Smart Card API - Windows

Librerie PKCS#11 e CSP per smart card

Manuale Utente

Versione 3.87

Autore:	Ministero Della Difesa - S.M.D. COR Difesa
Versione:	3.87
Data del documento:	Giugno 2024
No Doc.:	PTC-SCA-387

Contenuto

1 Introduzione

Questo manuale contiene una guida passo-passo per installare, disinstallare **Smart Card API** in ambiente Microsoft Windows così come le informazioni di configurazione e utilizzo.

Tutti gli esempi e le schermate mostrate in questo manuale, sono state catturate su un sistema Microsoft Windows 7 e 10. Se si stesse utilizzando un sistema operativo diverso, le finestre mostrate sullo schermo potrebbero essere leggermente differenti.

Il contenuto del pacchetto di distribuzione è il seguente:

File	Descrizione
SmartCardAPI.x86.Setup.exe	Pacchetto di installazione per sistemi Microsoft Windows a 32 bit
SmartCardAPI.x64.Setup.exe	Pacchetto di installazione per sistemi Microsoft Windows a 64 bit
Manuale Utente Smart Card API.pdf	Manuale Utente, ovvero il presente documento
Smart Card API Support.doc	Modulo per la richiesta di supporto

1.1 Destinatari del documento

Questo documento è stato ideato come riferimento per:

- Titolari di smart card che volessero utilizzarla con applicazioni in ambiente Microsoft Windows
- Utenti e sviluppatori che usano applicazioni che possono essere integrate con un CSP personalizzato e un PKCS#11 standard.
- Amministratori di sistema che volessero informazioni su come gestire il pacchetto.

Si presume che il lettore di questo documento abbia familiarità con la tecnologia delle smart card e le infrastrutture a chiave pubblica (*Public Key Infrastructure* (PKI)).

1.2 Copyright di terze parti

Lo standard Cryptographic Token Interface "RSA Security Inc. Public Key Cryptography Standard PKCS)" è copyright di RSA Security Inc. (www.rsasecurity.com).

Smart Card API utilizza routine di decompressione del progetto Zlib (http://www.zlib.net/). Il software zlib è copyright di Jean-loup Gailly e Mark Adler.

Smart Card API utilizza routine crittografiche del progetto OpenSSL (http://www.openssl.org). Il software OpenSSL è copyright di Eric Youg e del The OpenSSL Project.

Smart Card API utilizza routine per la gestione di file XML del progetto libxml2 (http://www.xmlsoft.org). Il software libxml2 è copyright di Daniel Veillard.

1.3 Cambiamenti rispetto alle versioni precedenti

Smart Card API è l'evoluzione del precedente software CMD API v2.2. Rispetto alla versione precedente, che era in grado di supportare solo smart card di tipo CMD, questa versione supporta anche le CMCC, rendendo quindi opportuno un cambiamento di nome.

Versione	Cambiamenti
3.00.0000	Cambiato il nome da CMD API ad Atos Smart Card API per indicare il supporto a più tipi di smart card
	Aggiornate tutte le librerie alle versioni più recenti
	Supporto per sistemi operativi Microsoft Windows a 32bit e 64bit
	Supporto per la smart card CMCC (Carta Multiservizi dei Carabinieri) per le operazioni di autenticazione e firma digitale
3.10.0000	Eliminata la funzione di sblocco PIN all'interno della finestra di richiesta PIN (utilizzare l'applicazione apposita di gestione PIN)
3.20.0000	Supporto dei file system di firma digitale aggiuntivi per la CMD-1
	Differenziazione visuale delle finestre di richiesta PIN/PIN Firma delle carte
	Risolto problema durante l'installazione delle icone nel menu Start per sistemi a 64bit
	Nuova funzionalità di cache del PIN di firma: l'utente in fase di prima immissione del PIN di firma, può decidere per quante operazioni di firma il PIN sarà memorizzato prima di essere chiesto nuovamente. Il valore iniziale è specificato nel file di configurazione (KEYUSECOUNT)
3.30.0000	Corretti alcuni bug sulla scrittura degli oggetti con la libreria PKCS#11
	Corretto un bug sulla scrittura dei log in directory diverse da %TEMP%
3.40.0000	Aggiunto il supporto della piattaforma Microsoft Windows 8 a 32 e 64 bit
3.50.0000	Aggiunto il supporto per la carta CMD-2
	Risolto il problema dell'utilizzo della libreria PKCS#11 sullo stesso computer ma con utenti differenti (ad esempio via Remote Desktop o in ambienti Cytrix)
3.51.0000	Risolto un problema sulle carte CMD-1 dotate di certificato di Smart Card Logon. Questo problema poteva causare dei crash di alcuni servizi di Windows.
3.52.0000	Risolto un piccolo bug
3.53.0000	Migliorata la compatibilità della libreria PKCS#11 con Java 1.8
3.60.0000	Aggiunti ulteriori oggetti PKCS#11 che contengono i dati personali del titolare della carta oltre a quelli standard CNS
	Corretto un difetto nella libraria PKCS#11 che causava problemi con alcuni software di terze parti.
	Aggiunte ulteriori informazioni nel presente manuale dedicate agli sviluppatori
3.61.0000	Risolto un problema di compatibilità minore su Windows 8/10/2012/2016

Versione	Cambiamenti
3.62.0000	Cambiato l'aspetto grafico delle schermate di richiesta PIN Carta/PIN Firma
	Corrette le diciture riguardanti il PIN Carta in modo da evitare ambiguità
	Adeguata la nomenclatura dei percorsi e dei collegamenti al software fornito dal TSP
3.63.0000	Eliminata la necessità di modificare il registro di Windows per gestire il timeout delle operazioni sulla smart card durante la richiesta del PIN (era trasparente per l'utente in quanto veniva inserita durante l'installazione del pacchetto, ma durante gli aggiornamenti di Windows, il settaggio veniva rimosso richiedendo la reinstallazione del pacchetto).
3.80.0000	Supporto per le smart card Modello ATe con chip Oberthur CNS COSMO ID/ONE v7, ovvero le nuove CMD-2 e le CMCC-2.
	Migliorata la messaggistica dell'applicazione di gestione dei PIN/PUK della carta.
3.81.0000	Aggiunto il supporto alle funzioni di Windows smart card logon con carte CMD-2 con chip Oberthur
3.82.0000	Supporto per le smart card non nominative "Pass Visitatore" del Ministero della Difesa con a bordo il servizio di Windows Smart Card Logon
3.84.0000	Supporto per le smart card Modello ATe con chip IDEMIA CNS COSMO ID/ONE v9.
	Migliorata la gestione dei certificati sull'inserimento della carta nel lettore: in questa versione a ogni inserimento, verranno contestualmente cancellati dallo store di Windows gli eventuali certificati propagati precedentemente dallo stesso lettore di smart card e non cancellati in corrispondenza della rimozione della carta dal lettore (ad esempio se si spegne il PC con la carta inserita nel lettore o si chiude lo Smart Card Monitor con la carta inserita nel lettore). In questo modo si riduce del 99% la possibilità di firmare erroneamente con un certificato non corrispondente alla carta inserita.
3.85.0000	Risolto un problema nella lettura dei certificati dalla carta che poteva manifestarsi in rari casi in cui nello store Personale di Windows si trovassero certificati di terze parti senza chiave privata.
3.86.0000	Aggiunto supporto alla nuova carta IDEM v9.1
3.87.0000	Aggiunto logo SMD.

2 Requisiti di sistema

2.1 Smart card supportate

Le smart card supportate da Smart Card API sono elencate nella seguente tabella con i relativi ATR e maschere:

Tipo	ATR e maschera (valori esadecimali)
CMD-1 (CMD-1 senza firma qualificata)	3B F2 98 00 FF C1 10 31 FE 55 C8 03 15 FF FF FF FF FF FF FF FF Ff FF FF FF FF 3B F2 98 00 FF C1 10 31 FE 55 C8 04 12 FF FF FF FF FF FF FF FF Ff FF FF FF FF 3B F0 98 00 FF C1 10 31 FE 55 DC FF FF FF FF FF FF FF FF Ff FF FF
CMD-1 v1.1 (CMD-1 con firma qualificata SHA-2)	3B 00 98 00 FF C1 10 31 FE 55 00 00 00 43 4D 44 00 00 00 00 FF 00 FF FF FF FF FF FF FF FF 00 00 00 FF FF FF 00 00 00 00
CMD-1 v1.5 (CMD-1 con firma qualificata SHA-2 e chip CardOS 4.2B)	3B F2 98 00 FF C1 10 31 FE 55 C8 04 12 FF FF FF FF FF FF FF FF Ff FF FF FF FF
CMCC	3B FF 18 00 FF 81 31 FE 55 00 6B 02 09 03 00 01 11 01 43 4E 53 11 31 80 8F FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
CMD-2 / Modello ATe (chip ST-Incard T&S 2048 CNS)	3B FF 18 00 FF 81 31 FE 55 00 6B 02 09 13 01 01 11 01 43 4E 53 11 31 80 9E FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
CMD-2 / CMCC-2 / Modello ATe (chip Oberthur CNS COSMO ID/ONE v7)	3B FF 18 00 00 81 31 FE 45 00 6B 11 05 07 00 01 11 01 43 4E 53 11 31 80 7B FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
CMD-2 / CMCC-2 / Modello ATe (chip IDEMIA CNS COSMO ID/ONE v9)	3B FF 18 00 00 81 31 FE 45 00 6B 05 05 20 00 01 21 01 43 4E 53 10 31 80 79 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
Pass Visitatore (non nominativa)	3B FF 18 00 00 81 31 FE 45 00 6B 11 05 07 00 01 21 01 43 4E 53 10 31 80 4A FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
Modello ATe (chip Oberthur v9.1)	3B FF 18 00 00 81 31 FE 45 00 6B 05 05 91 20 01 00 01 43 4E 53 10 31 80 38 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 00 FF FF FF FF FF FF FF FF

2.2 Requisiti software

Smart Card API è stato testato sui seguenti sistemi operativi:

- Microsoft Windows XP 32bit Service Pack 3
- Microsoft Windows XP 64bit Service Pack 2
- Microsoft Windows 7 32bit Service Pack 1
- Microsoft Windows 7 64bit Service Pack 1
- Microsoft Windows 8 32bit
- Microsoft Windows 8 64bit
- Microsoft Windows 10 64bit
- Microsoft Windows 2008 32bit
- Microsoft Windows 2008 64bit
- Microsoft Windows 2008 R2 64bit
- Microsoft Windows 2012 64bit

Assicurarsi di avere almeno 30MB di spazio disco libero prima dell'installazione.

Smart Card API lavora su tutte le applicazioni Windows che usano le interfacce Microsoft CAPI o PKCS#11 Cryptoki per l'accesso alla smart card. Una limitazione delle funzionalità potrebbe verificarsi, se l'applicazione chiamante non è completamente conforme alle specifiche dell'interfaccia o se utilizza delle funzioni proprietarie o non documentate di altri produttori.

2.3 Requisiti hardware

Il software Smart Card API è stato testato su una varietà di lettori di smart card conformi PC/SC (www.pcscworkgroup.com) su piattaforme Microsoft Windows. I driver appropriati per i lettori sono forniti dai rispettivi produttori e venditori del lettore.

Tutti i lettori di smart card compatibili PC/SC dovrebbero lavorare in maniera corretta. Comunque, possono verificarsi occasionali problemi per varie ragioni (per esempio alcune operazioni di base delle smart card non sono compatibili con il timeout del lettore, ecc.). Si consiglia quindi di utilizzare lettori dotati di driver forniti dal produttore.

Riguardo i requisiti hardware del PC o server, si faccia riferimento ai requisiti hardware del sistema operativo su cui viene eseguito.

3 Procedure di installazione e disinstallazione

Le procedure di installazione e disinstallazione del software Smart Card API richiedono l'utilizzo di credenziali di tipo Amministratore. Prima di eseguire una delle procedure elencate, assicurarsi di essere in possesso di tali credenziali.

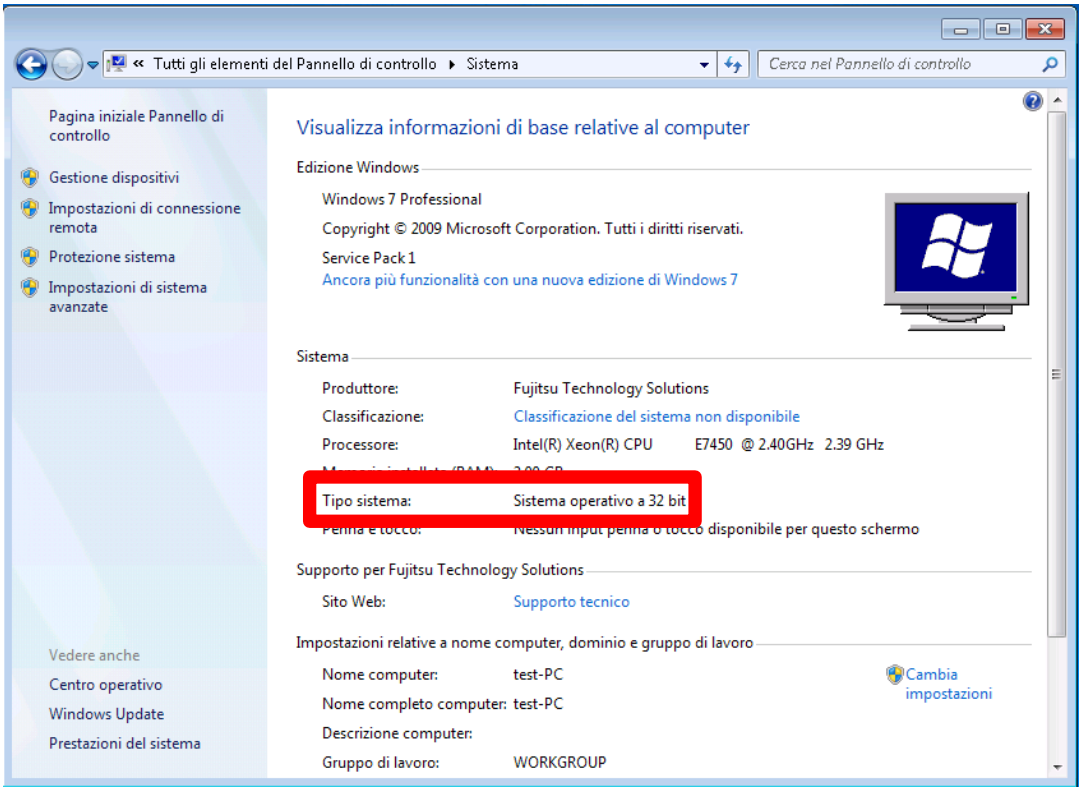
A causa di un cambiamento apportato da Microsoft ai sistemi operativi Windows con versione 8 e successive, se si è eseguito un aggiornamento da una delle precedenti versioni di Windows e Smart Card API era già presente sul proprio sistema, si consiglia di rieseguire l'installazione delle API in quanto l'aggiornamento di Windows reimposta alcuni valori impostati durante l'installazione delle API stesse.

3.1 Installazione

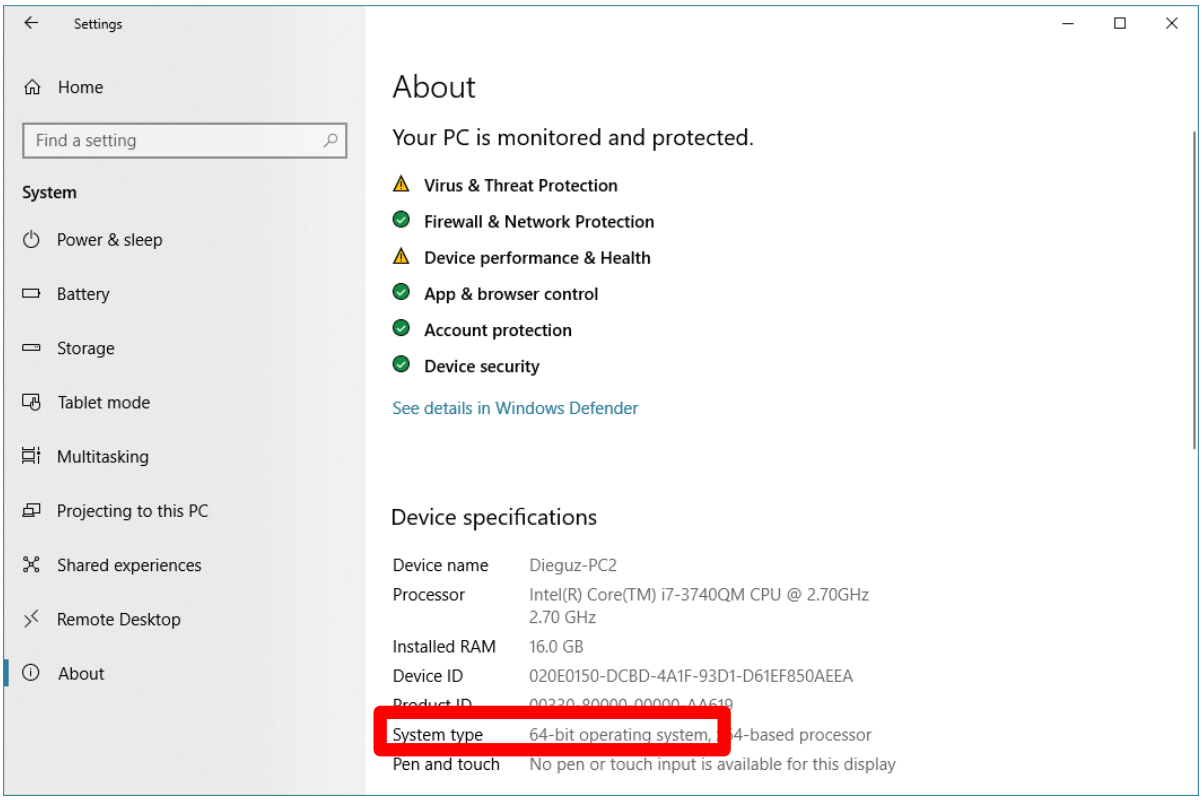
A seconda del proprio sistema operativo, l'installazione di Smart Card API avviene eseguendo il pacchetto di setup appropriato:

- **SmartCardAPI.x86.Setup.exe** per sistemi Microsoft Windows a 32bit
- **SmartCardAPI.x64.Setup.exe** per sistemi Microsoft Windows a 64bit

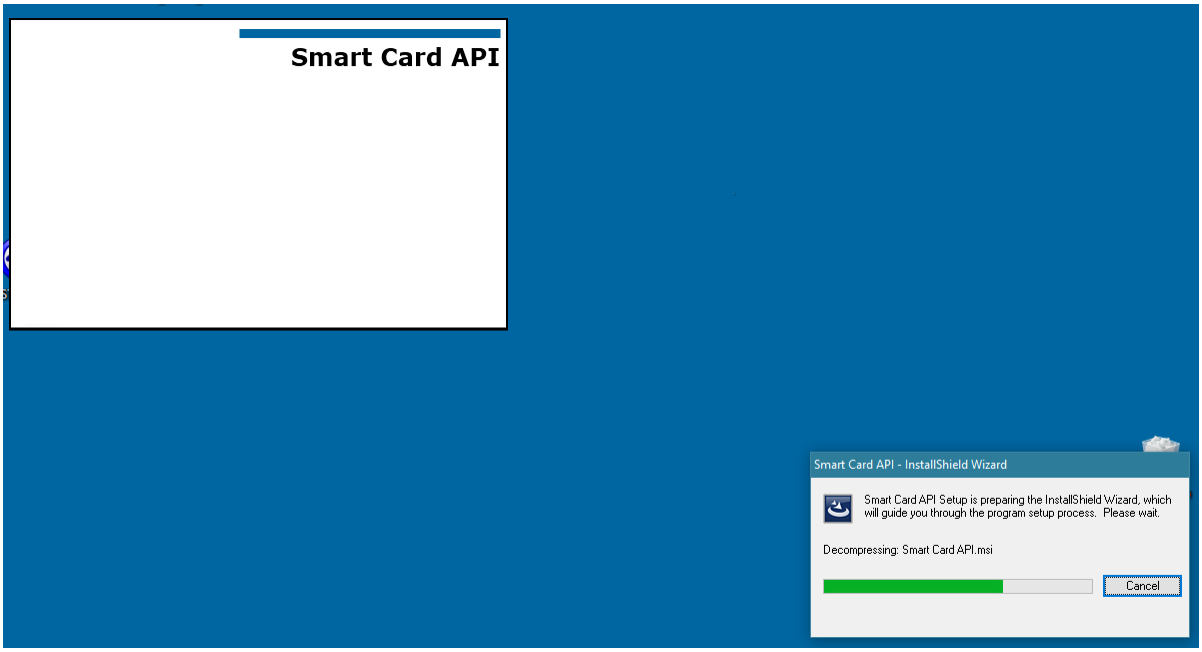
È fondamentale installare il pacchetto corretto sul proprio sistema, in caso contrario, Smart Card API funzionerà in modo scorretto. Se non si è a conoscenza di quale versione di sistema operativo si è in possesso, lanciare l'applicazione *Sistema* dal *Pannello di controllo* di Microsoft Windows, apparirà una schermata simile alla seguente, dove evidenziato in rosso viene indicato il tipo di sistema (esempio su Windows 7):



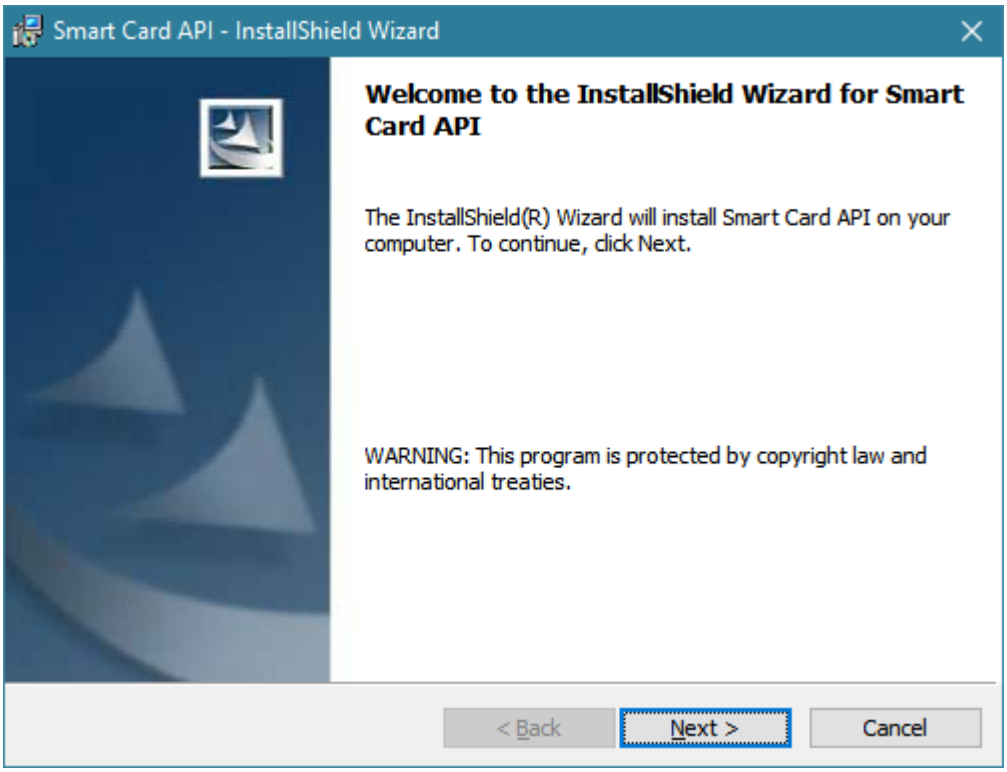
Oppure su Windows 10:



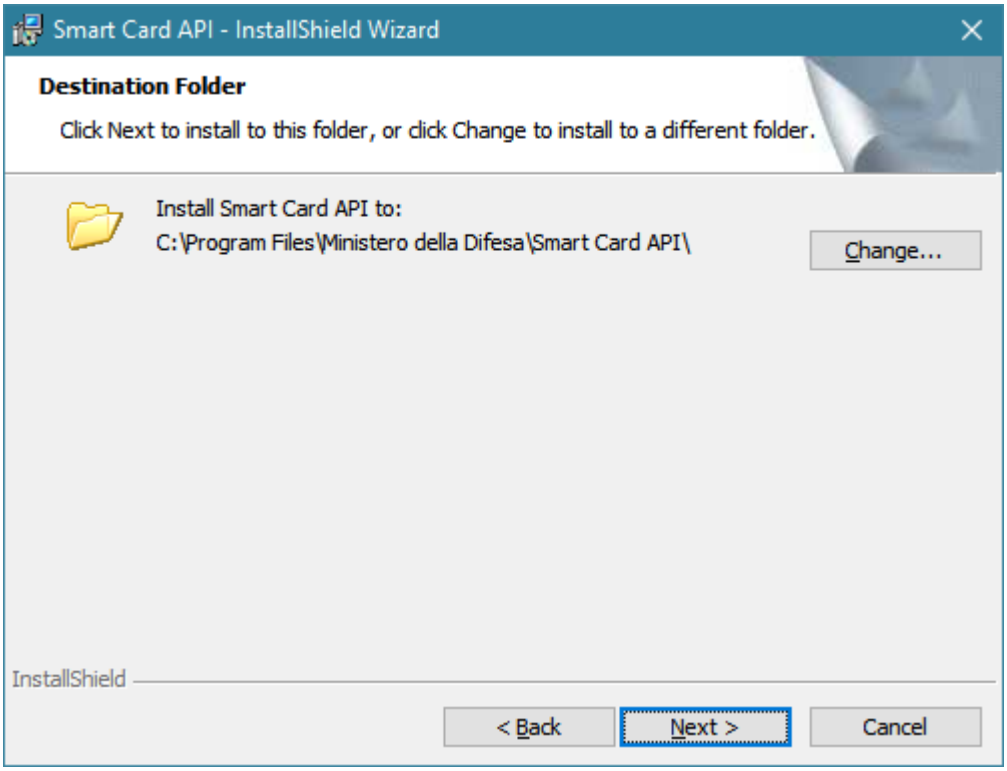
Una volta lanciato il pacchetto di setup corretto, apparirà la seguente schermata:



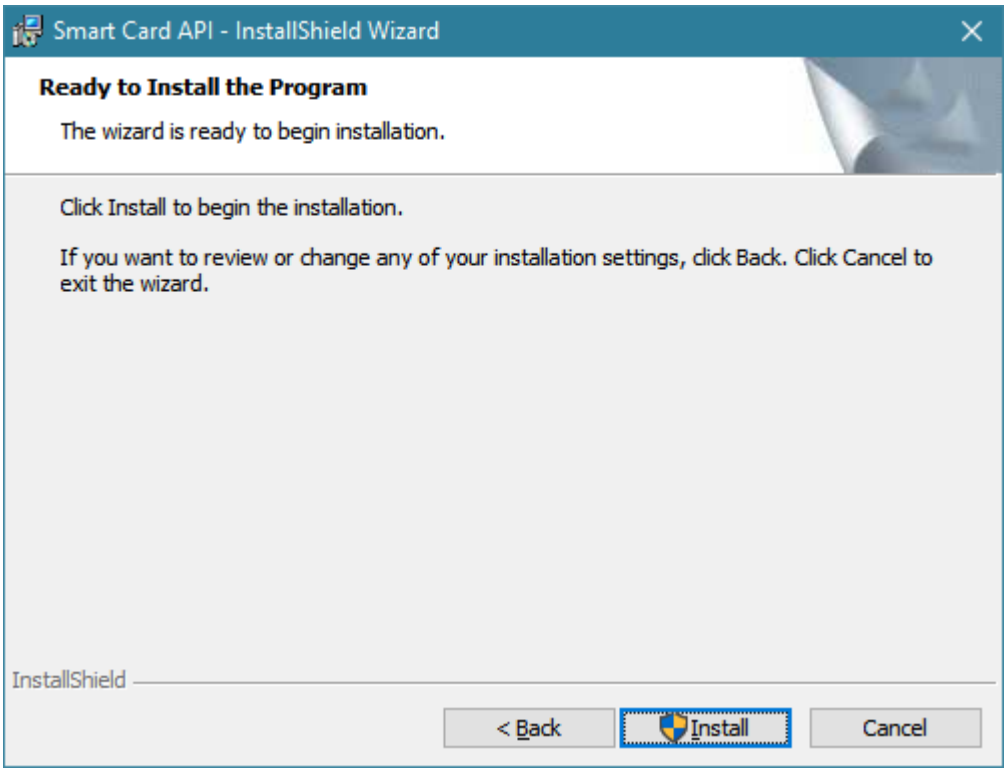
Attendere che il sistema predisponga il pacchetto di setup, al termine apparirà la seguente schermata:



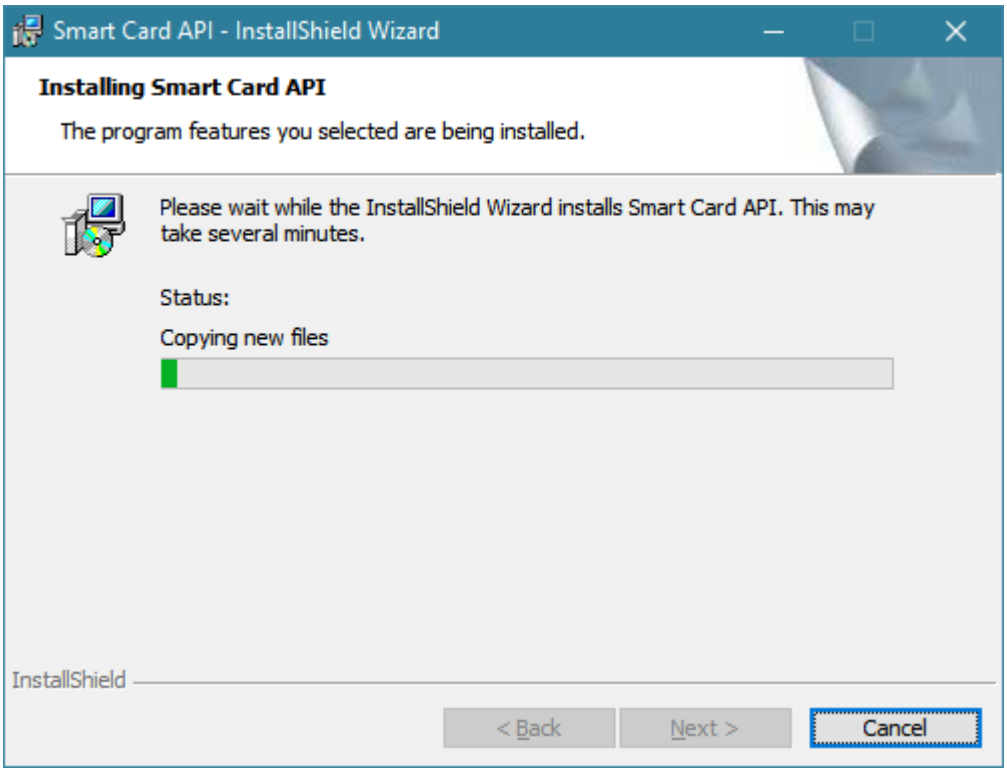
Premere il tasto **Next >**, apparirà la seguente schermata:



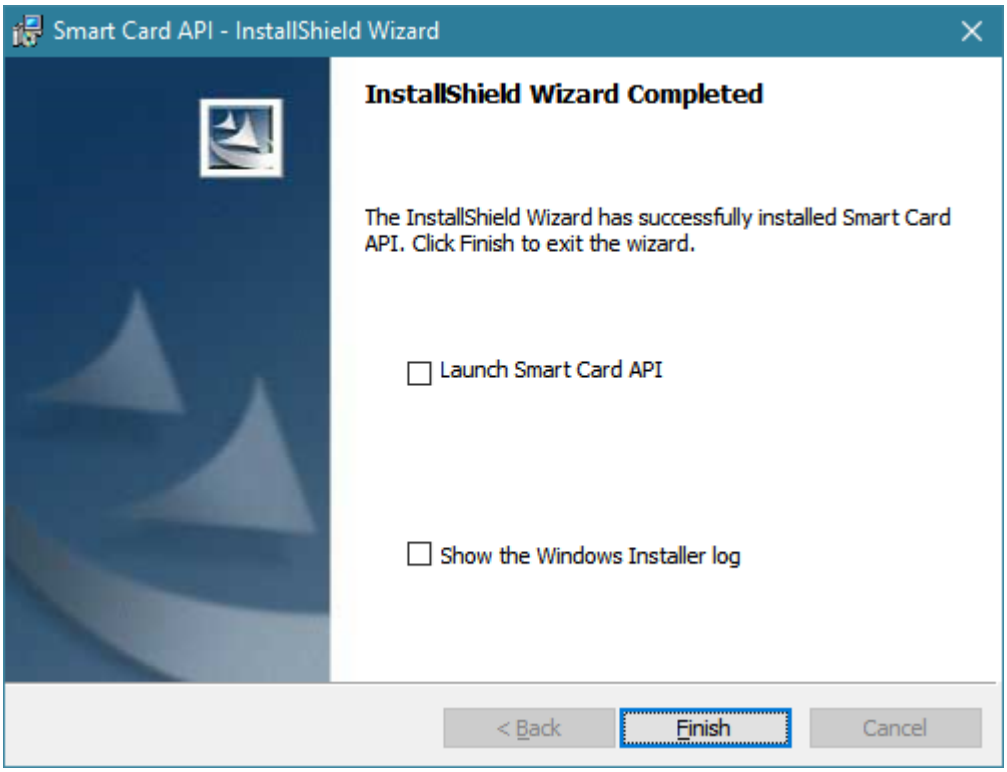
Premere il tasto **Next >** se si accetta il percorso suggerito, altrimenti cambiarlo con **Change...**, apparirà la seguente schermata:



Premere il tasto **Install** (su Windows Vista/7/2008 verrà richiesta la conferma di un'operazione come amministratore), apparirà la seguente schermata:

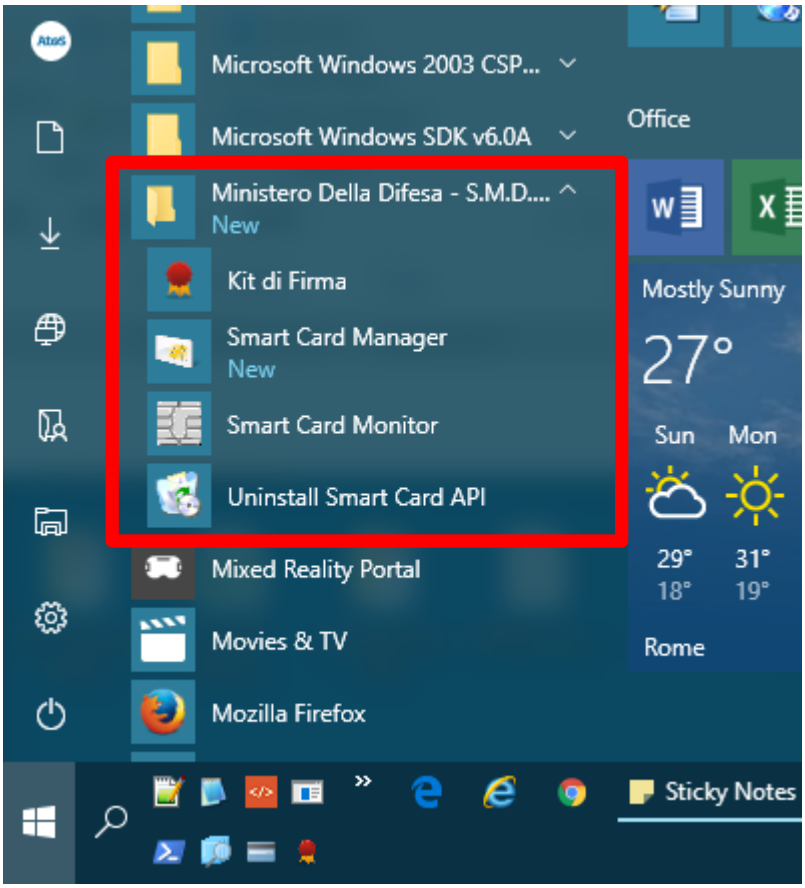


Attendere che l'applicazione di setup completi le operazioni, al termine apparirà la seguente schermata di conferma:



Selezionare **Launch Smart Card API** e premere il tasto **Finish**.

Al termine dell'installazione, nel menu *Start* di Microsoft Windows, *Tutti i programmi*, saranno presenti delle nuove icone nella cartella **Ministero Della Difesa - S.M.D. Comando C4**:



Smart Card Manager è l'applicazione per gestire la propria smart card (cambio e sblocco PIN, ecc…) (si veda la sezione 0), **Smart Card Monitor** è l'applicazione per la propagazione dei certificati della smart card (si veda la sezione 4) e **Uninstall Smart Card API** è l'applicazione per la disinstallazione di Smart Card API (si veda la sezione 1).

3.1.1 Installazione silente

Nel caso si volesse eseguire un'installazione senza alcun intervento dell'utente (modalità silente), è possibile eseguire il pacchetto di setup da riga di comando come amministratore nel seguente modo:

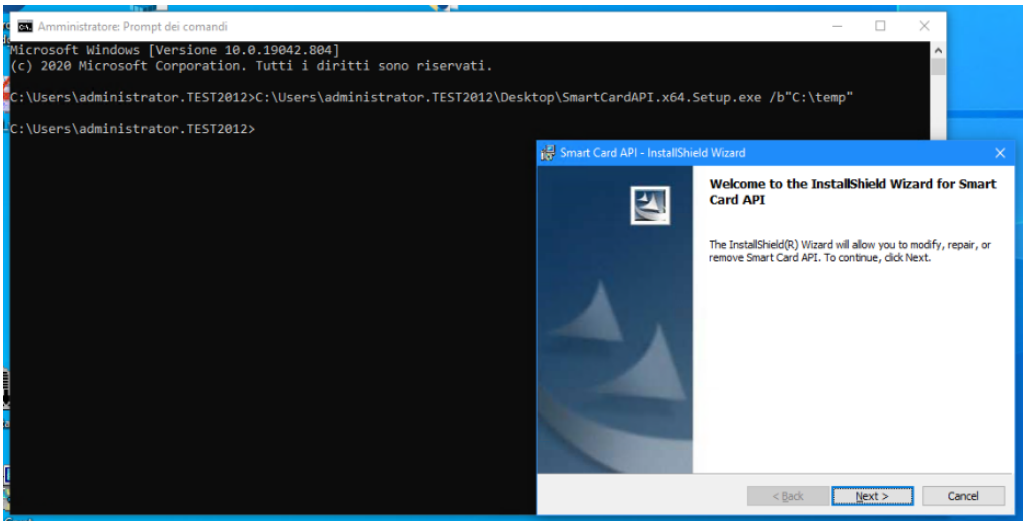
- **SmartCardAPI.x86.Setup.exe /S /v/qn** per sistemi Microsoft Windows a 32bit
- **SmartCardAPI.x64.Setup.exe /S /v/qn** per sistemi Microsoft Windows a 64bit

L'installazione procederà in maniera del tutto automatica, senza chiedere alcuna conferma all'utente.

3.1.2 Estrazione del pacchetto MSI

Se si avesse necessità del pacchetto di setup in formato MSI, ad esempio per sistemi di software distribution particolari, è possibile ottenerlo in un percorso fisso (ad esempio C:\Temp) lanciando il seguente comando:

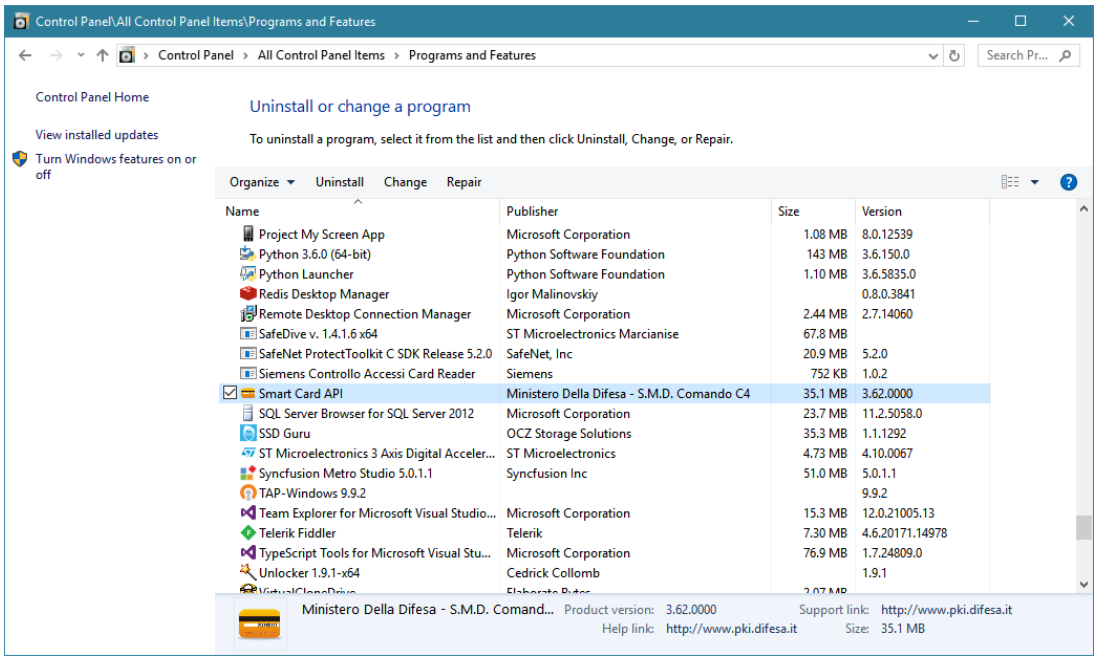
- **SmartCardAPI.x64.Setup.exe /b"C:\temp"** per la versione a 64bit
- **SmartCardAPI.x86.Setup.exe /b"C:\temp"** per la versione a 32bit



Attendere qualche secondo che compaia la prima schermata del setup e invece di proseguire, salvarsi il file **Smart Card API.msi** che si trova al percorso indicato, (rinominarlo opportunamente se serve distinguere versione e sistema operativo, ad esempio SmartCardAPI.385.x64.msi. Solo a questo punto annullare l'installazione tramite il tasto **Cancel**.

3.2 Disinstallazione

La disinstallazione di Smart Card API può essere eseguita o dal menu *Start*, *Tutti i programmi*, *Ministero Della Difesa - S.M.D. Comando C4*, **Uninstall Smart Card API**, oppure dall'applicazione *Programmi e funzionalità* nel *Pannello di controllo* di Microsoft Windows:

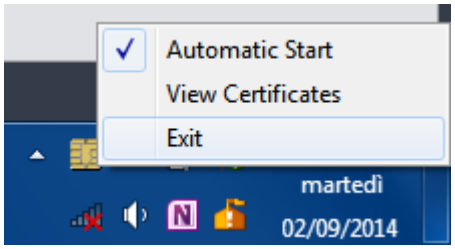


Selezionare **Smart Card API** dalla lista e premere il pulsante **Disinstalla**. Partirà un wizard per la disinstallazione. Seguire tutti i passi fino al termine del processo.

3.3 Aggiornamento

Nel caso di un aggiornamento del pacchetto in seguito al rilascio di una nuova versione, è consigliabile procedere secondo i seguenti passi:

- Chiudere tutte le applicazioni lanciate sulla propria postazione di lavoro;
- Chiudere l'applicazione di monitoraggio delle smart card (Smart Card Monitor) come in figura (tasto destro sull'icona e poi *Exit*):



- Disinstallare il pacchetto come indicato nella sezione 3.2;
- Riavviare la propria postazione di lavoro;
- Installare la nuova versione del pacchetto di installazione come indicato nella sezione 3.1;
- Riavviare la propria postazione di lavoro.

4 Utilizzo di Smart Card API

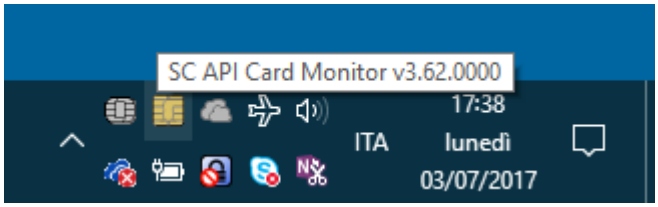
Affinché i certificati presenti su una smart card supportata da Smart Card API siano utilizzabili dalle applicazioni eseguite in ambiente Microsoft Windows, è necessario che l'applicazione di monitoraggio delle carte (**Smart Card Monitor**) sia in funzione. Ogni volta che una smart card viene inserita in un lettore, Smart Card Monitor propaga tutti i certificati presenti su di essa all'interno dello store di Microsoft Windows, ovvero la posizione del sistema operativo alla quale tutte le applicazioni Windows possono attingere per utilizzare i certificati.

Smart Card Monitor viene eseguito ogni volta che si esegue l'accesso a Windows e la sua icona è visibile nella barra delle applicazioni di Windows vicino all'orologio (evidenziata in rosso nella figura seguente).

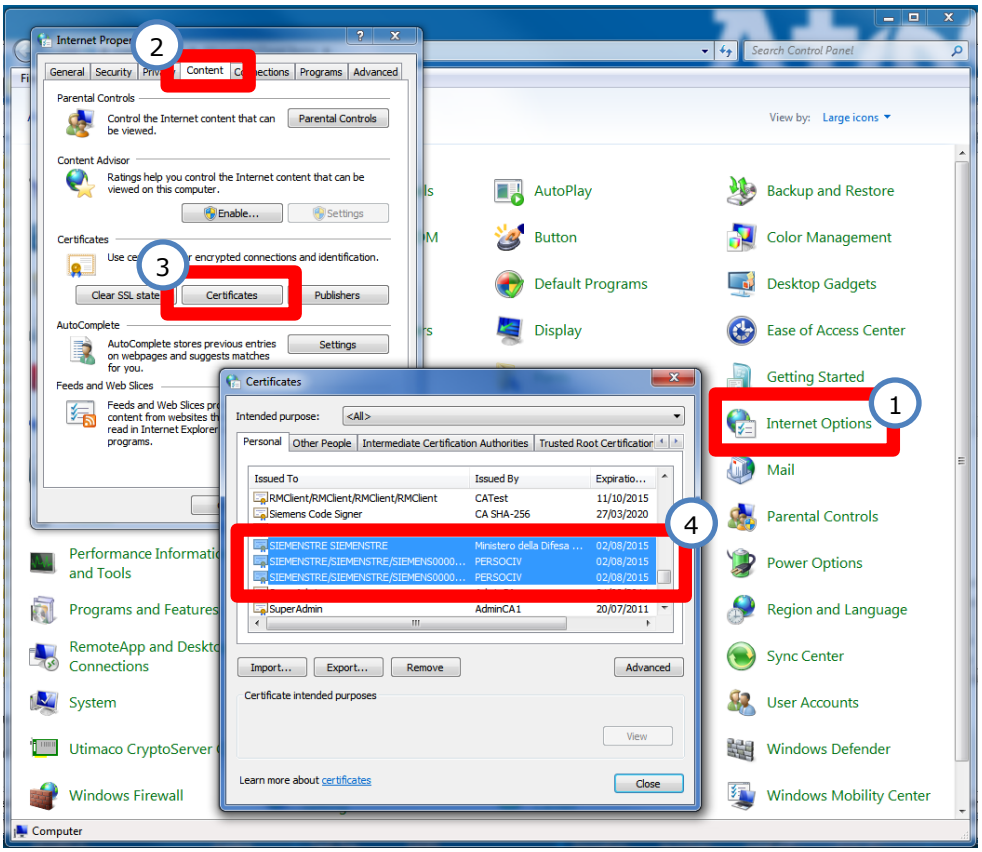
L'icona nella barra delle applicazioni può assumere vari aspetti e animarsi, a seconda della situazione attuale. Nella seguente tabella vengono elencati i significati dell'icona:

Icona	Significato
	Indica che Smart Card API è in attesa che venga inserita una smart card in uno dei lettori
	Se animata, indica che Smart Card API supporta la smart card inserita ed è in corso la propagazione dei certificati nello store di Microsoft Windows
	Indica che è stata inserita una smart card supportata da Smart Card API e i certificati al suo interno sono stati propagati nello store di Microsoft Windows
	Indica che è stata inserita una smart card non supportata da Smart Card API

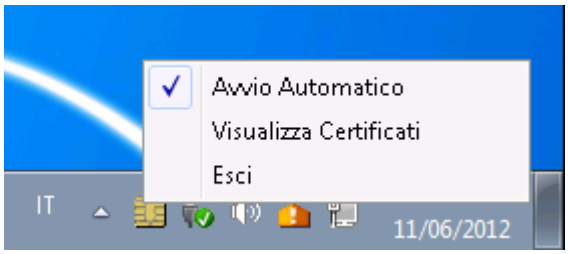
Tenendo fermo il puntatore del mouse sull'icona, è possibile visualizzare la versione di Smart Card API installata (utile in caso di segnalazioni di errori):



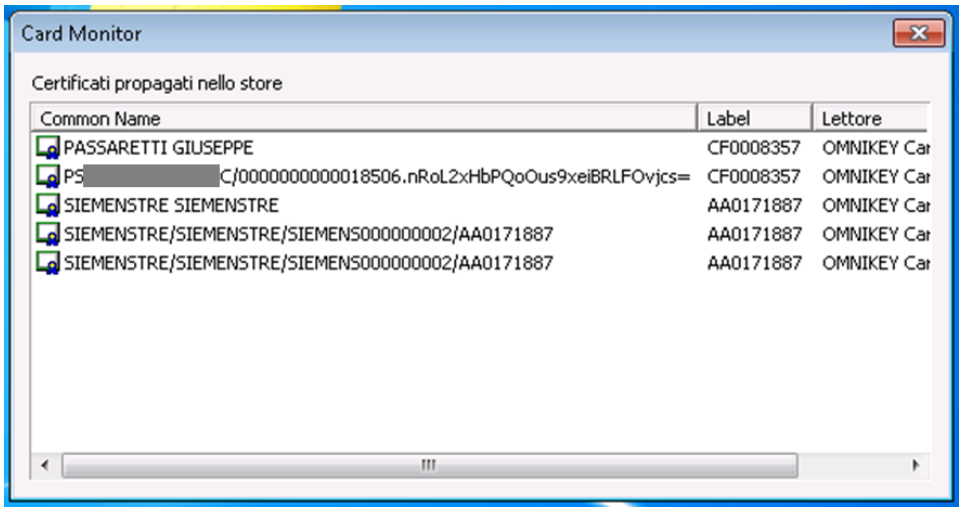
I certificati propagati si possono visualizzare lanciando l'applicazione *Opzioni Internet* nel *Pannello di controllo* di Microsoft Windows. Una volta lanciata l'applicazione, nella sezione *Contenuto*, premendo il pulsante *Certificati* è possibile visualizzare i certificati presenti nello store. Nella sezione *Personale* si trovano i certificati di cui l'utente è in possesso della corrispondente chiave privata, in *Altri utenti* tutti i certificati di altre persone di cui si possiede solo la chiave privata:



Premendo il tasto destro sull'icona della barra delle applicazioni, apparirà un menu:



La voce **Avvio Automatico** può essere utilizzata per attivare o disattivare l'avvio di Smart Card Monitor nel momento della login a Windows. La voce **Esci** permette di chiudere l'applicazione Smart Card Monitor, mente la voce **Visualizza Certificati** permette di visualizzare tutti i certificati propagati nello store di Microsoft Windows e le informazioni sulla smart card su cui sono presenti:



Facendo doppio click su uno dei certificati, questi verrà visualizzato.

Rimuovendo la smart card dal lettore mentre l'applicazione Smart Card Monitor è in esecuzione, i certificati propagati dalla smart card vengono rimossi dallo store di Windows automaticamente.

Se si spegne il PC con la smart card inserita, o si chiude l'applicazione Smart Card Monitor con la smart card inserita, i certificati non verranno rimossi. In tal caso riavviando Windows senza la smart card inserita, nella posizione *Personale* dello store si potrebbero incontrare certificati *"orfani"*, in quanto per Windows risultano con chiave privata, ma in realtà non lo sono in quanto la smart card non è inserita. Per ovviare al problema, cancellarli manualmente o reinserire la smart card nel lettore.

4.1 Richiesta dei PIN

Durante il normale utilizzo della smart card, nel momento in cui si eseguono operazioni con oggetti protetti da PIN (solitamente le chiavi private dei certificati), Smart Card API richiederà l'inserimento del PIN da parte dell'utente.

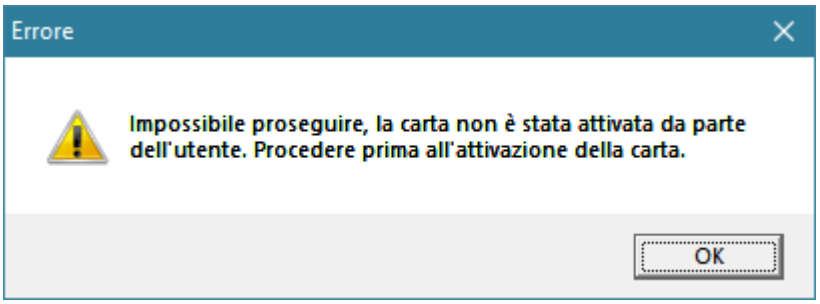
Al fine di agevolare la comprensione di quale PIN (Carta o Firma Digitale) e di quale carta tra quelle supportate il sistema sta chiedendo il PIN, Smart Card API rappresenta queste informazioni in modo chiaro all'interno della maschera di richiesta.

Tipo Carta	PIN Carta	PIN Firma
CMD-1		

Tipo Carta	PIN Carta	PIN Firma
CMCC		
CMD-2/Modello ATe (chip ST-Incard T&S 2048 CNS)		
CMD-2/CMCC-2/Modello ATe (chip Oberthur CNS COSMO ID/ONE v7 e IDEMIA CNS COSMO ID/ONE v9)		

Mentre per il PIN Carta, l'applicazione è in grado di ricordare il PIN immesso dall'utente per tutta la sessione di lavoro con un applicativo, per quanto riguarda il PIN Firma, l'utente può indicare anche per quante operazioni di firma dovrà essere ricordato prima di essere nuovamente richiesto all'utente. In questo modo l'utente ha sempre sotto controllo il numero di volte che la propria chiave di firma viene usata dall'applicativo durante una sessione di lavoro (nella finestra viene indicato nel campo **Per n. Firme**).

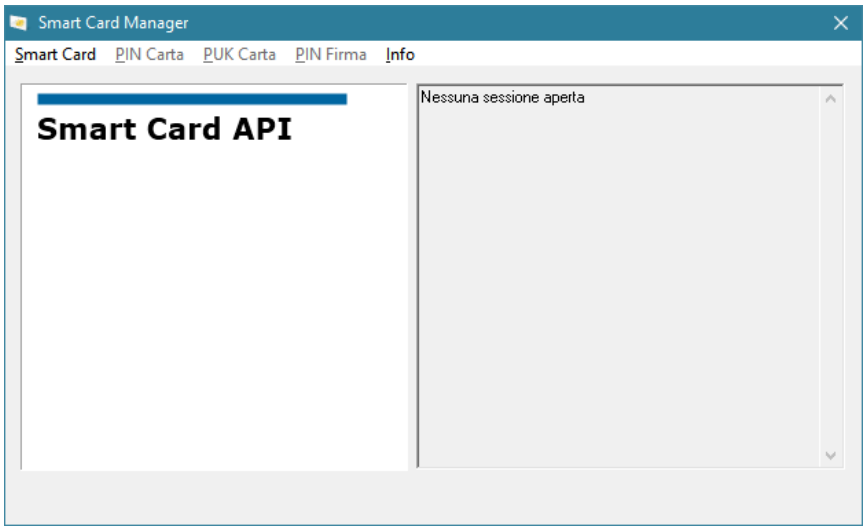
Una particolarità delle carte CMD-2 con chip Oberthur CNS COSMO ID/ONE v7 e IDEMIA CNS COSMO ID/ONE v9 rispetto alle altre è che se la carta non è stata attivata da parte dell'utente, non sarà possibile utilizzare tutti i certificati della carta (autenticazione, firma digitale e cifra/decifra), mentre con le vecchie non si poteva utilizzare solo la firma digitale. Se l'utente inavvertitamente usasse la carta senza attivarla, per evitare che all'utente vengano mostrati messaggi poco chiari, invece della richiesta di PIN Carta e/o PIN Firma, viene mostrato un messaggio di errore simile al seguente:



4.2 Applicazione di gestione della carta

Per gestire la propria smart card, Smart Card API fornisce una semplice applicazione, chiamata **Smart Card Manager**, che permette di gestire il PIN Carta, il PUK Carta e il PIN Firma.

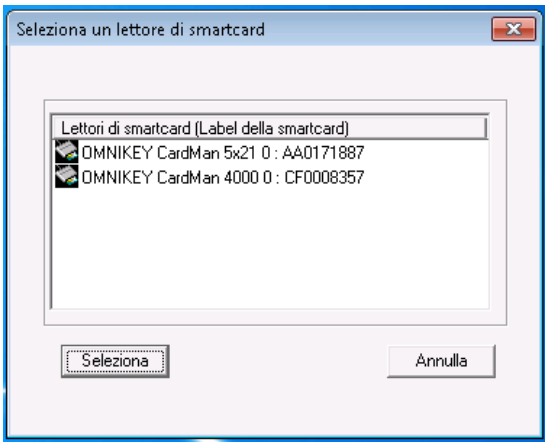
L'applicazione è eseguibile dal menu *Start*, *Tutti i programmi*, *Ministero Della Difesa - S.M.D. Comando C4*, *Smart Card Manager*. All'avvio l'applicazione si presenta nel seguente modo:



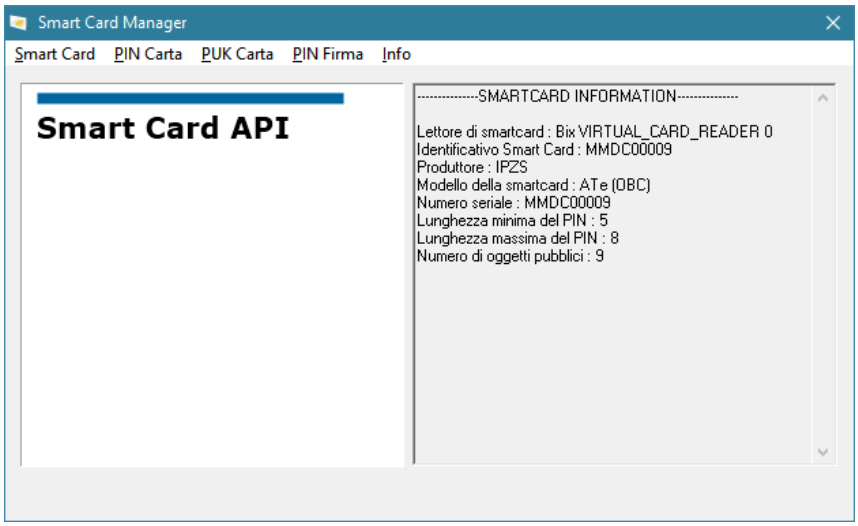
La versione dell'applicazione è visualizzabile in ogni momento dal menu *Info*, *Info su Card Manager*. Apparirà una finestra del tipo:

Prima di eseguire una qualunque operazione sulla smart card, è necessario aprire una sessione con essa, tramite il menu **Smart Card**, **Apri...**.

Nel caso ci fossero più carte presenti nei lettori di smart card, l'applicazione mostrerà una finestra per la selezione del lettore su cui eseguire ogni operazione:



A conferma dell'apertura della sessione, nella parte a sinistra della finestra appariranno le seguenti informazioni:

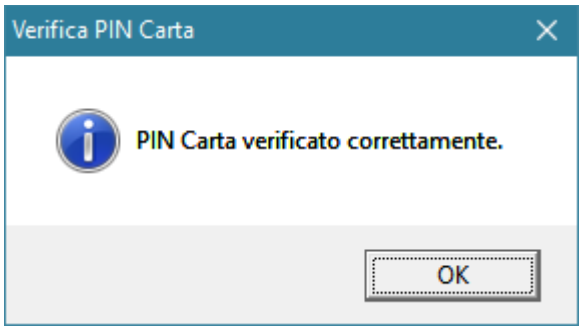


Per uscire dall'applicazione, premere il pulsante di chiusura in alto a destra (la X) oppure dal menu *Smart Card*, *Esci*.

4.2.1 Verifica PIN Carta

Dal menu *PIN Carta*, *Verifica/Login*:

Inserire il PIN Carta corretto e premere il tasto **Verifica**. In caso di PIN Carta corretto verrà mostrato il seguente messaggio:



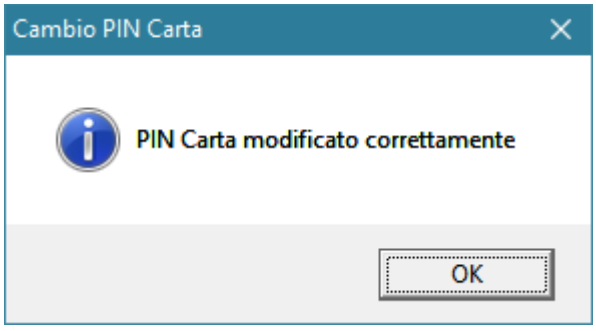
In caso invece di errore, verrà mostrata la descrizione dell'errore. Nel caso di eccessivi tentativi errati di verifica del PIN, quest'ultimo verrà bloccato e sarà necessario il suo sblocco tramite il PUK Carta.

Al termine dell'operazione, dal menu *PIN Carta*, eseguire *Logout*.

4.2.2 Cambio PIN Carta

Dal menu *PIN Carta*, *Cambia*:

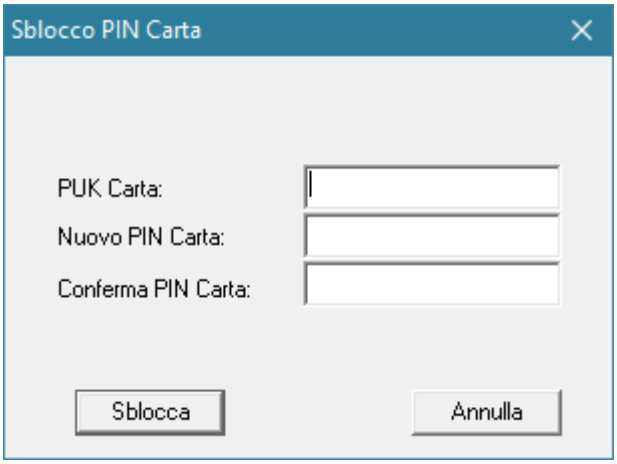
Inserire il vecchio PIN Carta e il nuovo PIN Carta (confermandolo). Quando terminato, premere il pulsante **Cambia** e in caso di successo apparirà un messaggio di conferma:



In caso di errore invece apparirà un messaggio che spiega la motivazione dell'errore. Nel caso di eccessivi tentativi errati di verifica del PIN, quest'ultimo verrà bloccato e sarà necessario il suo sblocco tramite il PUK Carta.

4.2.3 Sblocco PIN Carta

Dal menu *PIN Carta*, *Sblocca*:

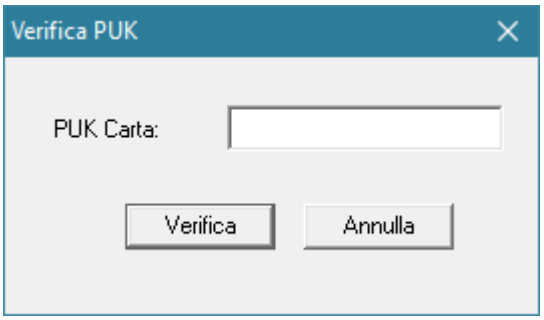


Inserire quindi il PUK Carta e il nuovo PIN Carta (confermandolo). Quando terminato, premere il pulsante **Sblocca**. In caso di successo, apparirà un messaggio di conferma:

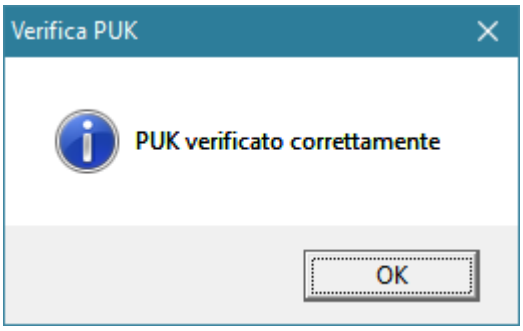
In caso di errore invece apparirà un messaggio che spiega la motivazione dell'errore. Nel caso di eccessivi tentativi errati di verifica del PUK, quest'ultimo verrà bloccato e la carta non sarà più utilizzabile.

4.2.4 Verifica PUK Carta

Dal menu *PUK*, *Verifica*:



Inserire il PUK Carta corretto e premere il tasto **Verifica**. In caso di PUK Carta corretto verrà mostrato il seguente messaggio:



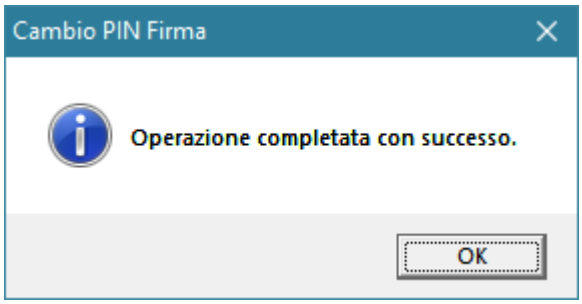
In caso di errore invece apparirà un messaggio che spiega la motivazione dell'errore. Nel caso di eccessivi tentativi errati di verifica del PUK, quest'ultimo verrà bloccato e la carta non sarà più utilizzabile.

4.2.5 Cambio PIN Firma

Dal menu *PIN Firma*, *Cambia PIN Firma*:

Inserire il PIN Carta corretto e premere il tasto **Verifica**. In caso di PIN Carta corretto verrà mostrata la schermata di cambio PIN Firma:

Inserire quindi il vecchio PIN Firma e il nuovo PIN Firma (confermandolo). Quando terminato, premere il pulsante **Cambia**. In caso di successo, apparirà un messaggio di conferma:



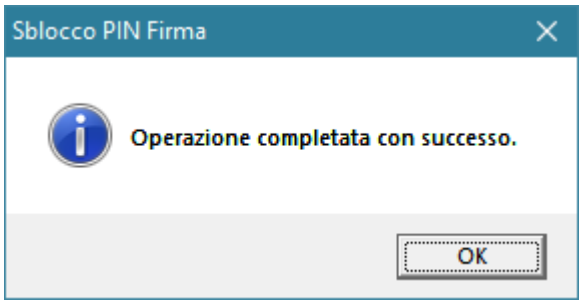
In caso di errore invece apparirà un messaggio che spiega la motivazione dell'errore. Nel caso di eccessivi tentativi errati di verifica del PIN Carta e PIN Firma, questi verranno bloccati e sarà necessario il loro sblocco rispettivamente tramite il PUK Carta e il PUK Firma.

4.2.6 Sblocco PIN Firma

Dal menu *PIN Firma*, *Sblocca PIN Firma*:

In caso positivo, apparirà la schermata per lo sblocco del PIN Firma:

Inserire quindi il PUK Firma e il nuovo PIN Firma (confermandolo). Quando terminato, premere il pulsante **Sblocca**. In caso di successo, apparirà un messaggio di conferma:



In caso di errore invece apparirà un messaggio che spiega la motivazione dell'errore.

4.3 Utilizzo della libreria PKCS#11

Per le applicazioni che utilizzano l'interfaccia PKCS#11 per l'accesso alla smart card, Smart Card API fornisce una libreria in standard PKCS#11. Il nome della libreria è **AtosSCAPIPKCS11.DLL** e si trova nei seguenti percorsi:

- Per sistemi Windows a 32 bit:
  - In `%SystemRoot%\System32\`
- Per sistemi Windows a 64 bit:
  - In `%SystemRoot%\System32\` per la versione a 64bit
  - In `%SystemRoot%\SysWOW64\` per la versione a 32bit

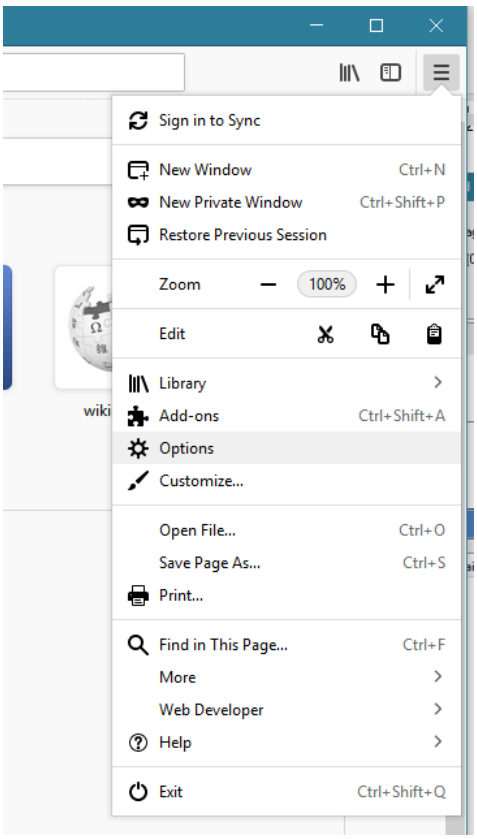
Per retrocompatibilità con la versione 2.0 delle API, la stessa libreria, ma con il vecchio nome **PKCS11.DLL** è presente negli stessi percorsi suddetti. Tuttavia, se possibile, si consiglia di utilizzare il nuovo nome.

Su sistemi operativi a 64bit si consiglia di non indicare il percorso assoluto della libreria PKCS#11 bensì di indicare, se possibile, solo il nome della libreria DLL in modo che sia Windows a scegliere la versione a 32 o 64 bit a seconda della versione dell'applicazione client.

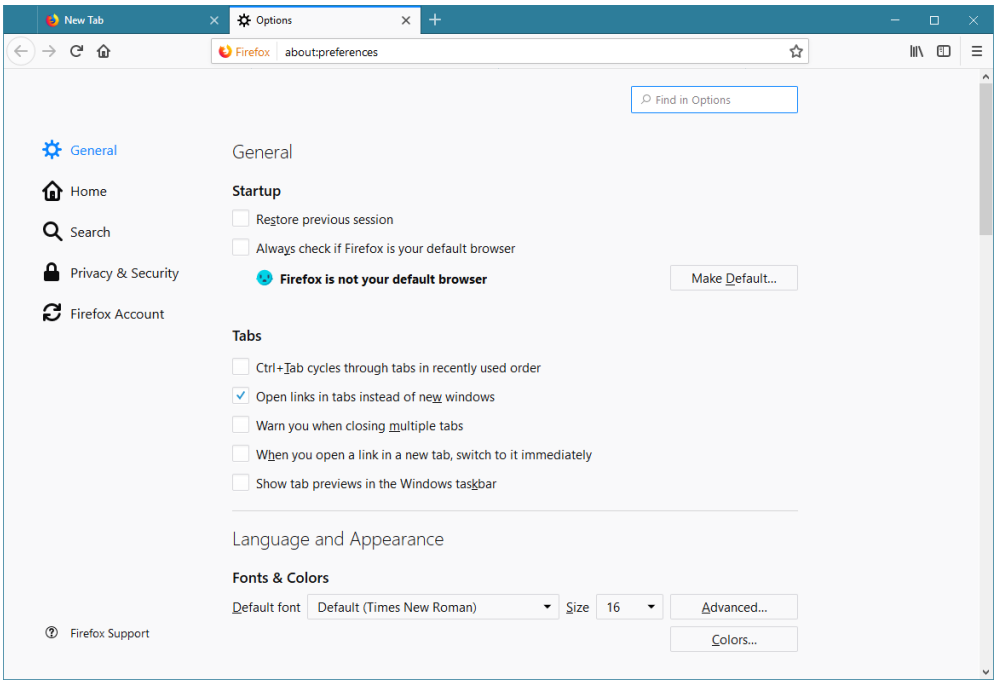
4.3.1 Utilizzo all'interno di Mozilla Firefox

Per poter utilizzare le smart card supportate da Smart Card API all'interno di Mozilla Firefox, è necessario configurare quest'ultimo in modo da utilizzare la libreria PKCS#11 AtosSCAPIPKCS11.dll. Le istruzioni nel seguito si riferiscono all'ultima release di Firefox disponibile nel momento della scrittura di questo documento, ovvero la 13.0.

Dopo aver lanciato Firefox, dal menu *"hamburger"* a destra:

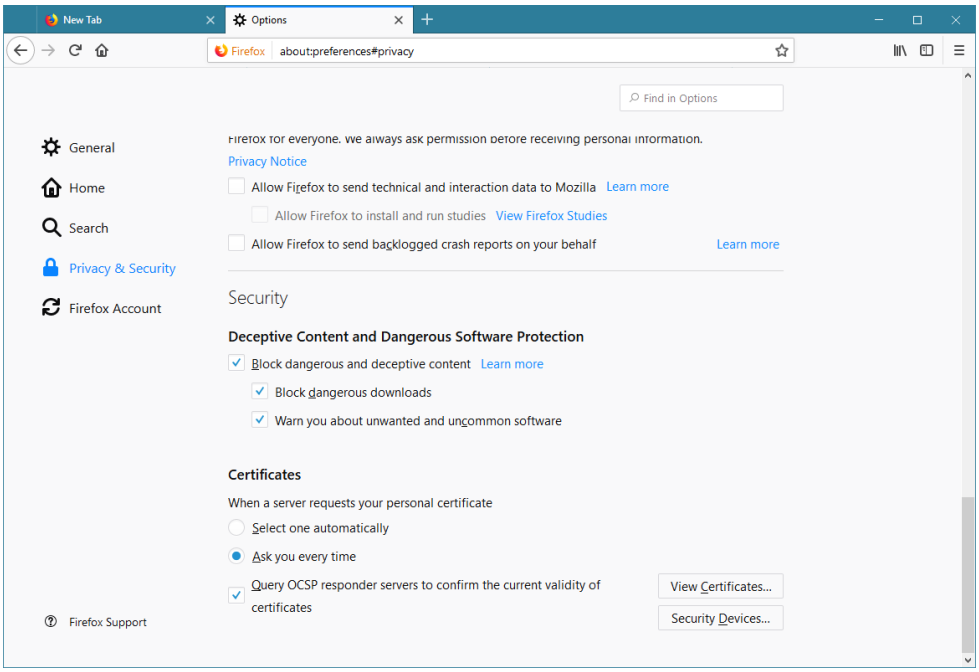


Accedere alle opzioni del browser *Options*. Apparirà la schermata delle opzioni:

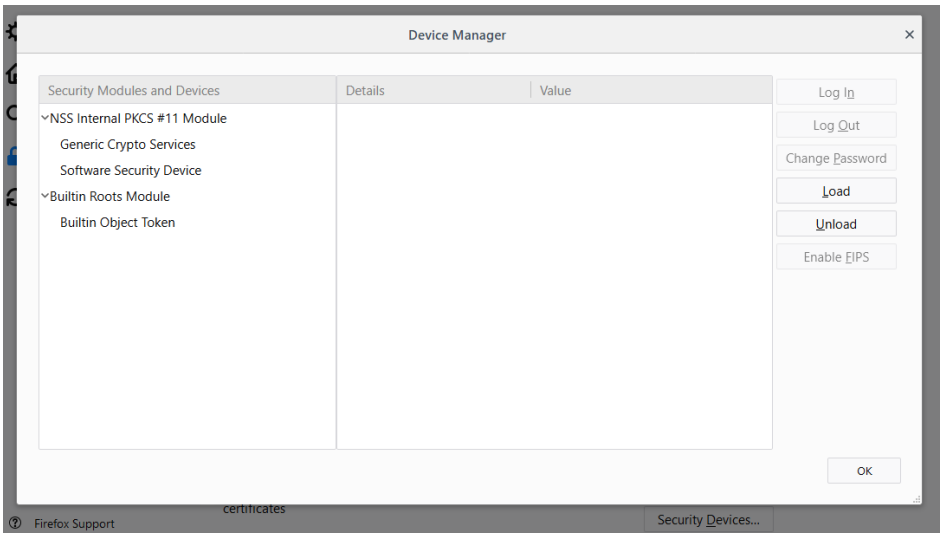


Selezionare la sezione **Privacy & Security**.

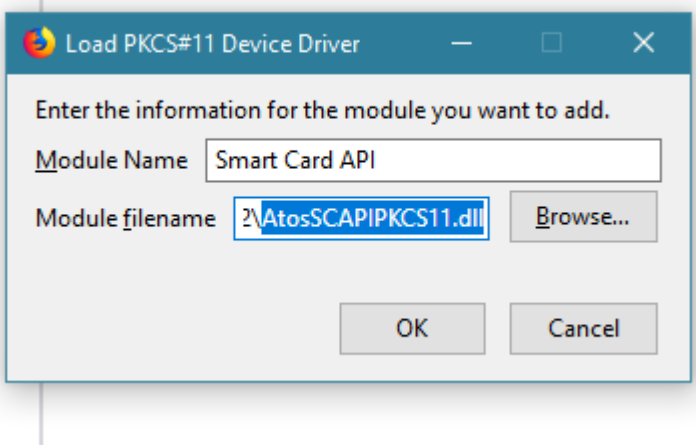
Scorrere la schermata fino in fondo verso la sezione **Security**, **Certificates** dove si trova il pulsante **Security Devices...**:



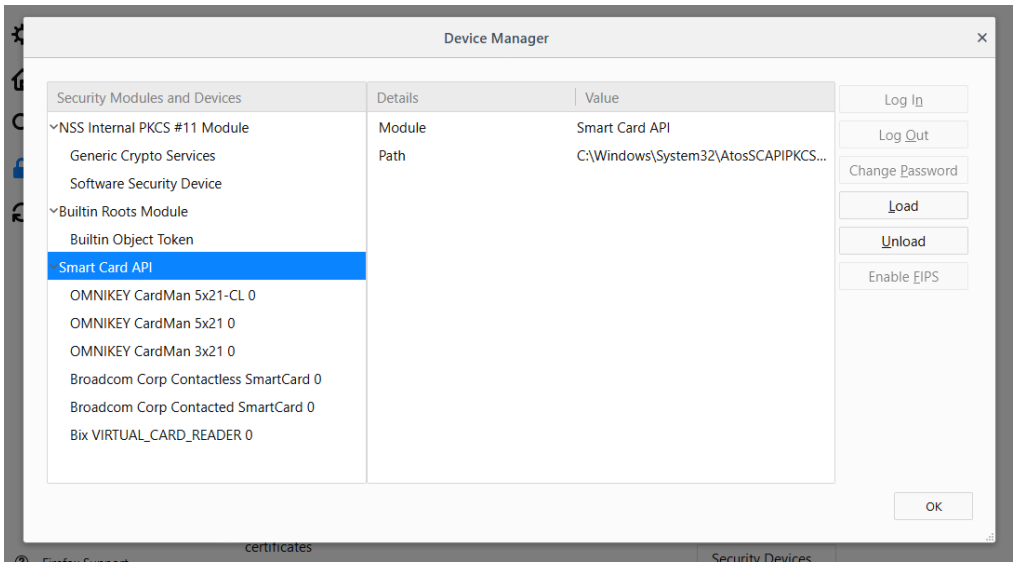
Premere il pulsante **Security Devices**, apparirà la schermata di configurazione dei dispositivi di sicurezza:



Premere il tasto **Load**, comparirà la schermata di inserimento delle informazioni sul PKCS#11:

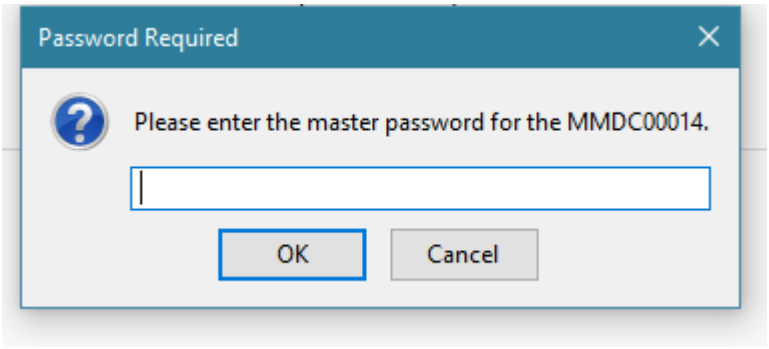


Inserire un nome per la libreria (ad esempio *Smart Card API*) e il percorso alla libreria PKCS#11 come indicato nella sezione 4.3 (tramite il tasto **Browse...**) e premere il tasto **OK**. Firefox caricherà quindi la libreria e la mostrerà nel seguente modo:



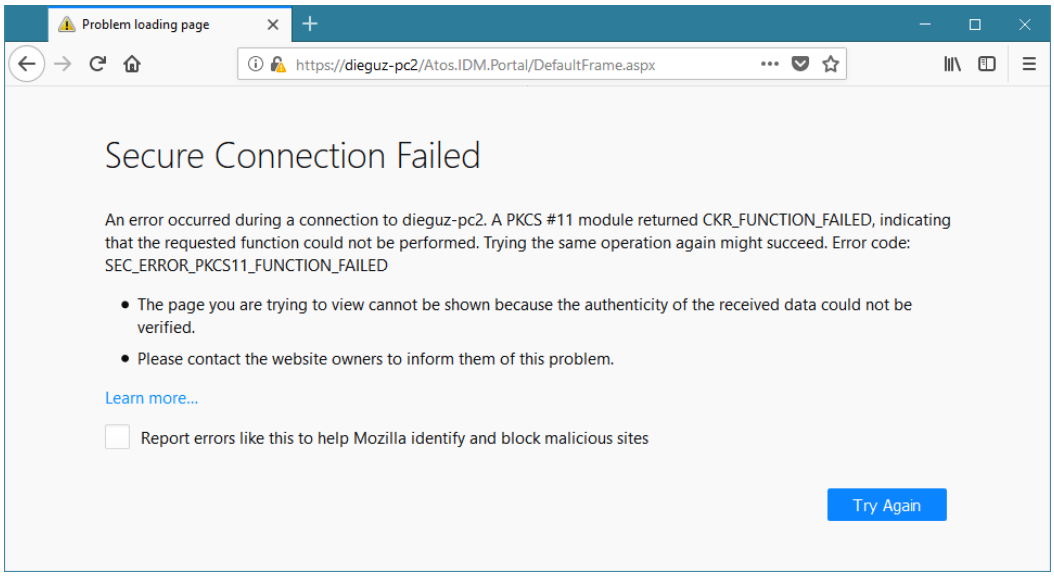
Tutte le carte inserite nei lettori verranno mostrate tramite la loro *Label* (ovvero l'ID Carta, AA0171887 nell'esempio), mentre i lettori vuoti verranno mostrati col loro nome. Una volta terminato premere il tasto **OK**.

Da questo momento in poi non sarà più necessario configurare la libreria PKCS#11 e ogni volta che si accederà a un sito web in HTTPS che richiede anche l'autenticazione client, una volta scelto il certificato da utilizzare tra quelli sulle smart card supportate, Firefox chiederà il PIN nel seguente modo:



Una volta inserito il PIN Carta e premuto il tasto **OK**, Firefox procederà con l'autenticazione sul sito web.

Una particolarità delle carte CMD-2 con chip Oberthur CNS COSMO ID/ONE v7 e IDEMIA CNS COSMO ID/ONE v9 rispetto alle altre è che se la carta non è stata attivata da parte dell'utente, non sarà possibile utilizzare il certificato di autenticazione. L'errore mostrato da Firefox sarà simile a quello mostrato nella schermata successiva, ovvero **CKR_FUNCTION_FAILED**:



4.4 Utilizzo del CSP

Smart Card API mette a disposizione l'accesso alla smart card tramite l'interfaccia Microsoft Smart Card Cryptographic Service Provider (CSP). Il nome del CSP installato è **Atos Smart Card API CSP**.

Grazie all'interfaccia CSP, tutte le applicazioni Windows che rispettano tale standard, sono in grado di utilizzare i certificati presenti sulle smart card supportate e propagati nello store di Microsoft Windows.

5 Configurazione di Smart Card API

5.1 Opzioni della libreria PKCS#11

La configurazione del sottosistema PKCS#11 di Smart Card API avviene attraverso il file di configurazione XML **AtosSCAPIPKCS11.xml** presente nei seguenti percorsi:

- Per sistemi Windows a 32 bit:
  - In `%SystemRoot%\System32\`
- Per sistemi Windows a 64 bit:
  - In `%SystemRoot%\System32\` per la versione a 64bit
  - In `%SystemRoot%\SysWOW64\` per la versione a 32bit

Si consiglia di non modificare le voci a meno di quelle relative ai log, le quali vengono trattate nel dettaglio nella seguente sezione 5.3.

Tra le opzioni che potrebbero essere di interesse all'utente finale, l'opzione **KEYUSECOUNT** (relativo ai vari nodi TEMPLATE sotto CONFIG\TEMPLATES\) permette di indicare il valore iniziale che compare nella finestra di immissione del PIN Firma come valore per il numero di operazioni di firma digitale per cui tenere in cache il PIN di Firma prima di richiederlo all'utente. Tale valore può essere modificato dall'utente sulla finestra per le prossime n firme.

Si tenga conto che, per le operazioni di firma digitale, è opportuno suggerire all'utente che tale valore sia sempre pari a 1 (uno) in quanto è opportuno essere sicuri che l'utente abbia coscienza delle volte in cui venga usata la propria chiave di firma. In condizioni in cui si fa la cache del PIN di Firma, un software di tipo malware, infatti, potrebbe far firmare a insaputa dell'utente più di un documento elettronico.

5.2 Opzioni del CSP

La configurazione del sottosistema PKCS#11 di Smart Card API avviene attraverso il file di configurazione XML **AtosSCAPIWindows.ini** presente nei seguenti percorsi:

- Per sistemi Windows a 32 bit:
  - In `%SystemRoot%\System32\`
- Per sistemi Windows a 64 bit:
  - In `%SystemRoot%\System32\` per la versione a 64bit
  - In `%SystemRoot%\SysWOW64\` per la versione a 32bit

Il contenuto del file di configurazione è simile al seguente:

```
[CSP]
CSPModule=AtosSCAPICSPModule.dll
CSPName=Atos Smart Card API CSP
CSPContainer=AtosSCAPICSPContainer.dll
PKCS11DLL=AtosSCAPIPKCS11.dll
LogLevel=0
LogPath=%TEMP%
ToolTip=Atos SC API Card Monitor v3.0.0.0
```

Si consiglia di non modificare le voci a meno di LogLevel e LogPath, le quali vengono trattate nel dettaglio nella seguente sezione 5.3.

5.3 Gestione dei log

5.3.1 Log PKCS#11

La configurazione del log per le operazioni del CSP è **AtosSCAPIPKCS11.xml** presente nei percorsi indicati nella sezione 5.1.

La sezione relativa ai log è rappresentata nella seguente immagine:

```
<CONFIG>
    <LOG ENABLED="0" MODE="SINGLE">
        <DIR>%TEMP%</DIR>
        <FUNCTION ENABLED="1" DEPTH="5"></FUNCTION>
        <PARAM ENABLED="1"></PARAM>
        <MODULES>
            <MODULE NAME="P11MDLL" ENABLED="1"></MODULE>
            <MODULE NAME="UTILLIB" ENABLED="1"></MODULE>
            <MODULE NAME="ASN1LIB" ENABLED="0"></MODULE>
            <MODULE NAME="CARDINT" ENABLED="1"></MODULE>
            <MODULE NAME="P11CNSA" ENABLED="1"></MODULE>
            <MODULE NAME="P11CMD1" ENABLED="1"></MODULE>
            <MODULE NAME="P11CMCC" ENABLED="1"></MODULE>
            <MODULE NAME="CRYPTOL" ENABLED="1"></MODULE>
            <MODULE NAME="P11OBJT" ENABLED="1"></MODULE>
        </MODULES>
        <THREADS></THREADS>
    </LOG>
```

Il tag **LOG** contiene le seguenti opzioni:

- **ENABLED** attiva (**1**) o disattiva (**0**) globalmente il sistema di registrazione dei log
- **MODE** indica la tipologia di registrazione dei log:
  - **SINGLE**: un solo file di log per tutti I moduli e tutti i thread (YYYY_MM_DD_AtosSCAPIPkcs11.log)
  - **MODULE**: un file di log per ogni modulo (YYYY_MM_DD_MODULE_AtosSCAPIPkcs11.log)
  - **THREAD**: un file di log per ogni thread (YYYY_MM_DD_THREAD_AtosSCAPIPkcs11.log)
  - **MODULE THREAD**: un file di log per ogni thread e per ogni modulo (YYYY_MM_DD_MODULE_THREAD_AtosSCAPIPkcs11.log)

Il tag **DIR** indica la directory in cui salvare i file di log. Può essere un percorso assoluto o il valore %TEMP% che punterà al percorso temporaneo di Windows.

Il tag **PARAM** contiene le seguenti opzioni:

- **ENABLED** attiva (**1**) o disattiva (**0**) la registrazione dei parametri delle funzioni nei file di log

I vari tag **MODULE** contengono le seguenti opzioni:

- **NAME** indica il nome del sottosistema di log
- **ENABLED** attiva (**1**) o disattiva (**0**) la registrazione dei log per il corrispondente sottosistema

I vari sottosistemi che scrivono voci di log sono i seguenti:

Codice	Descrizione
P11MDLL	Libreria PKCS#11 principale
UTILLIB	Libreria con le funzioni di utility
ASN1LIB	Parser ASN.1
CARDINT	Interfaccia PC/SC a basso livello con la smart card
P11CMD1	Libreria PKCS#11 relativa alla carta CMD-1
P11CMCC	Libreria PKCS#11 relativa alla carta CMCC
P11CMD2	Libreria PKCS#11 relativa alla carta CMD-2/Modello ATe (chip ST-Incard T&S 2048 CNS)
P11ATEO	Libreria PKCS#11 relativa alla carta CMD-2/CMCC-2/Modello ATe (chip Oberthur CNS COSMO ID/ONE v7 e IDEMIA CNS COSMO ID/ONE v9)
CRYPTOL	Funzioni crittografiche
P11OBJT	Contenitore degli oggetti PKCS#11

I file di log del PKCS#11 vengono salvati con un nome file nel formato **YYYY-MM-DD_AtosSCAPIPkcs11.log** dove **YYYY** indica l'anno del giorno in cui è stato prodotto il file di log, **MM** il mese, **DD** il giorno.

Per visualizzare il contenuto del file di log, utilizzare un normale editor di testo. Un esempio del contenuto del file è il seguente:

```
00091:[ 17:45:49.999 ] | PID=6800 | 3492 | P11MDLL |  OUT -> p11::CSlot::InitSlotList (36)
00092:[ 17:45:50.003 ] | PID=6800 | 6388 | CARDINT |  CCardContext::getContext ret:0 (line
39)
00093:[ 17:45:50.005 ] | PID=6800 | 3492 | P11MDLL |  C_Initialize ret:0 (line 331)
00094:[ 17:45:50.008 ] | PID=6800 | 6388 | CARDINT | OUT -> CCardContext::getContext (92)
00095:[ 17:45:50.011 ] | PID=6800 | 3492 | P11MDLL | OUT -> C_Initialize (8)
00097:[ 17:45:50.018 ] | PID=6800 | 7164 | P11MDLL | Fatto qualcosa in DllMain()
00098:[ 17:45:50.034 ] | PID=6800 | 7164 | P11MDLL | IN -> C_GetSlotList
param (00099): 0
param (00099): 0066AB3C(0)
param (00099): 0066AB38(16)
00099:[ 17:45:50.048 ] | PID=6800 | 7164 | P11MDLL |  C_GetSlotList ret:0 (line 270)
00100:[ 17:45:50.052 ] | PID=6800 | 7164 | P11MDLL | OUT -> C_GetSlotList (99)
00101:[ 17:45:50.055 ] | PID=6800 | 7164 | P11MDLL | IN -> C_GetSlotInfo
```

La prima colonna indica il progressivo numerico, la seconda colonna (tra [ ]) indica l'ora (al millisecondo) a cui si riferisce la voce di log. Segue il Process ID dell'applicazione che sta utilizzando la libreria PKCS#11 di Smart Card API. Segue poi il sottosistema della libreria PKCS#11 che sta registrando la voce di log. Infine, l'ultima colonna riporta il messaggio descrittivo della voce di log.

5.3.2 Log CSP

La configurazione del log per le operazioni del CSP è **AtosSCAPIWindows.ini** presente nei percorsi indicati nella sezione 5.2.

```
1 [CSP]
2 CSPModule=AtosSCAPICSPModule.dll
3 CSPName=Atos Smart Card API CSP
4 CSPContainer=AtosSCAPICSPContainer.dll
5 PKCS11DLL=AtosSCAPIPKCS11.dll
6 LogLevel=0
7 LogPath=%TEMP%
8 ToolTip=Atos SC API Card Monitor v3.0.0.0
```

- **LogLevel** permette di attivare (**1**) o disattivare (**0**) i messaggi di log
- **LogPath** permette di indicare la directory in cui salvare i file di log. Si consiglia di indicare il valore **%TEMP%** in modo che vengano scritti nella directory temporanea dell'utente (soprattutto su sistemi Windows post Vista).

I file di log del CSP vengono salvati con un nome file nel formato **YYYY-MM-DD_AtosSCAPICsp.log** dove **YYYY** indica l'anno del giorno in cui è stato prodotto il file di log, **MM** il mese, **DD** il giorno.

Per visualizzare il contenuto del file di log, utilizzare un normale editor di testo. Un esempio del contenuto del file è il seguente:

```
[ 2012-06-11 17:45:49.421 ] PID=6800 | CSPILB | IntroLibrary constructed
[ 2012-06-11 17:45:49.441 ] PID=6800 | CSPILB | -> InitializeP11
[ 2012-06-11 17:45:50.055 ] PID=6800 | CSPMON | do_thread() C_GetSlotList ...
[ 2012-06-11 17:45:50.108 ] PID=6800 | CSPMON | for() C_GetSlotInfo returned 0x0
[ 2012-06-11 17:45:50.109 ] PID=6800 | CSPMON | Added (3,OMNIKEY CardMan ...
[ 2012-06-11 17:45:50.162 ] PID=6800 | CSPMON | for() C_GetTokenInfo returned 0xe0
...
```

La prima colonna (tra [ ]) indica la data e l'ora (al millisecondo) a cui si riferisce la voce di log. Segue il Process ID dell'applicazione che sta utilizzando il CSP di Smart Card API. Segue poi il sottosistema del CSP che sta registrando la voce di log. Infine, l'ultima colonna riporta il messaggio descrittivo della voce di log.

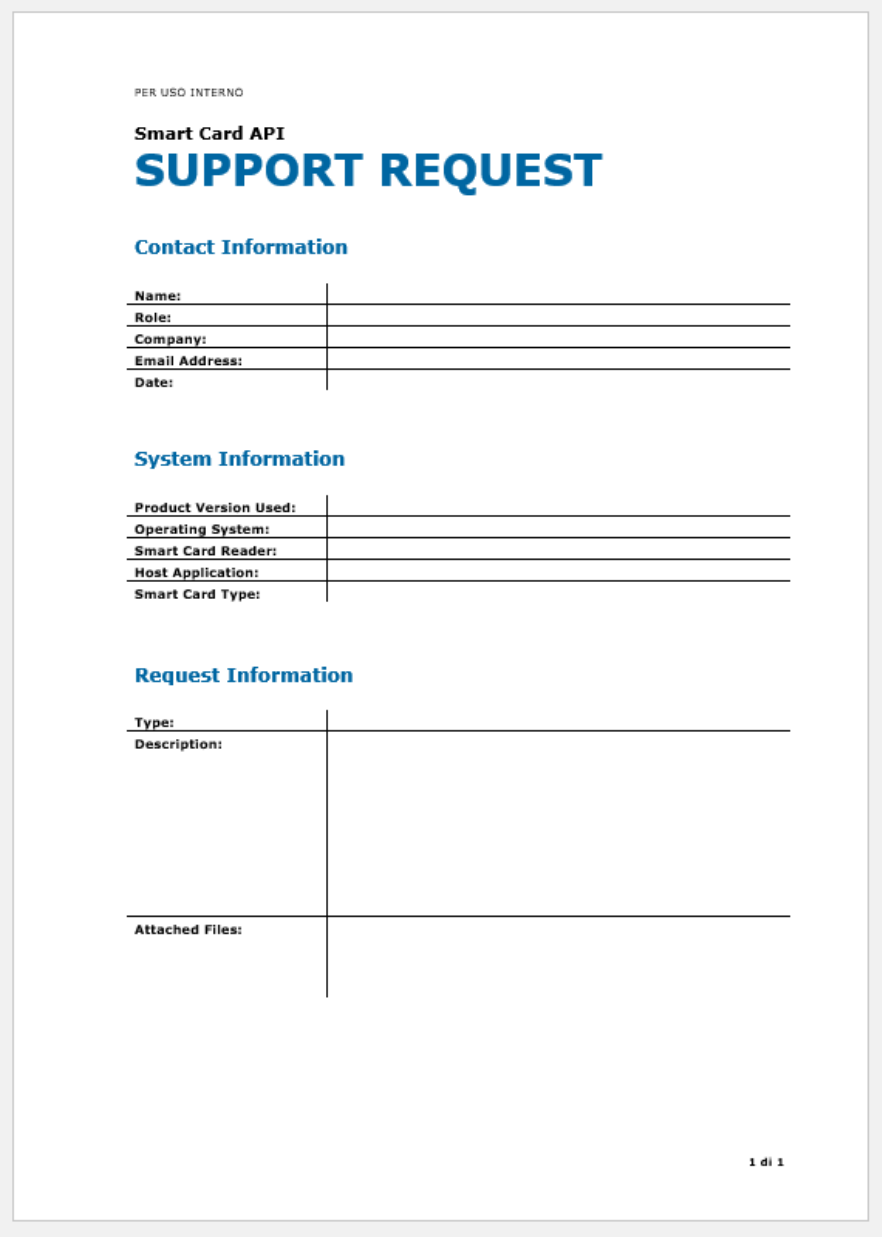
I vari sottosistemi che scrivono voci di log sono i seguenti:

Codice	Descrizione
CSPMON	Applicazione di monitoraggio della carta (Smart Card Monitor)
CSPCNT	Sistema contenitore dei certificati propagati
CSPMOD	Libreria che implementa l'interfaccia CSP di Microsoft
CSPILB	Sistema di propagazione dei certificati nello store di Microsoft Windows

6 Come ottenere supporto su Smart Card API

Per ottenere supporto dal team di supporto e/o sviluppo di Smart Card API, è necessario compilare correttamente il modulo allegato a questo documento (**Smart Card API Support.doc**).

Il modulo ha il seguente formato:



PER USO INTERNO

Smart Card API

SUPPORT REQUEST

Contact Information

Name:	
Role:	
Company:	
Email Address:	
Date:	

System Information

Product Version Used:	
Operating System:	
Smart Card Reader:	
Host Application:	
Smart Card Type:	

Request Information

Type:	
Description:	
Attached Files:	

1 di 1

Campi	Descrizione	Esempio
Name	Il nome della persona (o del punto di distribuzione) che richiede supporto	Mario Rossi

Campi	Descrizione	Esempio
Role	Il ruolo nell'utilizzo di Smart Card API, giocato dalla persona che invia il modulo di supporto (es. sviluppatore, utente finale….)	Sviluppatore
Company	Specificare il nome della compagnia (o il particolare dipartimento) nel quale lavora la persona che richiede il supporto	Ministero della Difesa
Email Address	Indirizzo Email per ricevere risposte dal team di sviluppo e/o supporto	mario.rossi@difesa.it
Date	La data in cui si è verificato il problema o la richiesta	15/01/2012
Product version used	La versione di Smart Card API usata	3.10.0000
Operating System	Il sistema operativo usato (indicare in modo preciso la Service Pack usata e se a 32 o 64 bit)	Windows XP Professional SP3 32bit
Smart Card Reader	Lettore di Smart Card usato	Precise Biometrics 200 MC
Host application	L'applicazione che si stava utilizzando quando si è verificato il problema	Internet Explorer 8.0
Smart Card Type	La tipologia di smart card usata (indicare uno dei modelli riportati nella sezione 2.1)	CMD-2 / Modello ATe (chip ST-Incard T&S 2048 CNS)
Type	Tipo di segnalazione: Errore, Nuova Funzionalità, Consigli	
Description	Descrizione del problema. Descrivere in dettaglio la situazione nella quale è apparso il problema e tutti i suoi effetti	*Il software non permette la firma di un documento tramite smart card*
Attached files	File di log, file di configurazione e qualunque altro file si ritiene utile ai fini della risoluzione di un problema. Per i file di log fare riferimento alla sezione 5.3 e se possibile alla sezione 6.1	

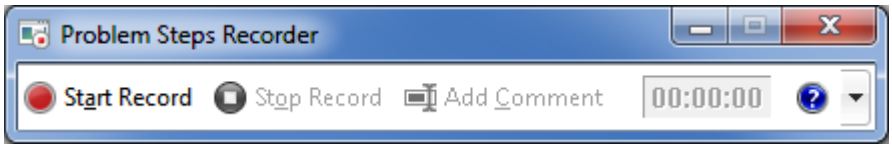
Nel caso di segnalazione di errori, si consiglia di allegare sempre quanti più log possibili e quante più informazioni possibili a disposizione. Nel caso di problemi con applicazioni di terze parti per le quali è possibile produrre un file di log, si consiglia di allegare anche quest'ultimo al fine di agevolare la comprensione del processo di utilizzo di Smart Card API.

Inviare il modulo di supporto e i file allegati per e-mail (o comunque in formato elettronico) al proprio contatto di supporto di primo livello, il quale dopo un'attenta analisi, se non in grado di risolvere il problema, procederà a inoltrare il tutto al team di supporto di secondo livello e/o agli sviluppatori del prodotto Smart Card API.

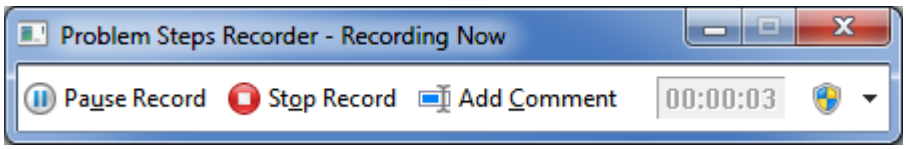
6.1 Registrare una sessione di lavoro su Windows 7

Nel caso si esegua Smart Card API su un sistema operativo Microsoft Windows 7 o superiore, è consigliato l'utilizzo dello strumento **Problem Steps Recorder** (PSR) di Windows per la registrazione delle sessioni di lavoro.

Nel caso di un errore ricorrente, attivare i log PKCS#11 e CSP di Smart Card API e attivare l'applicazione Problem Steps Recorder lanciando il comando **psr.exe** dal menu *Start*, *Esegui*, apparirà la seguente schermata:



Quando si è pronti per registrare, avviare la registrazione con **Start Record** ed eseguire tutti i passi con le applicazioni che poi portano al verificarsi dell'errore. Durante la registrazione, l'applicazione indicherà il tempo di registrazione a destra:



Quando si ritiene di aver terminato la registrazione, premere il pulsante **Stop Recording**. L'applicazione PSR chiederà di salvare la registrazione con un nome in un percorso a scelta. Indicare il nome e il percorso e allegare il file ZIP prodotto ai file di log della segnalazione di errore. La registrazione contiene informazioni molto utili alla risoluzione del problema da parte del team di sviluppo e/o supporto.

6.2 Soluzioni a problemi noti

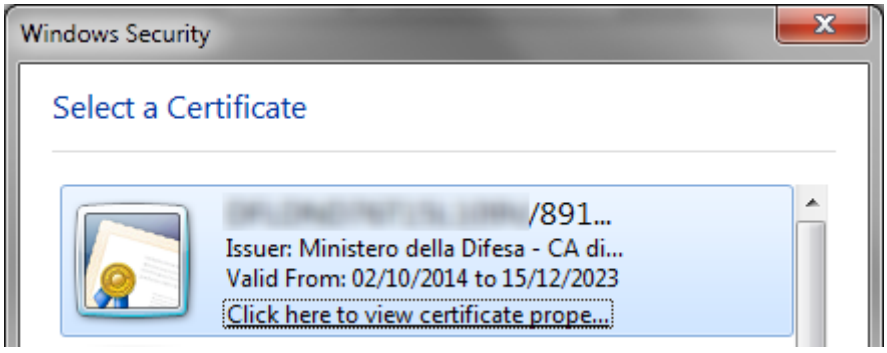
6.2.1 Problemi con Internet Explorer

IMPOSSIBILE ACCEDERE IN HTTPS CON CERTIFICATO (1° CASO)

Il momento della scelta del certificato può già mostrare un comportamento scorretto del software Internet Explorer:

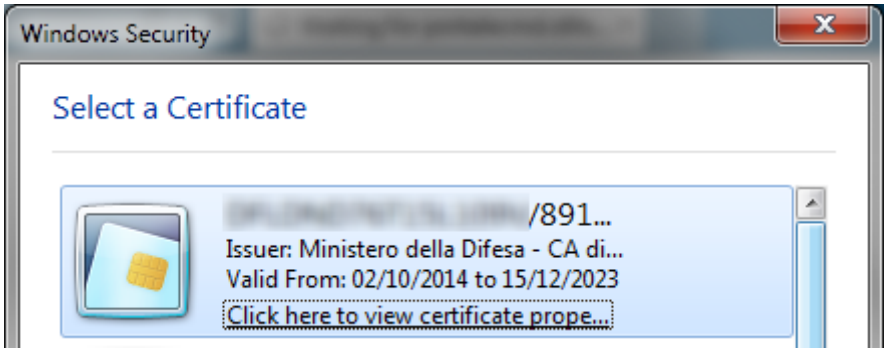
SCORRETTO

Il certificato della carta viene mostrato come un normale certificato installato su PC



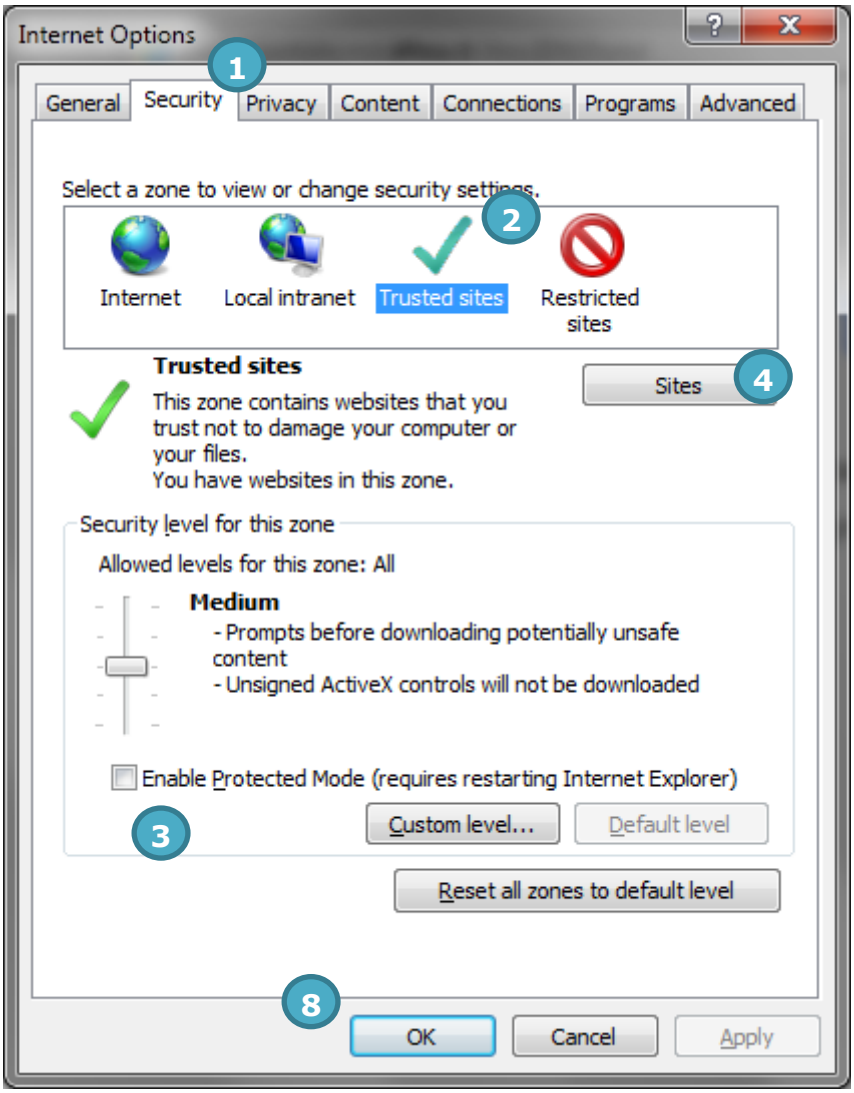
CORRETTO

Il certificato della carta viene mostrato come effettivamente presente sulla smart card

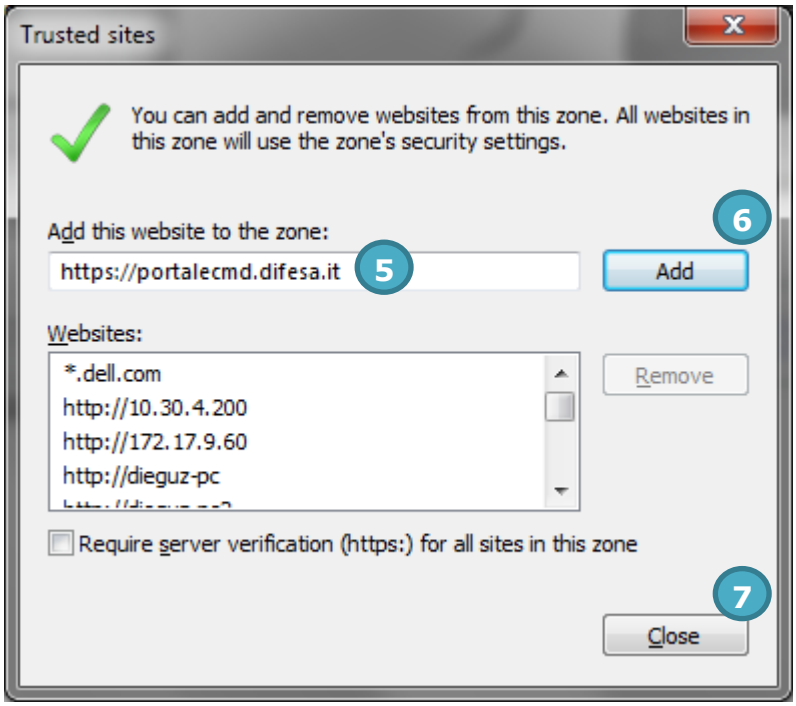


Per risolvere il problema, è necessario che il sito web a cui ci si sta collegando, sia presente nei *Siti Attendibili* (*Trusted sites*) e che per la zona Siti Attendibili sia disabilitata l'opzione *Attiva modalità protetta* (*Enable Protected Mode*).

Dalle **Opzioni Internet** (**Internet Options**), selezionare il tab *Sicurezza* (*Security*), selezionare l'icona *Siti attendibili* (*Trusted sites*), deselezionare *Attiva modalità protetta* (*Enable Protected Mode*):



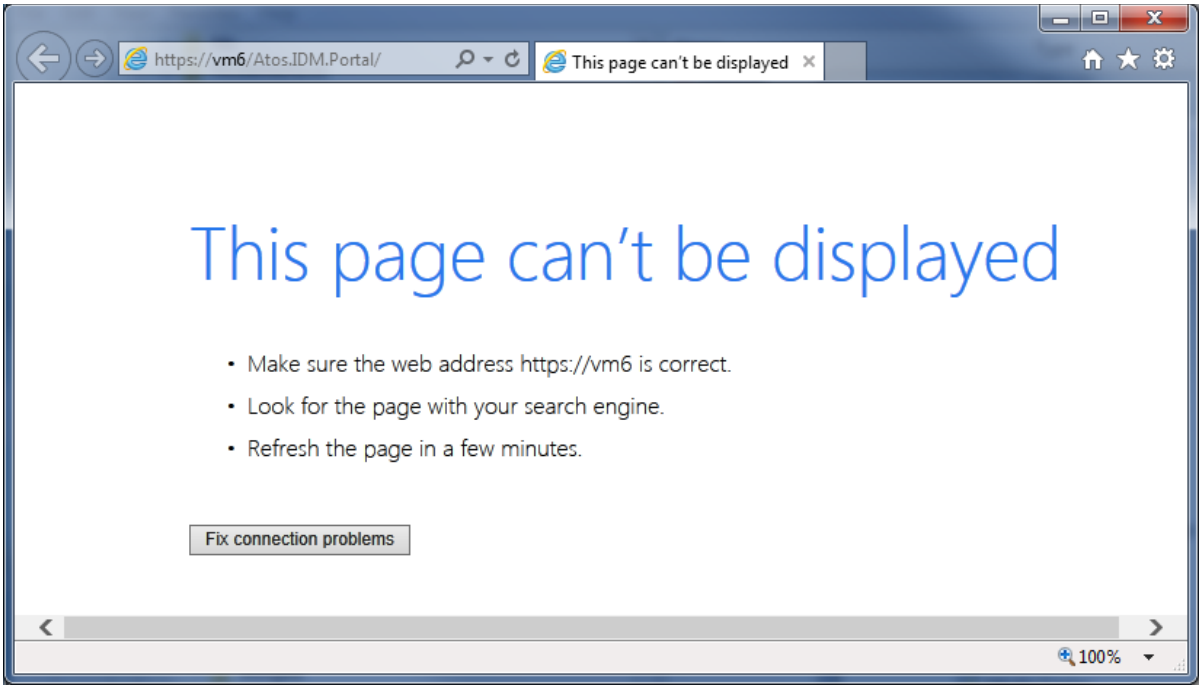
Premere il pulsante *Siti* (*Sites*):



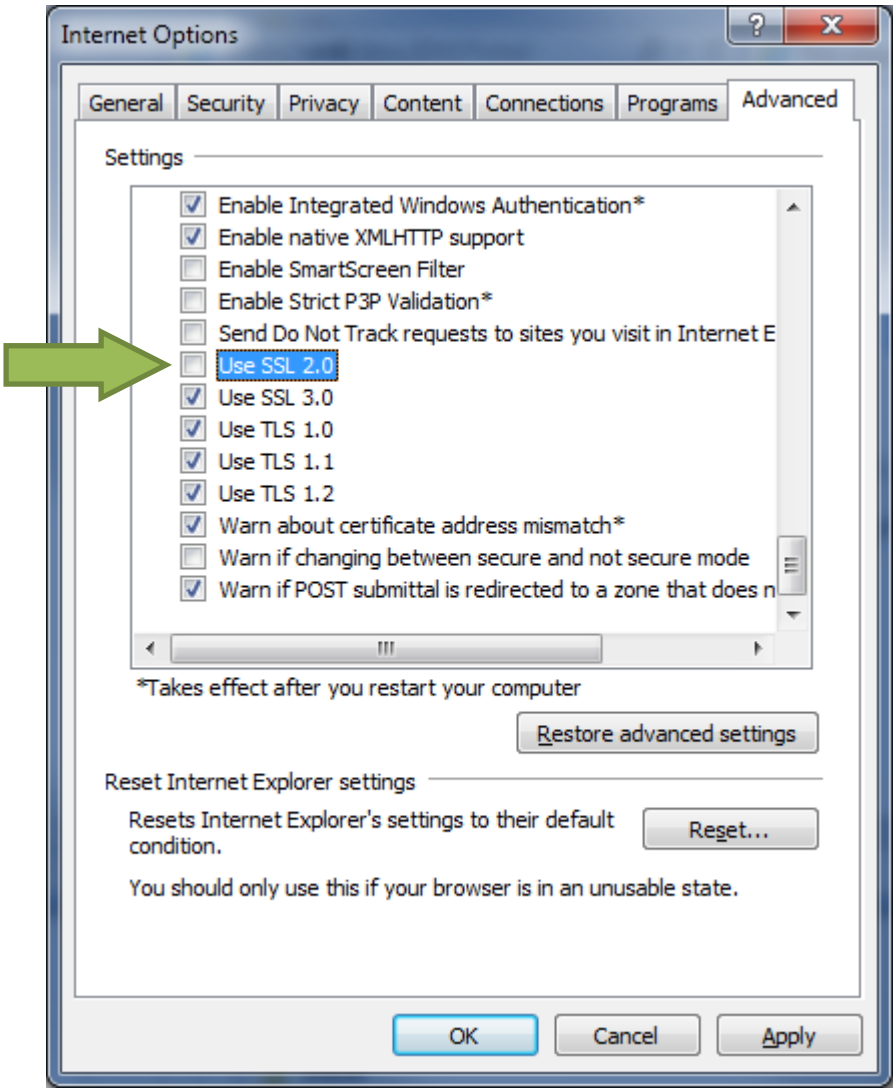
Indicare l'URL completa o solo la parte iniziale del sito da aggiungere (comprensivo della specificazione del protocollo (**https://**), premere il tasto *Aggiungi* (*Add*) e poi *Chiudi* (*Close*). Si tornerà alla schermata precedente dove si potrà premere il tasto *OK*. A questo punto riavviare Internet Explorer (facendo attenzione a chiudere tutte le finestre eventualmente aperte).

IMPOSSIBILE ACCEDERE IN HTTPS CON CERTIFICATO (2° CASO)

Nelle ultime versioni di Windows, la Microsoft ha deprecato l'utilizzo dello standard SSL versione 2.0: nel caso un'applicazione cerchi di utilizzare questa versione dello standard, all'applicazione viene vietato l'utilizzo di un certificato provocando un errore simile al seguente:



Per risolvere il problema con Internet Explorer, aprire le opzioni di Internet di Windows (*Start, Pannello di Controllo, Opzioni Internet, Avanzate*, oppure *Start, Control Panel, Internet Options, Advanced*) e disattivare **SSL 2.0** come di seguito mostrato:

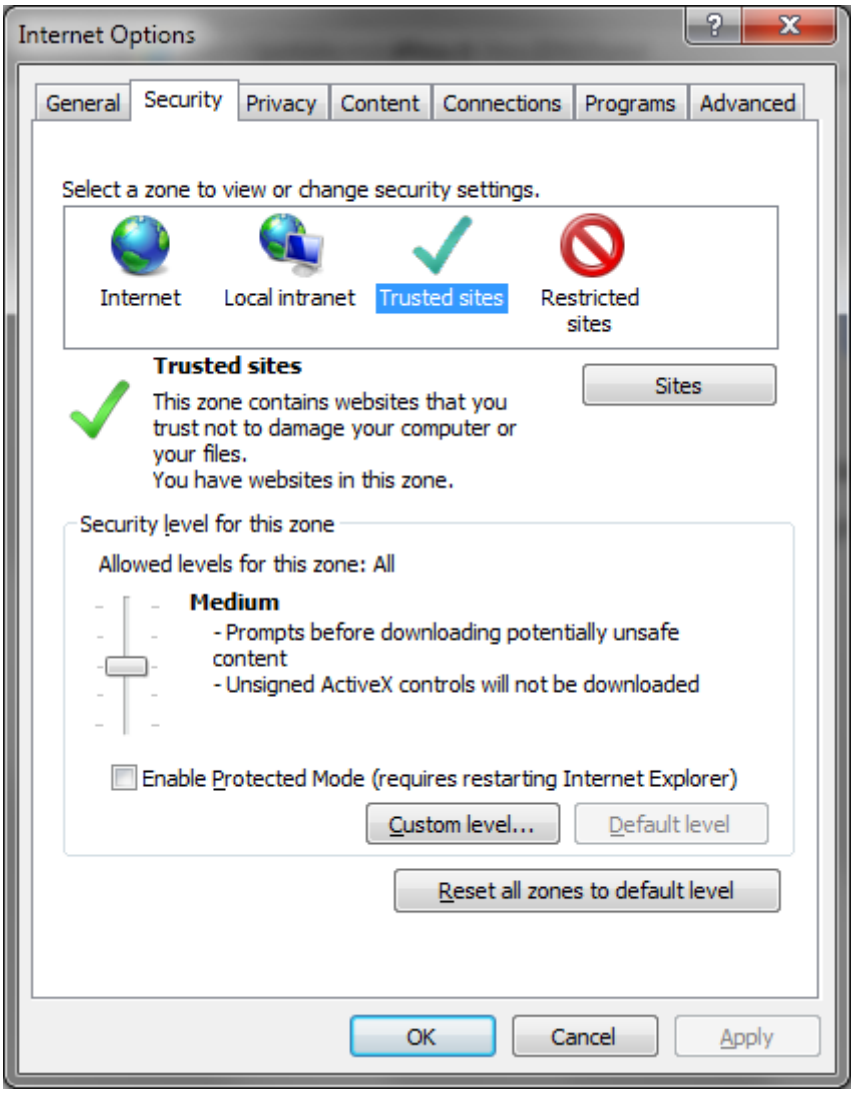


IMPOSSIBILE ACCEDERE IN HTTPS CON CERTIFICATO (3° CASO – PORTALI PUBBLICA AMMINISTRAZIONE)

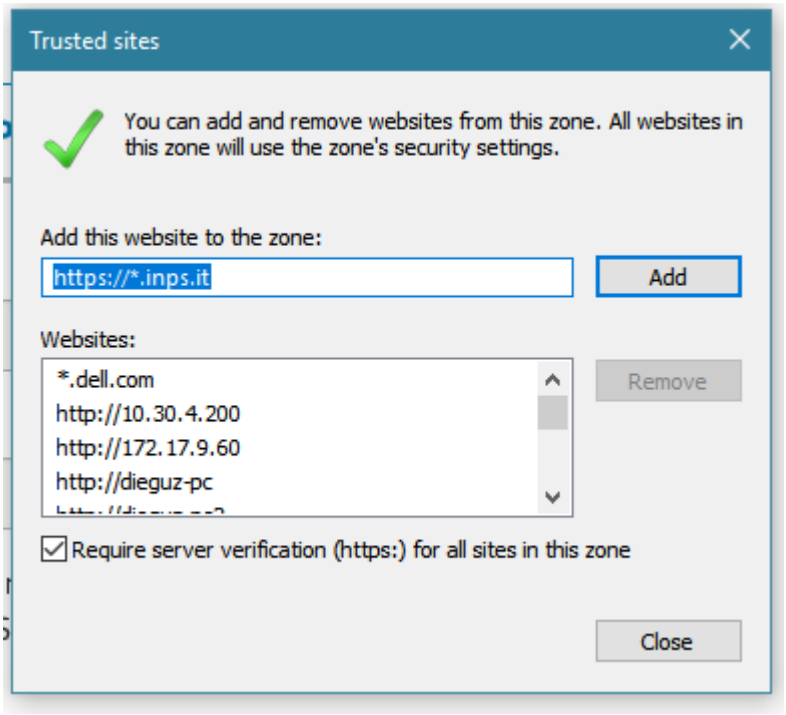
Alcuni portali web della pubblica amministrazione utilizzano un meccanismo di autenticazione che coinvolge tramite redirect più di un sottodominio dello stesso dominio di base (ad esempio www.inps.it, serviziweb2.inps.it, portal.inps.it). Per la mutua autenticazione, Internet Explorer su Windows richiede che tutti questi sottodomini siano presenti tra la lista dei siti attendibili, altrimenti la login fallirà.

Il problema si presenta solitamente nel seguente modo: l'utente dopo aver scelto la login con smart card e il certificato di autenticazione, invece di venirgli richiesto il PIN Carta, il portale ridirige su una pagina di errore 403 oppure viene richiesto il PIN Carta ma poi il browser ritorna sempre sulla stessa pagina.

Per risolvere il problema con Internet Explorer, dalle **Opzioni Internet** (**Internet Options**), selezionare il tab *Sicurezza* (*Security*), selezionare l'icona *Siti attendibili* (*Trusted sites*):



Premere il pulsante *Siti* (*Sites*) e aggiungere il sito non funzionante sostituendo la parte iniziale dell'indirizzo **www** con un ***** (asterisco). Ad esempio, invece di aggiungere https://www.inps.it , aggiungere https://*.inps.it :



Fare la stessa cosa per gli altri a cui si vuole accedere:

- https://*.inps.it
- https://*.agenziaentrate.gov.it

Il problema non si manifesta invece con altri browser come Mozilla Firefox o Google Chrome, in quanto non hanno il concetto dei Siti Attendibili.

6.2.2 Problemi con Remote Desktop

IMPOSSIBILE UTILIZZARE LA CARTA

Se dopo aver eseguito il logon su una macchina utilizzando il client di Remote Desktop Microsoft, all'interno della macchina remota non è possibile utilizzare la smart card in alcun modo, controllare prima di tutto se software di terze parti non abbiano abilitato una particolare chiave di registro. Utilizzando l'applicazione regedit.exe di Windows, controllare che la seguente chiave:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\
```

Se è presente un valore REG_DWORD chiamato `fEnableSmartCard` impostato a 0, cambiarlo in 1 e riavviare la macchina.

7 Informazioni per gli sviluppatori

Gli sviluppatori di software di terze parti che volessero utilizzare Smart Card API per interagire con le smart card supportate da tale pacchetto, possono utilizzare principalmente due modalità di interazione:

- Accesso tramite standard **Microsoft Crypto API** (CSP)[1]
- Accesso tramite standard **PKCS#11**[2]

L'accesso tramite CSP è trasparente per l'applicazione in quanto SC API, grazie all'applicazione Smart Card Monitor, rende disponibile a Windows i certificati presenti sulla carta in modo che l'applicazione di terze parti possa usarli in modo trasparente e astratto come se il certificato fosse presente sulla postazione dell'utente e non sulla smart card. L'utilizzo del CSP è supportato nativamente da tutte le applicazioni native Windows scritte principalmente su piattaforme C/C++ e .net Framework o più in generale su tutte le piattaforme che supportano Microsoft CAPI.

Se invece l'applicazione richiede un accesso a più basso livello alla smart card o se l'applicazione è basata su piattaforma Java nativa (ovvero senza l'utilizzo di librerie di terze parti[3]), allora è possibile utilizzare lo standard PKCS#11.

7.1 Interfaccia PKCS#11

Per gli sviluppatori che vogliono utilizzare l'interfaccia PKCS#11 per l'accesso alla smart card, Smart Card API fornisce una libreria in standard PKCS#11. Il nome della libreria è **AtosSCAPIPKCS11.DLL** e si trova nei seguenti percorsi:

- Per sistemi Windows a 32 bit:
  - In `%SystemRoot%\System32\`
- Per sistemi Windows a 64 bit:
  - In `%SystemRoot%\System32\` per la versione a 64bit
  - In `%SystemRoot%\SysWOW64\` per la versione a 32bit

Per retro-compatibilità con la versione 2.0 delle API, la stessa libreria, ma con il vecchio nome **PKCS11.DLL** è presente negli stessi percorsi suddetti. Tuttavia, se possibile, si consiglia di utilizzare il nuovo nome in quanto nelle prossime versioni delle SC API tale libreria potrebbe essere rimossa.

Su sistemi operativi a 64bit si consiglia di non indicare il percorso assoluto della libreria PKCS#11 bensì di indicare, se possibile, solo il nome della libreria DLL in modo che sia Windows a scegliere la versione a 32 o 64 bit a seconda della versione dell'applicazione client.

Per l'utilizzo della libreria PKCS#11, è richiesta la conoscenza di base dello standard PKCS#11 stesso e delle sue modalità di utilizzo da codice. Per tali informazioni si consiglia di consultare il manuale *"PKCS#11 Cryptographic Token Interface Base Specification"* nella versione desiderata e

[1] Informazioni su Microsoft CSP si trovano alla URL https://msdn.microsoft.com/en-us/library/aa380245.aspx

[2] PKCS#11 è uno standard inizialmente creato e gestito da RSA e poi confluito nell'organizzazione OASIS. Attualmente le specifiche OASIS si trovano alla URL https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pkcs11 mentre le specifiche RSA alla URL http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-11-cryptographic-token-interface-standard.htm

[3] Ad esempio "IAIK Provider for the Java™ Cryptography Extension (IAIK-JCE)" è una soluzione commerciale che aggiunge un provider JCA/JCE per l'utilizzo del CSP di Windows.

pubblicata sul portale OASIS o RSA. Tale manuale contiene i dettagli su come utilizzare le librerie PKCS#11 e alcuni esempi di codice in linguaggio C[4].

7.1.1 Informazioni sulle carte supportate

Utilizzando la funzione PKCS#11 **C_GetTokenInfo**, è possibile ottenere informazioni sulla smart card e distinguere la sua tipologia:

CK_TOKEN_INFO	Label	Model	SerialNumber
CMD-1	[IDCARTA]	CMD	[IDCARTA]
CMCC	[IDCARTA]	CMCC	[IDCARTA]
CMD-2 / Modello ATe (chip ST-Incard T&S 2048 CNS)	[IDCARTA]	CMD2	[IDCARTA]
CMD-2 / CMCC-2 / Modello ATe (chip Oberthur CNS COSMO ID/ONE v7 e IDEMIA CNS COSMO ID/ONE v9)	[IDCARTA]	ATe (OBC)	[IDCARTA]

[IDCARTA] è il seriale alfanumerico a 9 caratteri riportato sul fronte della carta stessa (ad esempio AA1234567 per le CMD-1, MMDA12345 per le CMD-2/Modello ATe, CC1234567 per le CMCC).

7.1.2 Informazioni sugli oggetti sulle carte

La libreria PKCS#11 permette di eseguire operazioni di sola lettura sulle smart card. I nomi degli oggetti presenti sulle smart card sono indicati nella seguente tabella (in italico gli oggetti privati, ovvero quelli protetti da PIN):

Tipo carta	Label	Tipo oggetto	Descrizione
CMD-1	PDATA	CKO_DATA	Dati pubblici del titolare
	PDATA_EXTRA	CKO_DATA	Dati pubblici aggiuntivi del titolare
	PDATA_VAR	CKO_DATA	Dati pubblici variabili del titolare
	PDATA_VAR_PRV	CKO_DATA	Dati privati variabili del titolare
	Firma Qualificata	CKO_PUBLIC_KEY	Chiave pubblica di firma digitale
	Firma Qualificata	*CKO_PRIVATE_KEY*	*Chiave privata di firma digitale*
	Firma Qualificata	CKO_CERTIFICATE	Certificato di firma digitale
	CA Firma Qualificata	CKO_CERTIFICATE	Certificato di CA di firma digitale
	Chiave di Autenticazione	CKO_PUBLIC_KEY	Chiave pubblica di autenticazione
	Chiave di Autenticazione	*CKO_PRIVATE_KEY*	*Chiave privata di autenticazione*
	Chiave di Autenticazione	CKO_CERTIFICATE	Certificato di autenticazione
	Data encipherment	CKO_PUBLIC_KEY	Chiave pubblica di cifra/decifra
	Data encipherment	*CKO_PRIVATE_KEY*	*Chiave privata di cifra/decifra*
	Data encipherment	CKO_CERTIFICATE	Certificato di cifra/decifra
CMCC	PDATA	CKO_DATA	Dati pubblici del titolare
	PDATA_EXTRA	CKO_DATA	Dati pubblici aggiuntivi del titolare
	Firma Qualificata	CKO_PUBLIC_KEY	Chiave pubblica di firma digitale

[4] Se si utilizzano piattaforme di sviluppo differenti dal C/C++, se la piattaforma non fornisce supporto nativo, è necessario utilizzare dei wrapper di terze parti che permettono a piattaforme quali .net e Java di utilizzare le librerie PKCS#11. Ad esempio IAIK PKCS#11 Wrapper e Sun PKCS#11 Provider per Java, Pkcs11Interop per .net

Tipo carta	Label	Tipo oggetto	Descrizione
	Firma Qualificata	*CKO_PRIVATE_KEY*	*Chiave privata di firma digitale*
	Firma Qualificata	CKO_CERTIFICATE	Certificato di firma digitale
	CNS0	CKO_PUBLIC_KEY	Chiave pubblica di autenticazione
	CNS0	*CKO_PRIVATE_KEY*	*Chiave privata di autenticazione*
	CNS0	CKO_CERTIFICATE	Certificato di autenticazione
CMD-2	PDATA	CKO_DATA	Dati pubblici del titolare
	PDATA_EXTRA	CKO_DATA	Dati pubblici aggiuntivi del titolare
	PDATA_VAR	CKO_DATA	Dati pubblici variabili del titolare
	PDATA_VAR_PRV	CKO_DATA	Dati privati variabili del titolare
	Firma Qualificata	CKO_PUBLIC_KEY	Chiave pubblica di firma digitale
	Firma Qualificata	*CKO_PRIVATE_KEY*	*Chiave privata di firma digitale*
	Firma Qualificata	CKO_CERTIFICATE	Certificato di firma digitale
	CNS0	CKO_PUBLIC_KEY	Chiave pubblica di autenticazione
	CNS0	*CKO_PRIVATE_KEY*	*Chiave privata di autenticazione*
	CNS0	CKO_CERTIFICATE	Certificato di autenticazione
	Data encipherment	CKO_PUBLIC_KEY	Chiave pubblica di cifra/decifra
	Data encipherment	*CKO_PRIVATE_KEY*	*Chiave privata di cifra/decifra*
	Data encipherment	CKO_CERTIFICATE	Certificato di cifra/decifra
CMCC-2	PDATA	CKO_DATA	Dati pubblici del titolare
	PDATA_EXTRA	CKO_DATA	Dati pubblici aggiuntivi del titolare
	Firma Qualificata	CKO_PUBLIC_KEY	Chiave pubblica di firma digitale
	Firma Qualificata	*CKO_PRIVATE_KEY*	*Chiave privata di firma digitale*
	Firma Qualificata	CKO_CERTIFICATE	Certificato di firma digitale
	CNS0	CKO_PUBLIC_KEY	Chiave pubblica di autenticazione e cifra/decifra
	CNS0	*CKO_PRIVATE_KEY*	*Chiave privata di autenticazione e cifra/decifra*
	CNS0	CKO_CERTIFICATE	Certificato di autenticazione e cifra/decifra

Per l'utilizzo degli oggetti privati, è necessario eseguire la login sulla carta tramite l'apposita funzione **C_Login**. Per quanto riguarda invece la chiave di Firma Qualificata, dopo la login con la funzione C_Login, nel momento dell'utilizzo della chiave di firma, verrà chiesto il PIN Firma all'utente tramite l'apposita finestra (sezione 4.1).

Una particolarità delle carte CMD-2 con chip Oberthur CNS COSMO ID/ONE v7 e IDEMIA CNS COSMO ID/ONE v9 rispetto alle altre è che se la carta non è stata attivata da parte dell'utente, non sarà possibile utilizzare i certificati della carta (autenticazione, firma digitale e cifra/decifra). Se quindi l'applicazione chiamante cerca di utilizzare le chiavi private di questi certificati senza che la carta sia stata attivata, l'errore ritornato sarà per convenzione: **CKR_FUNCTION_FAILED**.

7.1.3 Formato dei file personali del titolare

Facendo riferimento alla tabella nella sezione 7.1.2, in questa sezione viene descritto il formato dei file dati del titolare (PDATA, PDATA_EXTRA, PDATA_VAR e PDATA_VAR_PRV).

Le varie carte supportate dalle API purtroppo sono nate in periodi storici differenti (CMD-1, CMD-2/Modello ATe) oppure prodotte da enti differenti (CMCC, CMCC-2), per questo motivo, sebbene le idee di fondo e gli standard supportati siano gli stessi, esistono piccole varianti che vanno considerate quando si sviluppa il software client che voglia utilizzare tali informazioni.

Il contenuto dei file dati CKO_DATA delle carte supportate rispecchia le specifiche CNS[5]: è in formato ASCII e il contenuto non avvalorato è pari al valore 00. Ogni file presenta la seguente struttura:

- Intestazione di 6 byte in formato ASCII che rappresentano la lunghezza totale dei dati significativi all'interno del file (compresi i 6 byte dell'intestazione) in formato esadecimale. Ad esempio, i byte 30 30 30 30 38 45 corrispondono al valore esadecimale 0x00008E e quindi indicano che i primi 142 byte del file vanno considerati, i restanti sono tutti 00 da scartare. Sulla CMD-1 tale valore non include i 6 byte dell'intestazione, quindi è sempre pari al valore della lunghezza totale meno 6. Sulla CMCC tale valore è sempre pari alla lunghezza totale più 1.

- Lista dei valori rappresentati come coppia (LEN_i, VAL_i):

  - LEN_i è pari a 2 byte in formato ASCII e indica la lunghezza del valore i-esimo in formato esadecimale. Ad esempio, i byte 30 34 corrispondono al valore esadecimale 0x04 e quindi indicano che il valore i-esimo ha lunghezza 4 byte. Se la lunghezza è pari a 0x00, il campo i-esimo è vuoto.

  - VAL_i è a lunghezza variabile indicata dal corrispondente LEN_i ed è in formato ASCII

Esemplificando, si consideri il seguente contenuto di file:

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   30 30 30 30 38 45 30 34 38 39 31 32 30 38 30 32   00008E0489120802
00000010   31 30 32 30 31 34 30 38 31 35 31 32 32 30 32 33   10201408151220 23
00000020   30 39 44 45 20 46 45 4C 49 43 45 30 44 44 41 4D   09DE FELICE0DDAM
00000030   49 41 4E 4F 20 44 49 45 47 4F 30 38 31 36 31 30   IANO DIEGO081610
00000040   31 39 37 31 30 31 4D 30 33 31 38 35 31 30 58 58   197101M0318510XX
00000050   58 58 58 58 58 58 58 58 58 58 58 58 58 58 30 33   XXXXXXXXXXXXXX03
00000060   49 54 41 30 34 4C 31 30 39 30 30 30 37 41 54 32   ITA04L1090007AT2
00000070   33 34 35 36 30 34 46 32 38 34 31 30 56 49 41 20   345604F28410VIA
00000080   44 45 49 20 54 45 53 54 20 31 30 32 30 30 00 00   DEI TEST 10200..
00000090   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000000A0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000000B0   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

Va interpretato nel seguente modo:

- 00008E (142 decimale) = dimensione totale dei dati da considerare

  - 04 (4 decimale) = Lunghezza del campo 1
  - 8912 = Valore del campo 1

  - 08 (8 decimale) = Lunghezza del campo 2
  - 02102014 = Valore del campo 2

  - 08 (8 decimale) = Lunghezza del campo 3
  - 15122023 = Valore del campo 3

  - 09 (9 decimale) = Lunghezza del campo 4
  - DE FELICE = Valore del campo 4

  - 0D (13 decimale) = Lunghezza del campo 5
  - DAMIANO DIEGO = Valore del campo 5

[5] Decreto 9 dicembre 2004 "Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della carta nazionale dei servizi" e specifiche AgID "Linee guida per l'emissione e l'utilizzo della carta nazionale dei servizi"

- Ecc…

Il significato dei campi di un file è ben specificato sia dallo standard CNS per quanto riguarda l'oggetto PDATA (Dati Personali Pubblici) sia dagli standard interni all'organizzazione che rilascia la carta (ad esempio Ministero della Difesa per le CMD). Nelle tabelle seguenti vengono specificati i campi presenti nei file dati. I campi indicati in **Arancione** sono quei campi su cui è opportuno prestare attenzione a causa di alcune difformità tra le varie carte.

Vista la difformità sull'intestazione di 6 byte di ogni file, vista la difformità sui contenuti, si consiglia di ignorare l'intestazione di 6 byte e leggere tutti i campi in sequenza usando la lunghezza di ogni campo.

Visto la memoria esigua disponibile sulle smart card, tutti i formati dei file e alcuni valori sono rappresentati usando il minor numero di byte possibile, soprattutto per i campi codificabili. Per ottenere le transcodifiche dei campi con valori codificati (indicati con Codifica) è necessario contattare l'emettitore della rispettiva carta.

OGGETTO PDATA

Campo	CMD-1	CMD-2	CMCC/CMCC-2
Emettitore	Vuoto	Codice Emettitore Nazionale (x912 = Ministero della Difesa, dove x indica il tipo di carta: 5 paziente, 8 medico)	Codice Emettitore Nazionale (0705 = Arma dei Carabinieri)
Data di emissione del documento	Formato AAAAMMGG	Formato GGMMAAAA	Formato GGMMAAAA
Data di scadenza del documento	Formato AAAAMMGG	Formato GGMMAAAA	Formato GGMMAAAA
Cognome	Valore	Valore	Valore
Nome	Valore	Valore	Valore
Data di Nascita	Formato AAAAMMGG	Formato GGMMAAAA	Formato GGMMAAAA
Sesso	M = Maschile F = Femminile	M = Maschile F = Femminile	M = Maschile F = Femminile
Statura (cm)	Valore	Valore	Valore
Codice fiscale	Valore	Valore	Valore
Cittadinanza (codice)	Codice ISO 3166-1 alpha-3	Codice ISO 3166-1 alpha-3	Codice ISO 3166-1 alpha-3
Comune di Nascita	Codice Belfiore	Codice Belfiore	Codice Belfiore
Stato estero di Nascita	Codice ISO 3166-1 alpha-3	Codice ISO 3166-1 alpha-3	Codice ISO 3166-1 alpha-3
Estremi atto di nascita	Valore	Valore	Valore
Comune di residenza al momento dell'emissione	Codice Belfiore	Codice Belfiore	Codice Belfiore
Indirizzo di residenza	Valore	Valore	Valore
Eventuale annotazione in caso di non validità del documento per l'espatrio	Vuoto	Vuoto	**Campo Non Presente**

OGGETTO PDATA_EXTRA

Campo	CMD-1	CMD-2	CMCC/CMCC-2

Campo	CMD-1	CMD-2	CMCC/CMCC-2
Ente rilascio	Codice	Codice	**Oggetto PDATA_EXTRA vuoto**
Categoria di Ginevra	Codice	Vuoto	**Oggetto PDATA_EXTRA vuoto**
Matricola	Valore	Valore	**Oggetto PDATA_EXTRA vuoto**
Titolarità pensione	Y = sì N = no	Y = sì N = no	**Oggetto PDATA_EXTRA vuoto**

OGGETTO PDATA_VAR

Campo	CMD-1	CMD-2	CMCC/CMCC-2
Segni particolari	Valore	Valore	**Oggetto PDATA_VAR Assente**
Note	Valore	Valore	**Oggetto PDATA_VAR Assente**
Grado	Codice	Codice	**Oggetto PDATA_VAR Assente**
Anzianità assoluta	Formato AAAAMMGG	Formato GGMMAAAA	**Oggetto PDATA_VAR Assente**
Anzianità di grado	Formato AAAAMMGG	Formato GGMMAAAA	**Oggetto PDATA_VAR Assente**
Ruolo appartenenza ufficiali	Codice	Codice	**Oggetto PDATA_VAR Assente**
Incarico di specializzazione: settore attività	Codice	Codice	**Oggetto PDATA_VAR Assente**
Incarico di specializzazione: specialità impiego	Codice	Codice	**Oggetto PDATA_VAR Assente**
Incarico attuale	Codice	Codice	**Oggetto PDATA_VAR Assente**
Ente/Reparto di appartenenza	Codice	Codice	**Oggetto PDATA_VAR Assente**
Categoria	C = Civile S = Sottufficiale T = Truppa U = Ufficiale G = Graduato A = Generale/Ammiraglio	C = Civile S = Sottufficiale T = Truppa U = Ufficiale G = Graduato	**Oggetto PDATA_VAR Assente**
Ente	**Non Presente**	AM = Aeronautica Militare EI = Esercito Italiano MM = Marina Militare PC = Personale Civile MG = Magistratura Militare ID = AgID	**Oggetto PDATA_VAR Assente**

OGGETTO PDATA_VAR_PRV

Campo	CMD-1	CMD-2	CMCC/CMCC-2
Ultima attribuzione stipendiale	Valore	Valore	**Oggetto PDATA_VAR_PRV Assente**
Religione	Codice	Codice	**Oggetto PDATA_VAR_PRV Assente**