ALLEGATO B

MEMORANDUM DI SICUREZZA PER IL PERSONALE TITOLARE DELLA TESSERA MODELLO ATe

Destinatari: tutto il personale dell'Amministrazione della Difesa.

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

- **autenticazione** dell'interessato, che permette di usare il certificato di autenticazione 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, l'interessato è in grado di utilizzare la tessera mod. ATe come strumento di firma digitale di documenti, in conformità alle vigenti disposizioni di legge;
- **cifra** per cifrare i documenti, in modo che possano essere accessibili solo al destinatario. Le finalità sono di natura operativa e di rispetto di *security, privacy* e leggi penali.

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

In caso di inosservanza ovvero cattiva gestione della tessera mod. ATe sono previste sanzioni in attuazione ai regolamenti , alle norme contrattuali, ai regolamentari e alle leggi in materia disciplinare sia per il personale militare sia per il personale civile[1]

Di seguito sono elencate alcune regole di sicurezza che l'interessato 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, l'interessato è tenuto a adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri [2]. Alcune delle regole seguenti non sono strettamente collegate al sistema di firma ma sono regole di sicurezza generali nell'uso dei sistemi di elaborazione nella considerazione che la sicurezza complessiva del sistema di firma dipende anche dalla sicurezza generale della macchina su cui viene utilizzato.

DIVIETI:

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

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

SEGUE ALLEGATO B

DOVERI:

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

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

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

SEGUE ALLEGATO B

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

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

SEGUE ALLEGATO B

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

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

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

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

- 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 dell'interessato

- Chip o carta difettosa per guasto o cattivo funzionamento;
- Compromissione o sospetta compromissione delle chiavi private (firma e autenticazione);
- Cambio di almeno uno dei dati pubblicati nei certificati digitali o dati errati;
- Cessazione dal servizio nell'Amministrazione della Difesa (dimissioni, pensionamento, passaggio ad altra PA, ecc.);
- Furto, smarrimento o distruzione della carta (perdita di possesso);
- Scadenza della tessera mod. ATe;
- Dati non mutabili errati (Es. codice fiscale, cognome, nome, data di nascita)

UTILIZZO DELLA CARTA

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

Unitamente al dispositivo di firma, nei casi previsti, viene messo a disposizione dell'interessato 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 all'interessato di confermare la volontà di firmare il documento elettronico visualizzato. In caso di assenso, il software procede alla produzione del documento informatico in un file con estensione ".p7m" o "pdf". L'interessato per poter inviare posta elettronica firmata digitalmente dovrà obbligatoriamente avere configurato il client di posta elettronica (Outlook) in modo che la e-mail inviata riporti nel campo From (Da) l'indirizzo di posta elettronica inserito nel certificato.

SEGUE 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 dall'interessato devono verificare:

- che il certificato contenente la chiave pubblica dell'interessato firmatario del messaggio e/o evidenza informatica non sia temporalmente scaduto;
- che il certificato dell'interessato sia stato firmato con le chiavi di certificazione della Autorità di Certificazione presenti nell'Elenco Pubblico mantenuto dall'Amministrazione;
- l'assenza del certificato 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 dall'interessato;
- 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[8]. Infine si tenga conto delle problematiche relative alla eventuale presenza di macroistruzioni o codice eseguibile nel documento verificato.

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