



Federazione Lavoratori Pubblici e Funzioni Pubbliche

FLP DIFESA

Coordinamento Nazionale



✉ piazza Dante, 12 - 00185- ROMA - ☎ 06-77201726 ☎ 06-77201728 - @-mail: nazionale@flpdifesa.it - web: www.flpdifesa.it

NOTIZIARIO n. 071 del 22.05.2009

EMANATA DALLO STATO MAGGIORE DIFESA A SEGUITO DELL'INCONTRO CON LE OO.SS. DEL 1.12.2008

DIRETTIVA SMD SULLA C.M.D. (CARTA MULTISERVIZI DIFESA)

Come si ricorderà, nel corso della riunione del 1 dicembre 2008 con il Sottosegretario delegato on. Giuseppe Cossiga, originata da una specifica richiesta delle OO.SS. e relativa alle diverse problematiche segnalate dalle strutture territoriali in merito alla "Carta Mutiservizi Difesa" (CMD), l'Amministrazione, su nostra precisa sollecitazione, ci aveva assicurato che lo Stato Maggiore Difesa avrebbe emanato "una circolare destinata a tutti gli Enti con la quale si preciserà la non obbligatorietà per il personale civile di fornire dati sensibili (religione; etc.)", come abbiamo a suo tempo comunicato nel nostro Notiziario n. 156 di pari data.

In relazione a quanto sopra, e dando seguito alle tante richieste che ci sono pervenute nel corso di questi mesi da molte nostre strutture sindacali, confermiamo che l'Amministrazione, seppur con molto ritardo, ha ottemperato all'impegno assunto con le OO.SS. e ha emanato la Direttiva SMD n. 2/46 del 9 marzo 2009, che vi trasmettiamo in allegato al presente Notiziario, con la quale lo Stato Maggiore Difesa fornisce dettagliate informazioni sulla CMD e sul suo utilizzo.

In particolare, per quanto riguarda i dati sensibili che molti Enti avevano richiesto anche ai dipendenti civili sulla scorta di quanto avviene per il personale militare, cosa che aveva peraltro indotto il Sindacato a porre il problema al Gabinetto e a richiedere una specifica riunione, la **Direttiva SMD** chiarisce una volta per tutte che "per il personale civile non è prevista l'obbligatorietà di fornire dati sensibili quali:

- il campo "RELIGIONE";
- il gruppo sanguigno
- il template delle impronte digitali "

Si prega di dare al presente Notiziario la massima diffusione tra i lavoratori.

Fraterni saluti.

IL COORDINATORE GENERALE
(Giancarlo PITTELLI)



STATO MAGGIORE DELLA DIFESA

Prot. n. 2/46
All.: 1; Ann.: //

00147 Roma, 03 - 03 - 200

POC Col Fattorini tel 24048
sesto.5ul@cmd.difesa.it

OGGETTO: Carta Multiservizi Difesa (CMD).

A **GABINETTO DEL MINISTRO DELLA DIFESA**

ROMA

e, per conoscenza,

SOTTOSEGRETARIO DI STATO ALLA DIFESA

On.le Giuseppe COSSIGA

STATO MAGGIORE DELL'ESERCITO

STATO MAGGIORE DELLA MARINA

STATO MAGGIORE DELL'AERONAUTICA

SECRETARIATO GENERALE DELLA DIFESA DNA

STATO MAGGIORE DELLA MARINA		I RIVOLTO PERSONALE		ARCHIMEDE		POSTA IN ASSERVO	
STGH	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>	1	<input type="checkbox"/>
Arch	<input type="checkbox"/>	2	<input type="checkbox"/>	2	<input type="checkbox"/>	2	<input type="checkbox"/>
P.C.H.	<input type="checkbox"/>	3	<input type="checkbox"/>	3	<input type="checkbox"/>	3	<input type="checkbox"/>
1. UH	<input type="checkbox"/>	4	<input type="checkbox"/>	4	<input type="checkbox"/>	4	<input type="checkbox"/>
2. UH	<input type="checkbox"/>	5	<input type="checkbox"/>	5	<input type="checkbox"/>	5	<input type="checkbox"/>
3. UH	<input type="checkbox"/>	6	<input type="checkbox"/>	6	<input type="checkbox"/>	6	<input type="checkbox"/>
4. UH	<input type="checkbox"/>	7	<input type="checkbox"/>	7	<input type="checkbox"/>	7	<input type="checkbox"/>
5. UH	<input type="checkbox"/>	8	<input type="checkbox"/>	8	<input type="checkbox"/>	8	<input type="checkbox"/>
6. UH	<input type="checkbox"/>	9	<input type="checkbox"/>	9	<input type="checkbox"/>	9	<input type="checkbox"/>
7. UH	<input type="checkbox"/>	10	<input type="checkbox"/>	10	<input type="checkbox"/>	10	<input type="checkbox"/>

25 MAR 2009

4534

Di/25.3

25/3

non c'

^^^^^^^^^^

Rife. f. prot. n APC/55078/11-12-5 in data 23 dicembre 2008 (non a tutti).

^^^^^^^^^^

1. In ordine alle problematiche sulla Carta Multiservizi Difesa (CMD), alla rilevazione automatica delle presenze affrontate nella riunione del 1.12.2008, nonché a quanto chiesto con la lettera in riferimento, si allega una scheda che riporta dettagliate informazioni sulla CMD e sul suo utilizzo. In particolare, si evidenzia quanto segue:

- obbligatorietà dati sensibili personale civile: non c'è alcun obbligo (come meglio precisato nella predetta scheda allegata);
- discriminazione di trattamento militari e civili nei sistemi di rilevazione presenze: per lo Stato Maggiore Difesa è stata emanata la direttiva SMD-I-018 "Modalità esecutive per l'impiego dei Sistemi Automatici di rilevazione delle presenze e governo del personale nell'ambito dello Stato Maggiore della Difesa" (diffusa anche agli altri Enti e pubblicata sul sito intranet ARCHIMEDE) nella quale si stabilisce che tutto il personale dell'area SMD (militari e civili) è tenuto ad utilizzare i dispositivi di rilevazione presenze all'uopo predisposti;
- utilizzo della CMD per ingresso in sedi diverse da quelle di appartenenza: l'utilizzo della CMD anche per l'ingresso in sedi diverse da quelle di servizio è una funzionalità prevista ed auspicata, tenuto presente che tale funzionalità è subordinata alla necessaria autorizzazione da parte del responsabile della sicurezza del sedime. All'uopo è stata realizzata una

SMD-24/03/2009-Poc-25215/1REP-PCN

procedura che, a cura del personale addetto al controllo dei varchi, consente di autorizzare in via temporanea o stabilmente l'ingresso dei visitatori tramite la registrazione della CMD sugli apparati di lettura/sblocco tornelli.

2. Si invitano quindi gli SM/SGD in indirizzo ad impartire disposizioni agli Enti dipendenti per informare le locali rappresentanze del personale civile di quanto riportato al precedente paragrafo e di distribuire l'allegata scheda sulla Carta Multiservizi Difesa.

d'ordine
IL SOTTO CAPO DI STATO MAGGIORE
(Gen. C.A. Domenico VILLANI)





CARTA MULTISERVIZI DELLA DIFESA (CMD)



1. PREMESSA

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 notevole impulso alla digitalizzazione della PA, aveva posto come obiettivo strategico l'erogazione on-line dei servizi al cittadino prevedendo l'introduzione della Carta d'Identità Elettronica (CIE), della Carta Nazionale dei Servizi (CNS) e la diffusione della firma digitale stabilendo gli standard e i criteri organizzativi da seguire.

In ambito Difesa, peraltro, la necessità di una carta elettronica era stata avvertita quale esigenza operativa da parte dell'Esercito allorché ebbe l'urgente necessità di fornire alla Commissione Governativa "Mandelli" i dati anagrafici e sanitari del personale impiegato in operazione nei Balcani. Furono pertanto avviate le azioni necessarie per realizzare il software per la gestione delle informazioni di carattere personale e sanitario attraverso l'utilizzo di una "smart card" capace di memorizzare dati.

La Difesa, conseguentemente, allo scopo di dare una corretta e sinergica collocazione alle diverse attività in atto, elaborò un progetto unitario per la realizzazione della Carta Multiservizi della Difesa (CMD).

Per dare validità legale alla CMD quale documento di riconoscimento e valenza internazionale quale carta sanitaria, la Difesa richiese ed ottenne:

- il riconoscimento della CMD come "carta valori" e l'inserimento di essa tra le "carte valori" (denominato Modello ATe) da parte del Dipartimento del Tesoro del Ministero dell'Economia e delle Finanze, secondo le attuali disposizioni legislative;
- la registrazione della carta stessa presso l'Ente Nazionale di Unificazione per le tecniche informatiche (UNINFO) e Registration Authority per l'Italia, con il conseguente rilascio del previsto Issuer Identification Number (IIN).

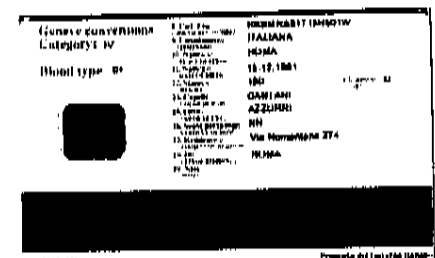
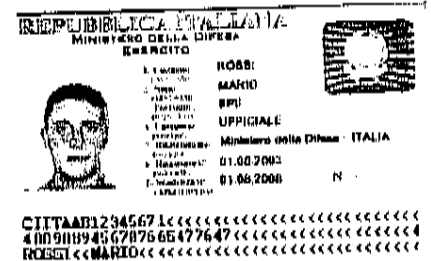
Il progetto della CMD fu molto apprezzato in ambito governativo, tanto che il Comitato dei Ministri per la Società dell'Informazione, nel corso della riunione del 29 luglio 2003, ne ha riconosciuto la validità e ne ha approvato i contenuti.

Infine, la realizzazione e distribuzione a tutti i dipendenti pubblici di carte multiservizi è stata inserita dal Ministro per l'Innovazione e le Tecnologie nella direttiva "Linee guida in materia di digitalizzazione dell'amministrazione per l'anno 2004", fra i settori di intervento prioritari.

2. REQUISITI DI BASE

Nell'elaborazione del progetto della Carta Multiservizi Difesa fu deciso che la stessa dovesse avere una valenza giuridica sia "Esterna" all'Amministrazione Difesa sia "Interna" ad essa. Quindi utilizzabile a "vista" ed in forma elettronica in modo che:

- costituisse "Documento di Riconoscimento" (identità personale). Allo scopo di ampliare il suo utilizzo furono inseriti il codice "International Civil Aviation Organization" (ICAO), a similitudine del passaporto, e le indicazioni per il riconoscimento dei militari prigionieri di guerra
- fosse in grado di contenere i certificati di "Firma Digitale" e "Strong Authentication" pienamente rispondenti alle attuali normative di legge;
- contenesse i dati sanitari del dipendente necessari ad assicurare le funzionalità di "emergency card";



- contenesse le impronte digitali (dita mano destra e sinistra) registrate in forma di template per garantire la "privacy safe" (il template è un codice numerico, memorizzato solo sulla smart card, che non permette di risalire al dato biometrico originale);
 - fosse predisposta per memorizzare altre evidenze biometriche (es. geometria della mano, impronta facciale, iride, ecc.);
 - realizzasse la piena e completa interoperabilità a livello:
 - Nazionale, con la carta d'Identità Elettronica (CIE),
 - Internazionale, con la struttura dati sanitari "NetLink",
 - Interforze ed in ambito Ministero della Difesa;
 - fosse dotata di banda magnetica, idonea a salvaguardare gli investimenti pregressi.
- Inoltre fu parimenti considerato requisito irrinunciabile, ai fini della sicurezza INFOSEC e DATASEC, la certificazione a livello ITSEC "E4-High", relativa al "Chip" ed al Sistema Operativo.

3. PROCEDURE PER IL RILASCIO DELLA CMD

a. ORGANIZZAZIONE

Per l'emissione e la gestione di una CMD il riferimento è la Registration Authority e il Card Management System del dominio - F.A./Persociv - cui appartiene il militare/civile. Le due PKI distinte di cui si avvale la Difesa condividono il Trust Center (o Centro di Certificazione) dove vengono fisicamente emesse e gestite le CMD.

La Registration Authority è un elemento complesso costituito da unità logiche periferiche, le Local Registration Authority (LRA), che, distribuite sul territorio, sovrintendono alle operazioni di raccolta, identificazione, registrazione ed invio dei dati ad un elemento centralizzato (RA), che, dopo gli opportuni controlli di congruità, li rende disponibili per il successivo ciclo produttivo.

Tale organizzazione poggia la propria funzionalità su alcune figure chiave.

(1) **Responsabile per il Trattamento**

Il Responsabile per il Trattamento è la figura dell'Ente Periferico che ha il compito di acquisire i dati personali, amministrativi, militari e biometrici (foto ed impronte digitali) del personale cui deve essere rilasciata la CMD.

È opportuno precisare che per il personale civile non è prevista l'obbligatorietà di fornire dati sensibili quali:

- il campo "RELIGIONE";
- il gruppo sanguigno (che sarà indicato su base volontaria e solo se il dipendente presenta una valida attestazione medica, tesserino AVIS, attestazione rilasciata da un laboratorio analisi o simili);
- Il template delle impronte digitali.

(2) **Responsabile Periferico**

Il Responsabile Periferico è la figura dell'Ente periferico che ha il compito di approvare le richieste di emissione delle CMD certificando con la propria CMD la veridicità e regolarità dei dati acquisiti.

Nomina il Responsabile per il Trattamento e, opzionalmente, può delegare le proprie incombenze di Responsabile Periferico a personale di sua fiducia.

Questa figura si identifica in genere con il Responsabile dell'Ente (Comandante, Direttore, ecc.) che, certificando l'acquisizione dei dati del personale del proprio Ente e degli Enti vicini che fanno riferimento al suo Centro di Registrazione, approva la richiesta di emissione di una CMD.

(3) **Responsabile della certificazione**

Il Responsabile della Certificazione è la figura che nel CMS è responsabile delle procedure per la generazione, la sospensione e la revoca dei certificati.

b. ACQUISIZIONE DEI DATI

La procedura acquisizione dei dati avviene presso i Locali Centri di Registrazione dislocati, ove possibile, presso il Reparto/Ente del richiedente.

Il Responsabile del Trattamento (ufficialmente nominato dal Responsabile Periferico), effettuata l'identificazione del richiedente con un valido documento di riconoscimento, procede all'acquisizione dei dati personali, delle impronte e della foto attraverso specifiche procedure,

convalida i dati con la propria firma digitale e fa firmare all'interessato una copia cartacea dei dati raccolti che poi lui stesso controfirma.

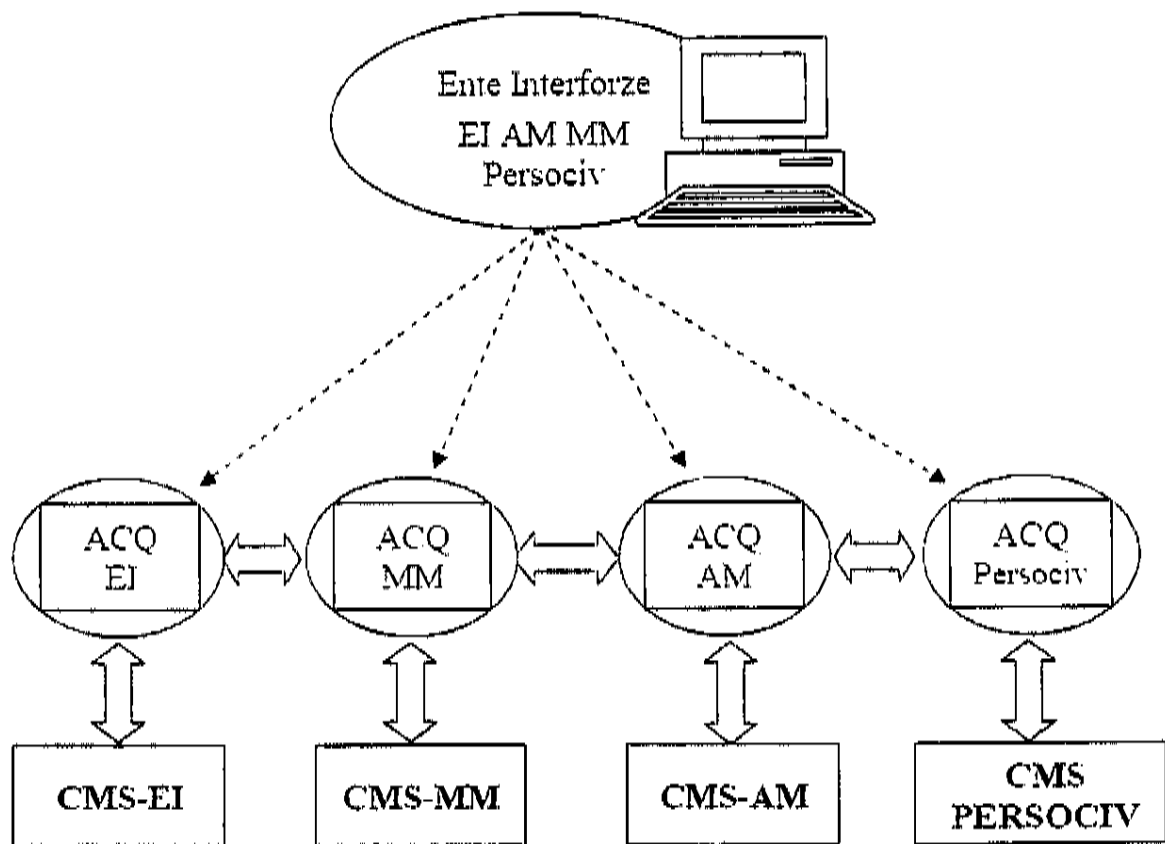
Il Responsabile Periferico (o suo delegato), attraverso una apposita procedura di approvazione, convalida i dati firmandoli con la propria firma digitale e, contestualmente, controfirmando tradizionalmente la copia cartacea.

Successivamente i dati vengono inviati, opportunamente protetti, al CMS di competenza dove vengono verificate le firme digitali apposte dal Responsabile del Trattamento e dal Responsabile Periferico.

c. ACQUISIZIONE DEI DATI IN AMBITO INTERFORZE

L'acquisizione dei dati al livello interforze è garantita dalla interoperabilità tra i CMS delle FF.AA e Persociv realizzata tramite moduli specifici di interscambio.

Di seguito viene mostrato uno schema esemplificativo.



I circuiti di acquisizione di F.A. e Persociv, abbreviati in figura con ACQ, comunicano sia con i relativi CMS che con gli altri circuiti di acquisizione.

Tale capacità di interscambio è strumentale al rilascio della CMD in tutte quelle occasioni in cui il richiedente lavora in un dominio differente dal proprio (altre F.A. o strutture interforze della Difesa). In tale contesto il Responsabile Periferico può convalidare la procedura perché il circuito di acquisizione, con cui è normalmente in collegamento, trasferirà automaticamente la richiesta alla corretta struttura di emissione.

d. ACQUISIZIONE DEI DATI PRESSO ALTRO ENTE

Considerata la varietà e la frammentazione sul territorio di alcuni Enti/Uffici, non in tutti sarà ritenuto conveniente costituire un locale Centro di Registrazione (LRA). Pertanto il personale di questi Enti sarà indirizzato presso specifici Centri vicini che, in base al "concetto di ospitalità", si faranno carico dell'acquisizione e certificazione dei dati indipendentemente dalla categoria e /o FA del richiedente. Potrà essere prerogativa del Centro quella di esigere che il personale

proveniente da altro Ente giunga provvisto di una scheda anagrafico-amministrativa vidimata dal proprio Comando.

e. EMISSIONE E RILASCIO DELLA CMD

La CMD viene pre-stampata presso l'Istituto Poligrafico e Zecca dello Stato e contiene elementi che la rendono non replicabile; in particolare viene impresso con una tecnologia di "laser engraving" l'identificativo progressivo della carta, che contestualmente viene anche memorizzato a bordo del chip in un'area immodificabile. Presso i CMS di F.A./Persociv avviene la seconda fase di personalizzazione con la stampa dei dati.

4. FUNZIONALITÀ DELLA CARTA

La realizzazione della CMD risponde pienamente al D.Lgs. 7 marzo 2005, n. 82 "Codice dell'amministrazione digitale" (Capo V - Dati delle pubbliche amministrazioni e servizi in rete, Sezione IV - Carte elettroniche) che prevede che "Le tessere di riconoscimento rilasciate dalle amministrazioni dello Stato ai sensi del decreto del Presidente della Repubblica 28 luglio 1967, n. 851, possono essere realizzate anche con modalità elettroniche e contenere le funzionalità della carta nazionale dei servizi per consentire l'accesso per via telematica ai servizi erogati in rete dalle pubbliche amministrazioni"

In tale contesto, la Carta Multiservizi Difesa garantisce le seguenti funzionalità essenziali:

a. Identificazione

Le caratteristiche di identificazione sono soddisfatte secondo le seguenti modalità:

- a "vista" tramite i dati riportati sul fronte e sul retro della carta senza l'ausilio di mezzi informatici;
- "elettronica", conforme allo standard previsto per la CIE, attraverso il controllo dei dati anagrafici;
- "in rete", grazie al certificato digitale di autenticazione presente sulla carta, abilitando l'utente all'accesso ed ai servizi su canale sicuro "Secure Socket Layer" (SSL) attraverso un software specifico ("browser"). La funzione deve essere attivata digitando un apposito "Personal Identification Number" (PIN).

b. Firma Digitale

La Carta contiene una struttura di Firma Digitale, la cui esecuzione è possibile tramite l'inserimento di un PIN aggiuntivo, esclusivamente dedicato a tale funzione. Il certificato digitale e la coppia di chiavi di firma digitale sono distinti e indipendenti da quelli usati per l'autenticazione.

La smart card, tramite la quale viene apposta la firma digitale, espleta più funzioni, tra cui la custodia e protezione della chiave privata necessaria per apporre la firma digitale con valore legale e per eseguire i calcoli crittografici connessi con questa operazione. In aggiunta è prevista un'ulteriore coppia di chiavi da utilizzare per cifrare documenti prima di spedirli in formato elettronico.

La smart card utilizzata per la firma digitale soddisfa una serie di caratteristiche di sicurezza tra le quali vi è la capacità di resistere, qualora cada in mani estranee, ai tentativi di estrarre da essa le chiavi private custodite.

In ordine alla Firma digitale la Difesa dal 21/09/2006 è iscritta nell'elenco pubblico dei Certificatori accreditati presso il Centro Nazionale per l'Informatica nella Pubblica Amministrazione (i certificatori sono soggetti pubblici o privati che hanno richiesto ed ottenuto il riconoscimento del possesso dei requisiti per fornire i servizi di certificazione inerenti la firma digitale ed emettono certificati qualificati conformi alla Direttiva europea 1999/93/CE e nazionale in materia).

c. Dati Sanitari

La Carta contiene una struttura dei dati sanitari rispondente alle necessità operative della Difesa. Detta struttura è compatibile con il protocollo di standardizzazione dei dati sanitari adottato a livello internazionale (NetLink).

Il suddetto modello NetLink (HC4016) prevede la seguente suddivisione:

- (1) **Dati ad accesso limitato**, questi dati possono essere letti in condizioni di emergenza sia dal personale autorizzato dal Servizio Sanitario Nazionale (SSN) sia dal personale autorizzato dal Servizio Sanitario Militare (SSM); essi sono riferiti a dati amministrativi (cognome, data di nascita, codice fiscale, indirizzo, ecc.) e a dati sanitari da trattare in caso di emergenza (gruppo sanguigno e trasfusioni, immunizzazioni, terapie correnti, organi mancanti, ecc.);
- (2) **Dati ad accesso protetto**, questi dati devono poter essere letti e scritti solo da personale autorizzato in possesso di chiavi di lettura/scrittura rilasciate dal SSM congiuntamente all'assenso del titolare della carta attraverso la digitazione del proprio PIN. Come già detto, le informazioni proprie di questa area sono quelle di carattere medico-sanitario necessari alle F.A. (vedasi Teatri Operativi).

d. **Dati di Vestiario e Matricolari**

Nella Carta possono essere inserite le informazioni relative all'attagliamentamento, alle misure antropometriche ed alla Tabella Vestiario del titolare. I dati matricolari inseriti sono quelli standard previsti dal Sistema Informativo del Personale dell'Amministrazione Difesa (SIPAD) (grado, anzianità di servizio, anzianità di grado, incarico ricoperto, ecc.).

5. **PUNTO DI SITUAZIONE SULLA IMPLEMENTAZIONE DELLA CARTA**

Attualmente la CMD è stata distribuita alla gran parte del personale Militare della Difesa (EI, MM, AM) e del personale Civile. L'Arma dei CC, per la propria peculiarità adoterà una CMD "ad hoc" pienamente compatibile con la Carta Multiservizi Difesa.

Entro il 2009 tutto il personale della Difesa (EI, MM, AM e personale Civile) sarà dotato di CMD. Anche il Comando Generale della Guardia di Finanza ha aderito al progetto CMD implementando una propria struttura di PKI (che riconosce quale Autorità di Certificazione principale la CA-Difesa).

6. **IMPIEGHI ATTUALI E SVILUPPI FUTURI**

Sistema GO.PERS: allo stato l'impiego più diffuso (ed individuale) della Carta Multiservizi Difesa è nel sistema per la rilevazione automatica delle presenze e gestione e governo del personale della Difesa "GO.PERS".

Il sistema (proprietà intellettuale Difesa) gestisce l'orario di servizio del personale dell'A.D. (ingresso/uscita, permessi, licenze, straordinario, ecc.). Per il suo utilizzo, da parte di tutti gli Enti, è stata emanata un'apposita direttiva.

L'interazione con il Go.Pers. avviene attraverso la Carta Multiservizi Difesa (CMD) che, inserita negli appositi lettori di Smart-Card (in ambito SMD sono stati installate apparecchiature Bio-Clock con relativo SW di gestione) posizionati presso i varchi di accesso alle infrastrutture, ne consente l'estrazione dei dati di ingresso/uscita del personale.

Al fine di ottimizzare le risorse, soprattutto in termini di gestione, l'applicativo è installato centralmente presso il Comando C4 Difesa (sia per lo SMD che per SGD). Per quanto attiene agli aspetti legati alla "privacy" si sottolinea che il sistema consente la compartimentazione sicura dei dati rilevati e pertanto la gestione del personale (orario di ingresso/uscita, statini riepilogativi, attribuzione straordinario, ecc.) è perimetrata al singolo Ente/Comando alla stessa stregua della attuale modalità cartacea.

Posta sicura: scambio di e-mail firmate e/o cifrate con garanzia di autenticità del mittente integrità e sicurezza.

In ordine agli sviluppi futuri la CMD potrà essere usata in particolare per le seguenti applicazioni:

- **Gestione dati sanitari:** le informazioni sanitarie sono inserite automaticamente, sotto la responsabilità di un medico militare, tramite le procedure informatiche sviluppate in ambito infermerie/ospedali militari;
- **Postazione di lavoro sicura:** accesso in totale sicurezza alla postazione di lavoro (eventualmente congiunta all'uso dell'impronta digitale);
- **Ingresso ad aree riservate:** autenticazione forte tramite utilizzazione congiunta della CMD e delle evidenze biometriche in essa contenute;
- **Accesso a servizi:** rifornimento carburanti, prelievo materiale/vestiario, acquisto beni presso strutture della Difesa (borsellino elettronico).

7. RICONOSCIMENTO DELLA CMD QUALE MOD. AT

La Presidenza del Consiglio dei Ministri, vista l'esperienza effettuata in ambito Difesa con la CMD e considerato il desiderio delle altre Pubbliche Amministrazioni di dotarsi di un analogo documento elettronico, ha avviato una attività interministeriale, guidata dal CNIPA, per la redazione di un decreto con cui stabilire le regole tecniche per il rilascio, in formato elettronico, ai dipendenti di ruolo delle amministrazioni pubbliche statali della tessera personale di riconoscimento Modello AT (di cui al decreto del Presidente della Repubblica 28 luglio 1967, n. 851).

Nella bozza di tale decreto è previsto il riconoscimento, a tutti gli effetti di legge, delle CMD già rilasciate dal Ministero della Difesa quale modello AT, fino alla loro naturale scadenza o revoca.