MEMORANDUM DI SICUREZZA PER TITOLARI DELLA CARTA MULTISERVIZI DELLA DIFESA (C.M.D.)

CMD N°	
Data di emissione:	
Data di scadenza:	
A favore di:	
Grado:	
Cognome e Nome	
Ente di appartenenza:	
e-mail personale di servizio:	_____@esercito.difesa.it

Referenti del Titolare: (Indicazione su dove trovare personale autorizzato a rispondere in caso di necessità)	**Responsabile Periferico (Comandante/Certificatore)** tel.
	Responsabile per il trattamento (Operatore CMD) tel.
C.S.I.E. Sezione CMD (da contattare al più presto in caso di furto, perdita o compromissione della CMD)	**Email:** **cmdsospensione@csie.esercito.difesa.it** **cmdinfo@csie.esercito.difesa.it** **Telefoni:** **Numero telefonico Sotrin : 10.3.7851** **Numero telefonico Urbano : 06.4735.7851**

Destinatari: gli utenti che, per un qualsiasi motivo, necessitino di operare in qualità di utilizzatori della Carta Multiservizi della Difesa (C.M.D.).

Obbiettivo: detto memorandum si prefigge di fornire indicazioni utili al fine di porre gli utenti della C.M.D. in grado di operare in sicurezza, evitare di subire falsificazioni od abusi nell'uso di questo moderno strumento, in particolar modo per quanto concerne:

- **identificazione elettronica** del titolare per usare la carta per l'accesso a sistemi informatici, sia a livello di rete, sia a livello di applicativo, in sostituzione delle procedure che prevedono l'utilizzo di "username" e "password";
- **autenticazione** (che permette l'uso della C.M.D. come strumento di accesso ad una rete od in particolare ad un portale web o ad una procedura informatica appositamente predisposta);
- **firma digitale** (firma a valore legale): è un supporto per effettuare operazioni di firma e cifra di documenti: attraverso un apposito certificato inserito nel microchip, il titolare è in grado di utilizzare la C.M.D. come strumento di firma digitale di documenti ed e-mail, 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.

Il presente memorandum viene fornito quale supporto cartaceo su cui l'utente può annotare, informazioni utili alla richiesta di supporto (n° CMD, data di scadenza CMD, passphrase, nominativi dei responsabili, etc.).
Pertanto, qualora la tabella sia compilata, questo memorandum dovrà essere custodito in luogo sicuro e comunque sempre separatamente dalla CMD stessa.

Modalità di pubblicazione: questo memorandum viene reso disponibile sulla rete EINET all'indirizzo:
http://acqs.csie.esercito.difesa.it/Modulistica/Modulistica.htm
e a richiesta dall'indirizzo e-Mail:
cmdinfo@csie.esercito.difesa.it.

Sanzioni in caso di inosservanza: come da: "Regolamento di disciplina", Codice Civile e Codice Penale vigenti. Fonti normative di riferimento:

- Legge 23 Dic. 1993 n° 547;
- Legge 8 Agosto 1974 n° 98;
- Leggi correlate.

Vengono ora 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 e in generale del PC che lo ospita. Infatti, il Titolare è tenuto a adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri [D.Lgs. 82 del 7 marzo 2005 (Codice dell'Amministrazione Digitale)] art. 32, comma 1[1]. Alcune delle regole seguenti non sono strettamente collegate al sistema di firma ma sono regole di sicurezza generali nell'uso del PC perché la sicurezza complessiva del sistema di firma dipende anche dalla sicurezza generale del PC su cui viene usato.

Si tratta di una lista semplice, spesso basata su considerazioni di buon senso, che riassume indicazioni già fornite altrove.

DIVIETI:

- **Non è consentito l'uso di questo sistema per informazioni coperte dal Segreto di Stato**. Per approfondimenti ulteriori su questo punto rivolgetersi al proprio Incaricato per la Sicurezza E.A.D..
- E' vietata la duplicazione della chiave privata di firma e dei dispositivi che la contengono ([DPCM 13 gennaio 2004], art.7, comma 1[2]).
- Non è consentito l'uso di una chiave per funzioni diverse da quelle previste dalla sua tipologia ([DPCM 13 gennaio 2004], art. 4, comma 5[3]), 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 fornito dal Certificatore, ovvero un dispositivo scelto tra quelli indicati dal Certificatore stesso ([DPCM 13 gennaio 2004], art. 6, comma 5[4]).

DOVERI:

- Con il sistema è possibile trattare informazioni sensibili in termini di privacy oppure informazioni d'ufficio di carattere "delicato".
- Custodire correttamente e diligentemente la smart card di firma portandola sempre con se, evitandone lo smarrimento e proteggendo la C.M.D. dal deterioramento in quanto contenente la chiave privata del militare, al fine di garantirne l'integrità e la massima riservatezza ([DPCM 13 gennaio 2004], art. 7, comma 3[5]).

---

[1] Art. 32. Obblighi del titolare e del certificatore
1. Il titolare del certificato di firma e' tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri ed a custodire e utilizzare il dispositivo di firma con la diligenza del buon padre di famiglia.

[2] Art. 7. Conservazione delle chiavi
1. É vietata la duplicazione della chiave privata e dei dispositivi che la contengono.

[3] Art. 4. Caratteristiche generali delle chiavi per la creazione e la verifica della firma
... omissis ...
5. Non é consentito l'uso di una coppia di chiavi per funzioni diverse da quelle previste, per ciascuna tipologia, dal precedente comma 4.

[4] Art. 6. Modalità di generazione delle chiavi
... omississ ....
5. Il titolare é tenuto ad utilizzare esclusivamente il dispositivo fornito dal certificatore, ovvero un dispositivo scelto tra quelli indicati dal certificatore stesso.

[5] Art. 7. Conservazione delle chiavi
... omissis ...
3. Il titolare della coppia di chiavi deve:
a) conservare con la massima diligenza la chiave privata o il dispositivo che la contiene al fine di garantirne l'integrità e la massima riservatezza;
b) conservare le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo contenente la chiave;
c) richiedere immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma difettosi o di cui abbia perduto il possesso.

- Non abbandonare la smart card di firma inserita nel lettore. Custodire la smart card nel vostro portafogli insieme alle vostre carte di credito e utilizzarla per il solo tempo necessario ad apporre la firma.
- Non scrivere il PIN di abilitazione della smart card 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 ([DPCM 13 gennaio 2004], art. 7, comma 3), e custodire con la massima diligenza i codici riservati ricevuti dal Certificatore al fine di preservarne la riservatezza. Quando viene digitato il PIN fare in modo che nessuno possa dedurlo osservando il movimento delle mani durante la digitazione.
- 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 smart card (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 vostra firma a un vostro collaboratore.
- 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 Call Center allo 1037851 (sotrin) oppure allo +39.06.4735.7851. A tale scopo conservare con cura la *"pass phrase"* che è stata inviata, unitamente al PIN/PUK, con la busta cieca. 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 Responsabile Periferico i possibili malfunzionamenti riscontrati sul dispositivo di firma.
- Devono essere, altresì, prontamente comunicati 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 per iscritto la revoca o la riattivazione dello stesso.
- Richiedere immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma difettosi o di cui si abbia perduto il possesso ([DPCM 13 gennaio 2004], art. 7, comma 3).
- Cessare l'utilizzo della C.M.D. ed i certificati in essa contenuti alla data della loro scadenza.
- Evitare di firmare digitalmente su stazioni di firma (PC) non fidate.
- Prestare attenzione alla configurazione del PC che usate per firmare digitalmente. Soprattutto evitate di installare programmi di cui non abbiate la certezza dell'origine e dell'affidabilità. Il rischio è l'installazione involontaria di software maligno (es. trojan, macrovirus o virus).
- I sistemi operativi della famiglia MS Windows® consentono di condividere risorse quali cartelle di lavoro e stampanti: va ricordato che se viene deciso di condividere un documento attraverso la condivisione di una cartella di lavoro situata sulla propria stazione di firma, gli utenti abilitati avranno accesso all'intero contenuto della cartella fintanto che non ci si ricordi di rimuovere la condivisione; si sconsiglia pertanto di usare tale possibilità, ma di avvalersi in alternativa delle cartelle condivise predefinite sui server di rete o di utilizzare la posta elettronica per spedire il documento.
- I PC delle reti in uso nell'E.I. sono protetti con anti-virus mantenuti costantemente aggiornati. Nel caso venga intercettato un virus o un trojan avvisate immediatamente l'Incaricato locale alla Sicurezza Informatica. E' ammesso usare la propria C.M.D. anche sul PC personale, pertanto è buona norma usare (e non disabilitiate mai), anche sul proprio computer personale, un buon programma anti-virus da mantenere costantemente 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 da disabilitare al rientro in sede.

- 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, (file con estensione .exe), ricevuti con messaggi di posta elettronica, memento da utenti fidati, dato che esistono virus che prendono dalla rubrica del client sul PC infetto indirizzi di utenti legittimi ai quali inviano file di qualsiasi tipo (anche .doc o .xls) 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.
- Curare un'adeguata protezione del proprio ambiente di lavoro: considerate che, secondo le statistiche, la gran parte delle violazioni di protezione avviene ad opera di personale interno, accedendo ad esempio ad un documento sensibile lasciato incustodito su una scrivania; evitate perciò di visualizzare a video, o di lasciare incustoditi su carta, documenti sensibili se non siete soli o in presenza di personale fidato, custodite con cura floppy disk, CD-ROM, chiavette USB, iPod, hard-disk portatili ed ogni altro strumento in grado di memorizzare informazioni il cui accesso deve essere ristretto.

CASI PREVISTI PER LA SOSPENSIONE E LA REVOCA DELLA CARTA A CURA DEL TITOLARE

Non appena si verifichi uno dei casi seguenti il Titolare di C.M.D. dovrà provvedere a richiedere la sospensione della carta.

Elenco dei casi di sospensione della carta a cura del Titolare

- Chip o carta difettosa per guasto o cattivo funzionamento
- Compromissione/perdita dei codici PIN e PUK
- Furto/smarrimento del dispositivo di firma (C.M.D.)
- 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 della chiave privata del militare o della macchina
- Compromissione o sospetta compromissione del certificato di autenticazione
- Cambio di almeno uno dei dati pubblicati nel certificato o dati errati
- Cessazione di utilizzo del servizio (dimissioni, pensionamento, altra PA, ecc.)
- Furto, smarrimento o distruzione del dispositivo di firma (C.M.D.) (perdita di possesso)
- Scadenza della C.M.D.
- Dati non variabili errati (ad es. il codice fiscale, il cognome, il nome, etc)

Modalità operative per l'utilizzo e la generazione delle firme digitali

Il Certificatore, unitamente al dispositivo di firma, nei casi previsti, consegna al Titolare della carta un lettore di smart card ed il software necessario per le operazioni di firma e cifra, disponibile anche sul sito https://acgs.csie.esercito.difesa.it/software.htm, per l'apposizione della firma digitale.

Il software consente la selezione del file da firmare, richiede l'inserimento della smart card nel lettore e la digitazione del PIN per l'attivazione della smartcard.
Il software consente la selezione della coppia di chiavi di firma da utilizzare, consentendo anche la visualizzazione del relativo certificato, e di visualizzare il 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" ([AIPACR24]).
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.

Formato dei documenti
L'automazione di ufficio 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, ad esempio, effettuare calcoli matematici.
L'art. 3, comma 3[6] del ([DPCM 13 gennaio 2004], ci dice che l'apposizione della firma su documenti elettronici contenenti "macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati", non produce gli effetti di cui al [DPR 445 del 2000], art. 10, comma 3[7].
Altresì il comma 2[8] dell'art. 21, del [D.Lgs. 82 del 7 marzo 2005 (Codice dell'Amministrazione Digitale)] stabilisce che "*il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che sia data prova contraria*".
Tali elementi di codice possono infatti produrre alterazioni al "contenuto" dipendenti dal contesto dell'ambiente di visualizzazione in uso.
Ad esempio, supponiamo che in una dichiarazione, dove normalmente a sinistra del gruppo firma viene messo "Luogo, lì ___", al posto della linea venga inserita una macroistruzione per la visualizzazione della data corrente e venga firmato il documento in data 18 aprile 2006. Supponiamo poi che la dichiarazione venga inviata il giorno dopo a destinazione, colui che la riceve vedrà che la dichiarazione è stata fatta il 19 aprile 2006 e non il 13 aprile, cioè vedrà visualizzata la data impostata riportata sul computer in uso, e se verificherà la firma del documento tutto sembrerà essere in regola.
Quanto sopra è da valorizzare quando deve essere firmato un documento di particolare "delicatezza/importanza".
Poiché non sono disponibili metodi certi per la verifica della presenza di tutti gli elementi in grado di alterare i contenuti di tali documenti presentati ai fini della apposizione e della verifica della firma, è sconsigliabile, finché possibile, il loro utilizzo per documenti particolarmente critici.

---

[6] Art. 3. Norme tecniche di riferimento
... omissis ...
3. Il documento informatico, sottoscritto con firma digitale o altro tipo di firma elettronica avanzata basata su un certificato qualificato e generata mediante un dispositivo sicuro per la creazione di una firma, non produce gli effetti di cui all'art. 10, comma 3, del testo unico, se contiene macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati.
[7] Articolo 10 (R) Forma ed efficacia del documento informatico
... omissis ...
3. Il documento informatico, quando é sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma é basata su di un certificato qualificato ed é generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto.
[8] Art. 21. Valore probatorio del documento informatico sottoscritto
... omissis...
2. Il documento informatico, sottoscritto con firma digitale o con un altro tipo di firma elettronica qualificata, ha l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma si presume riconducibile al titolare, salvo che sia data prova contraria.

Pertanto, soprattutto per i documenti critici, si suggerisce l'uso di formati documentali statici quali ad esempio:

- Puro testo - ".txt",
- Immagine - ".tif",
- Portable Document Format - ".pdf" (se privo di campi modulo).

Si faccia riferimento alla SMD - I - 002 (Formati di scambio di documenti di testo in formato elettronico nell'ambito della Difesa) per ulteriori informazioni in merito.

Obblighi dei destinatari

I destinatari dei messaggi elettronici e/o delle evidenze informatiche firmate digitalmente da Titolare della C.M.D. 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'Amminsitrazione;
- 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".

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 [D.Lgs. 82 del 7 marzo 2005 (Codice dell'Amministrazione Digitale)] art. 30, comma 3[9].

Infine si tenga conto delle problematiche relative alla eventuale presenza di macroistruzioni o codice eseguibile nel documento verificato di cui al paragrafo "Formato dei documenti".

[9] Art. 30. Responsabilità del certificatore

... omissis ...

3. Il certificato qualificato può contenere limiti d'uso ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, purche' i limiti d'uso o il valore limite siano riconoscibili da parte dei terzi e siano chiaramente evidenziati nel processo di verifica della firma secondo quanto previsto dalle regole tecniche di cui all'articolo 71. Il certificatore non e' responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.