERCITO, 85	ROMA	OO143	RM	LAZIO
EI	DIPARTIMENTO MILITARE DI MEDICINA LEGALE TIPO A (RM)	CECCHIGNOLA - VIA DEI BERSAGLIERI, 10	ROMA	OO143	RM	LAZIO
EI	REPARTO OPERATIVO DEL GENIO INFRASTRUTTURALE	CECCHIGNOLA - VIALE DELL'ESERCITO, 123 / VIA	ROMA	OO143	RM	LAZIO
EI	SCUOLA DELLE TRASMISSIONI E INFORMATICA	CECCHIGNOLA - VIA DEI GENIERI, 287	ROMA	OO143	RM	LAZIO
EI	DIREZIONE GENERALE DELLE PENSIONI MILITARI DEL COLLOCAMENTO LAVORO VOL.	CECCHIGNOLA - VIALE DELL'ESERCITO, 186	ROMA	OO143	RM	LAZIO
EI	CENTRO SPORTIVO OLIMPICO DELL ESERCITO	CECCHIGNOLA - VIA DEGLI ARDITI, 1	ROMA	OO143	RM	LAZIO
EI	COMANDO GENIO	CECCHIGNOLA - VIALE DELL'ESERCITO, 123 / VIA	ROMA	OO143	RM	LAZIO
EI	COMANDO PER LA FORMAZIONE SPECIALIZZAZIONE E DOTTRINA DELL	CECCHIGNOLA - VIALE DELL'ESERCITO, 170	ROMA	OO143	RM	LAZIO
EI	SCUOLA DEI TRASPORTI E MATERIALI	CECCHIGNOLA - VIALE DELL'ESERCITO, 102	ROMA	OO143	RM	LAZIO
EI	CROCE ROSSA ITALIANA	VIA LUIGI PIERANTONI, 5	ROMA	OO146	RM	LAZIO
EI	SMD-CENTRO INTELLIGENCE INTERFORZE	VIA MONTE CARNEVALE, 381	ROMA	OO148	RM	LAZIO
EI	PARCO MATERIALI TLC (RM)	VIA DEL TRULLO, 533	ROMA	OO148	RM	LAZIO
EI	8 CENTRO RIFORNIMENTI MANTENIMENTO	VIA PRENESTINA, 931	ROMA	OO155	RM	LAZIO
EI	COMANDO B.MEC."GRAN.DI SARDEGNA"	VIA DEL FORTE DI PIETRALATA, 7	ROMA	OO158	RM	LAZIO
EI	1 REGGIMENTO "GRANATIERI DI SARDEGNA"	VIA FORTE DI PIETRALATA, 7	ROMA	OO158	RM	LAZIO
EI	REPARTO COMANDO E SPT.TAT."GRA.DI SARD."	VIA TIBURTINA, 780	ROMA	OO159	RM	LAZIO
EI	COMANDO RAGGRUPPAMENTO LOGISTICO CENTRALE	VIALE CASTRO PRETORIO,123	ROMA	OO161	RM	LAZIO
EI	STATO MAGGIORE/ COMANDO LOG.E.	VIA NOMENTANA, 274	ROMA	OO162	RM	LAZIO
EI	DIPARTIMENTO TRASPORTI E MATERIALI/COMANDO LOG.E.	VIA NOMENTANA, 274	ROMA	OO162	RM	LAZIO
EI	RAGGRUPPAMENTO UN.DI.(RUD)	VIA PINETA SACCHETTI, 216	ROMA	OO168	RM	LAZIO
EI	11 BATTAGLIONE TRASPORTI "FLAMINIA"	VIA CASILINA, 1014	ROMA	OO169	RM	LAZIO
EI	8 REPARTO INFRASTRUTTURE (RM)	VIA TODI, 6	ROMA	OO181	RM	LAZIO
EI	POLICLINICO MILITARE (RM)	PIAZZA CELIMONTANA, 50	ROMA	OO184	RM	LAZIO
EI	COMANDO RAGGRUPAMENTO AUTOMO MD	PALAZZO ESERCITO - VIA NAPOLI, 41	ROMA	OO184	RM	LAZIO
EI	SME-III RIF-COE-UFFICIO SICUREZZA (SOLO EPASSPORT)	VIA XX SETTEMBRE, 123A	ROMA	OO184	RM	LAZIO
EI	UFFICIO AMM.PERS.MIL.VARI	VIA MARSALA, 104	ROMA	OO185	RM	LAZIO
EI	REGGIMENTO C.LINEA PE."LANC.MONTEB."(8)	VIA FLAMINIA VECCHIA, 826	ROMA	OO191	RM	LAZIO
EI	CENTRO DOCUMENTALE ROMA	VIA CARLO ALBERTO DALLA CHIESA, 2	ROMA	OO192	RM	LAZIO
EI	CENTRO SELEZIONE VFP-1 ROMA	VIA CARLO ALBERTO DALLA CHIESA, 2	ROMA	OO192	RM	LAZIO
EI	POLO MANTENIMENTO MZ.TLC ELT.E OPTOE.	VIALE ANGELICO, 19	ROMA	OO195	RM	LAZIO
EI	CENTRO SISTEMI INFORMATICI ESERCITO	VIA GUIDO RENI, 22	ROMA	OO196	RM	LAZIO
EI	ISPETTORATO INFRASTRUTTURE EI	VIA SCIPIO SLATAPER, 2	ROMA	OO197	RM	LAZIO
EI	COMANDO MILITARE DELLA CAPITALE	VIA SCIPIO SLATAPER, 2	ROMA	OO197	RM	LAZIO
EI	CENTRO MILITARE DI EQUITAZIONE	VIA MONTELIBRETTESE KM 1	MONTELIBRETTI	OOO10	RM	LAZIO
EI	DIPARTIMENTO LUNGODEGENZA(ANZIO)	VIA ROMA, 15	ANZIO	OOO42	RM	LAZIO
EI	COMANDO TRASM. E INFORMAZIONI ESERCITO (CO.TIE)	VIA ARDEATINA , 16	ANZIO	OOO42	RM	LAZIO
EI	11 REGGIMENTO TRASMISSIONI	S.S. AURELIA NORD KM 78,500	CIVITAVECCHIA	OOO53	RM	LAZIO
EI	7 REGGIMENTO DIFESA NBC "CREMONA"	LARGO ACQUARONI, 24	CIVITAVECCHIA	OOO53	RM	LAZIO
EI	CENTRO TEC.LOG.NBC	VIA BRACCIANESE CLAUDIA S.N.C.	CIVITAVECCHIA	OOO53	RM	LAZIO
EI	CENTRO SIMULAZIONE E VALIDAZIONE ESERCITO	VIA LEOPOLI, 36	CIVITAVECCHIA	OOO53	RM	LAZIO

FA	DENOMINAZIONE ENTE	INDIRIZZO	CITTA	CAP	PROV	REGIONE
EI	SCUOLA DI FANTERIA	VIA DELLA STAZIONE DI CESANO	CESANO	OOO60	RM	LAZIO
EI	1 REGGIMENTO SOSTEGNO AVES IDRA	VIA DEL SASSO, 2A	BRACCIANO	OOO62	RM	LAZIO
EI	COMANDO ARTIGLIERIA	VIA BRACCIANESE CLAUDIA, S.N.C.	BRACCIANO	OOO62	RM	LAZIO
EI	CENTRO POLIFUNZIONALE SPERIMENTAZIONE	VIA MONTELIBRETTESE KM. 2,5	MONTELIBRETTI	OOOO10	RM	LAZIO
MM	DIREZIONE MARITTIMA GENOVA		GENOVA	16100	GE	LIGURIA
MM	MARIDROGRAFICO GENOVA		GENOVA	16100	GE	LIGURIA
MM	COMANDO MARITTIMO NORD		LA SPEZIA	19100	SP	LIGURIA
MM	DIREZIONE MARITTIMA VENEZIA		VENEZIA	30100	VE	VENETO
MM	MARISCUOLANAV		VENEZIA	30100	VE	VENETO
MM	DIREZIONE MARITTIMA TRIESTE		TRIESTE	34100	TS	FRIULI
MM	CAPITANERIA DI PORTO SEDE DI DIREZIONE MARITTIMA - RAVENNA		RAVENNA	48120	RA	EMILIA ROMAGNA
MM	DIREZIONE MARITTIMA LIVORNO		LIVORNO	57100	LI	TOSCANA
MM	MARINACCAD LIVORNO		LIVORNO	57100	LI	TOSCANA
MM	DIREZIONE MARITTIMA ANCONA		ANCONA	60100	AN	MARCHE
MM	QGM ANCONA QUARTIER GENERALE MARINA ANCONA		ANCONA	60100	AN	MARCHE
MM	CAPITANERIA DI PORTO SEDE DI DIREZIONE MARITTIMA - PESCARA		PESCARA	65120	PE	ABRUZZO
MM	DIREZIONE MARITTIMA BARI		BARI	70100	BA	PUGLIA
MM	CAPITANERIA DI PORTO BRINDISI		BRINDISI	72100	BR	PUGLIA
MM	COMANDO MARITTIMO SUD		TARANTO	74120	TA	PUGLIA
MM	DIREZIONE SELEZIONE VOLONTARI A FERMA PREFISSATA (MARIDIRSELEZ TA)		TARANTO	74120	TA	PUGLIA
MM	MARISCUOLA TARANTO		TARANTO	74120	TA	PUGLIA
MM	DIREZIONE MARITTIMA NAPOLI		NAPOLI	80100	NA	CAMPANIA
MM	MARITELE NAPOLI		NAPOLI	80100	NA	CAMPANIA
MM	QUARTIER GENERALE MARINA NAPOLI (QGM NA)		NAPOLI	80100	NA	CAMPANIA
MM	DIREZIONE MARITTIMA REGGIO CALABRIA		REGGIO CALABRIA	89100	RC	CALABRIA
MM	DIREZIONE MARITTIMA PALERMO		PALERMO	90100	PA	SICILIA
MM	DIREZIONE MARITTIMA CATANIA		CATANIA	95100	CT	SICILIA
MM	MARISICILIA		AUGUSTA	96011	SR	SICILIA
MM	CAPITANERIA DI PORTO MESSINA		MESSINA	98100	ME	SICILIA
MM	MARISCUOLA LA MADDALENA		LA MADDALENA	O7024	OT	SARDEGNA
MM	CAPITANERIA DI PORTO SEDE DI DIREZIONE MARITTIMA - OLBIA		OLBIA	O7026	OT	SARDEGNA
MM	COMANDO SUPPORTO LOGISTICO (MARISUPLOG CA)		CAGLIARI	O9100	CA	SARDEGNA
MM	DIREZIONE MARITTIMA CAGLIARI		CAGLIARI	O9100	CA	SARDEGNA
MM	COMANDO MILITARE MARITTIMO AUTONOMO DELLA CAPITALE		ROMA	OO100	RM	LAZIO
MM	QUARTIER GENERALE MARINA ROMA S.ROSA	VIA DELLA STORTA, 601	ROMA	OO123	RM	LAZIO
MM	ISP GENERALE DELLE CAPITANERIE DI PORTO	VIA DELL'ARCHITETTURA	ROMA	OO141	RM	LAZIO
MM	MARITELE ROMA	PIAZZALE DELLA MARINA, 1	ROMA	OO196	RM	LAZIO
MM	DIREZIONE MARITTIMA CIVITAVECCHIA		CIVITAVECCHIA	OOO53	RM	LAZIO
SGD	UFFICIO TECNICO TERRITORIALE	VIA BRIONE, 1	TORINO	10143	TO	PIEMONTE
SGD	STABILIMENTO GENIO MILITARE	VIA RIVIERA, 42	PAVIA	27100	PV	LOMBARDIA

FA	DENOMINAZIONE ENTE	INDIRIZZO	CITTA	CAP	PROV	REGIONE
SGD	TRIBUNALE MILITARE (VR)	STRADONE PORTA PALIO, 22	VERONA	37122	VR	VENETO
SGD	STABILIMENTO MILITARE RIP.REC.MU.	VIA BORGHETTO 3	NOCETO DI PARMA	43015	PR	EMILIA ROMAGNA
SGD	STABILIMENTO CHM.FARMAC.MIL.	VIA REGINALDO GIULIANI, 201	FIRENZE	50141	FI	TOSCANA
SGD	UFFICIO TECNICO TERRITORIALE COM. (FI)	VIA REGINALDO GIULIANI, 208	FIRENZE	50141	FI	TOSCANA
SGD	MARICORDERIA - CASTELLAMMARE	VIA ACTON 12	CASTELLAMMARE DI STABIA	80053	NA	CAMPANIA
SGD	TRIBUNALE MILITARE (NA)	PIAZZA S. MARIA DEGLI ANGELI, 2	NAPOLI	80132	NA	CAMPANIA
SGD	STABILIMENTO MILITARE PIROTECNICO	VIA GRAN QUARTIERE, 4	CAPUA	81043	CE	CAMPANIA
SGD	STABILIMENTO MILITARE PROPELLENTI	CORSO TRIESTE, 2	FONTANA LIRI	O3035	FR	LAZIO
SGD	STABILIMENTO MILITARE MUNIZIONAMENTO TERRESTRE	VIA ACQUASPARTA 10	BAIANO DI SPOLETO	O6040	PG	UMBRIA
SGD	CONSIGLIO MAGISTRATURA MILITARE		ROMA	OO100	RM	LAZIO
SGD	DIREZIONE GENERALE PERSONALE CIVILE		ROMA	OO100	RM	LAZIO
SGD	GABINETTO MINISTRO DIFESA		ROMA	OO100	RM	LAZIO
SGD	MD-SEGRETARIATO GENERALE DIFESA-UFF.SEGRETARIO GENERALE DIF./DNA		ROMA	OO100	RM	LAZIO
SGD	UFFICIO CENTRALE ISPEZIONI AMMINISTRATIVE		ROMA	OO100	RM	LAZIO
SGD	DIREZIONE GENERALE PERSONALE MILITARE	CECCHIGNOLA - VIALE DELL'ESERCITO, 186	ROMA	OO143	RM	LAZIO
SGD	CENTRO ALTI STUDI PER LA DIFESA	PIAZZA DELLA ROVERE, 83	ROMA	OO165	RM	LAZIO
SGD	CENTRO OPV.INTERF./COMANDO OPV.INTERF.	VIA DELL'AEROPORTO DI CENTOCELLE, 301	ROMA	OO175	RM	LAZIO
SGD	DIREZIONE GENERALE SANITA MILITARE	VIA DI SANTO STEFANO ROTONDO, 4	ROMA	OO184	RM	LAZIO
SGD	UFFICIO CENTRALE DEL BILANCIO E DEGLI AFFARI FINANZIARI	VIA XX SETTEMBRE	ROMA	OO184	RM	LAZIO
SGD	DIREZIONE DEGLI ARMAMENTI AERONAUTICI	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
SGD	DIREZIONE GENERALE ARMAMENTI TERRESTRI	VIA MARSALA, 104	ROMA	OO185	RM	LAZIO
SGD	DIREZIONE GENERALE TELECOMUNICAZIONI INFT.E TEC.AVANZATE	VIALE DELL'UNIVERSITÀ, 4	ROMA	OO185	RM	LAZIO
SGD	DIREZIONE GENERALE ARMAMENTI NAVALI	PIAZZA DELLA MARINA, 4	ROMA	OO196	RM	LAZIO
SGD	DIREZIONE GENERALE DEI SERVIZI GENERALI	PIAZZA DELLA MARINA, 4	ROMA	OO196	RM	LAZIO
SGD	GENIODIFE - SEGR.	PIAZZA DELLA MARINA, 4	ROMA	OO196	RM	LAZIO
SGD	UFFICIO TECNICO TERRITORIALE ARM. TERRESTRI		NETTUNO	OOO48	RM	LAZIO

Pagina intenzionalmente bianca

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	**<u>Per sospensione</u>:** **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** **<u>Per Revoca</u>:** **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)	**<u>Per sospensione</u>:** ▪ Entro **10 minuti** per un totale **TRS >= 98%**; ▪ Entro **30 minuti** per il residuo **TRS <= 2%** **<u>Per revoca</u>:** ▪ 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%**

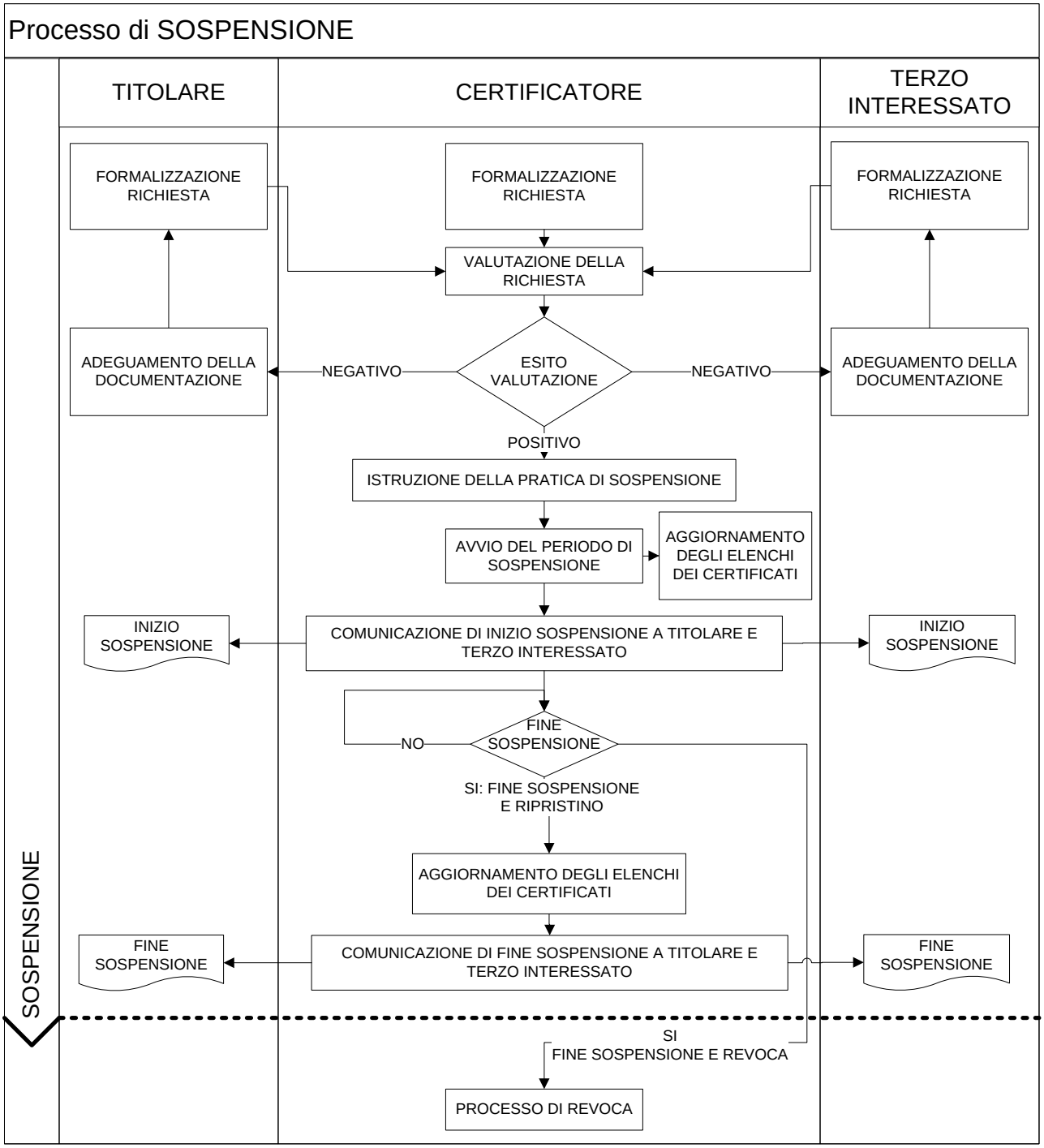
SEGUE ALLEGATO G

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