Middleware Universale

Per smart card CNS Oberthur COSMO ID/ONE

Indice

DEFINIZIONI, ACRONIMI, ABBREVIAZIONI....3
MIDDLEWARE UNIVERSALE....4
CARATTERISTICHE DEL MODULO CSP....5
CARATTERISTICHE DEL MODULO PKCS#11....5
CARATTERISTICHE DEL MODULO DI GESTIONE DEL PIN....7
GESTIONE DEL PIN DI FIRMA FORTE....9
INSTALLAZIONE....11

Revisione	Autori	Note
B (20/02/2007)	Giuseppe Amato Vincenzo Palazzo	

Revisione	Autori	Note
C (05/03/2007)	Giuseppe Amato	Update interfaccia utente del PIN manager
D (06/06/2007)	Giuseppe Amato	Update interfaccia utente e funzionalità del PIN manager Gestione default container
E (04/07/2007)	Giuseppe Amato	Aggiunto Windows Vista alla lista dei sistemi operativi supportati
F (30/10/2008)	Giuseppe Amato	Aggiunte istruzioni per creare il file dati personali CNS: PDATA

Definizioni, Acronimi, abbreviazioni

PKCS#11	interfaccia di programmazione (API) standard, multi piattaforma, per l'accesso a generici token crittografici, quali le smart card, sviluppata da RSA
Libreria o modulo PKCS#11	Modulo software che implementa della API PKCS#11 specifica per uno o più token crittografici di un determinato produttore.
CSP	Interfaccia di programmazione (API) proprietaria Microsoft che permette di aggiungere funzioni crittografiche, anche fornite da hardware come le smart card, nei sistemi operativi Windows; un CSP è un modulo software che può essere utilizzato esclusivamente tramite API crittografiche del sistema operativo (CryptoAPI)
CryptoSPI	Acronimo che sta per Crypto Service Provider Interface, indica in modo specifico la API che un modulo CSP deve implementare.
API	Acronimo che sta per Application Programming Interface, indica ogni insieme di procedure disponibili al programmatore, di solito raggruppate a formare un set di strumenti specifici per un determinato compito
CryptoAPI	Acronimo che sta per Cryptographic Application Programming Interface; rappresneta l'interfaccia di programmazione che i sistemi operativi Windows mettono a disposizione delle applicazioni per l'uso della crittografia.
Tray-bar	Nei sistemi operativi Microsoft Windows rappresenta l'area localizzata tra la barra delle applicazioni e l'orologio, in cui le applicazioni possono installare un'icona che le rappresenti quando non sono in primo piano.
PIN	Acronimo di Personal Identification Number; nell'ambito delle smart card rappresneta un codice che permette di accedere alle funzioni il cui uso è riservato esclusivamente al possessore della carta; generalmente il PIN si blocca dopo un numero predefinito di tentativi con valori errati, bloccando dunque l'accesso alla smart card
PUK	Acronimo che sta per Pin Unblocking Key; nell'ambito delle smart card è uno codice del tutto simile al PIN, il cui scopo generalmente è esclusivamente quello di sbloccare un PIN bloccato dai troppi tentativi con valori non corretti.
CNS	Carta Nazionale dei Servizi; in questo documento può indicare la specifica CNS rilasciata dal CNIPA oppure le sole specifiche del file system.
MU	Middleware Universale, il software in oggetto
file system	Nell'ambito delle smart card indica la struttura ed il formato dei file e dei dati presenti un una smart card e che servono a d implementare una determinata funzionalità/applicazione.
ATR	Acronimo che sta per **Answare To Reset**; è un codice restituito da una smart card quando viene inserita nel lettore o resettata che viene spesso utilizzato per identificare il tipo di smart card in maniera univoca.
Store di certificati	Rappresenta il punto in cui il sistema operativo Windows memorizza i certificati di sicurezza, in modo che possano essere utilizzati dalle applicazioni che fanno uso delle CryptoAPI
SSL	Acronimo che sta per **Secure Socket Layer**: protocollo standard di comunicazione cifrata che permette anche la mutua autenticazione tra le parti comunicanti (SSL Server authentication e Client Authentication)
TLS	Acronimo che sta per **Transport Layer Security:** è il successore del protocollo SSL.
FS	Acronimo che sta per File System
DS	Acronimo che sta per Digital Signature: indica il files ystem di firma digitale (in questo documento può indicare anche un file system non CNS)

Middleware Universale

Il "Middleware Universale" (in seguito MU) consiste in:

- Modulo di libreria che espone una API compatibile con specifica di standard PKCS#11 v2.11.
- Modulo di sistema che espone una API compatibile con specifica di standard Microsoft Cryptographic Service Provider (CryptoSPI/2006).
- Modulo di sistema "certificate store" che implementa un meccanismo di importazione automatica dei certificati nello store utente windows.
- Modulo utente per la gestione PIN/PUK (cambio PIN, sblocco PIN).

Tali moduli offrono ai software che ne utilizzano le relative interfacce di programmazione la possibilità di utilizzare le smart card supportate come token crittografici.

Smart Card supportata: CNS Oberthur COSMO ID/ONE con doppio Filesyste:

- Filesystem CNS conforme alla specifica CNS del CNIPA (v.1.1.3)
- Filesystem di firma proprietario Oberthur definito nei seguenti documenti:
  - RequirementsAD.doc
  - ProtocolloCollaudoAA.doc
  - DS ARCHITECTURE02-2006.doc

Le funzionalità garantite dall'interfaccia PKCS#11 sono le seguenti.
Per il filesystem CNS:

- Firma digitale e decifra tramite la chiave RSA di autenticazione CNS,
- Lettura e scrittura del certificato di autenticazione CNS,
- Lettura e scrittura del file dei dati personali CNS (PDATA)
- Generazione di una coppia di chiavi RSA di autenticazione CNS
- Cancellazione degli oggetti

Per il filesystem proprietario di firma:

- Firma digitale e decifra tramite la chiave RSA di autenticazione,
- Firma digitale tramite la chiave RSA di firma forte,
- Generazione di una coppia di chiavi RSA di autenticazione
- Generazione di una coppia di chiavi RSA di Firma forte
- Lettura e scrittura di certificati di autenticazione o di firma forte,
- Cancellazione degli oggetti

Le funzionalità garantite dall'interfaccia CSP sono le seguenti:
Per il filesystem CNS:

- Firma digitale e decifra tramite la chiave RSA di autenticazione CNS,
- Lettura e del certificato di autenticazione CNS,

Per il filesystem proprietario di firma:

- Firma digitale e decifra tramite la chiave RSA di autenticazione
- Lettura dei certificati di autenticazione o di firma forte,

Il modulo utente di gestione PIN-PUK è una applicazione attivabile mediante una icona presente nella tray-bar. Consente il cambio del PIN, lo sblocco del PIN mediante PUK.

Il MU comunica con le smart card attraverso un lettore di smart card controllato dallo strato PC/SC implementato nei sistemi operativi Microsoft.

I moduli che espongono le due interfacce PKCS#11 e CSP si appoggiano su di un unico "motore" che gestisce gli oggetti di sicurezza presenti sulle smart card CNS. Tale motore ha la possibilità di essere esteso attraverso un meccanismo di "plug-in".

Il modulo che espone l'interfaccia PKCS#11 viene interfacciato direttamente dalle applicazioni che utilizzano tale API per utilizzare i servizi offerti dalle smart card. Attraverso l'interfaccia PKCS#11 è possibile leggere il certificato di autenticazione e utilizzare la chiave privata RSA presente sulla smart card.

Il modulo che espone l'interfaccia CryptoSPI viene interfacciato dal sistema operativo che integra le funzioni esposte con quelle di più alto livello del CSP che poi saranno messe a disposizione delle applicazioni.

Il modulo "certificate store" viene interfacciato dal sistema operativo che estende in questo modo lo store di certificati "logico" dell'utente (o store "My") estendendolo utilizzando uno store di certificati "fisico" afferente alla smart card. Tale modulo consente l'uso dei certificati presenti sulla smart card da parte delle applicazioni che fanno uso delle CryptoAPI in maniera del

tutto automatica e trasparente. Alla rimozione della smart card i certificati verranno automaticamente rimossi. Il modulo "certificate store" può essere disattivato ed in tal caso sarà il sistema operativo, all'inserimento della carta, ad importare automaticamente i certificati nello store dei certificati personali; in tal caso i certificati saranno visibili nel sistema anche dopo la rimozione della smart card.

Il modulo "gestione PIN/PUK" non espone una interfaccia di programmazione (API) ma ha una interfaccia utente (GUI) che consente all'utente di svolgere le minimali attività per il cambio e lo sblocco del PIN. L'interfaccia utente può essere attivata intervenendo su di una icona presente nella tray-bar che fornisce inoltre anche informazioni sull'attuale stato di attività della smart card.

Sistemi operativi supportati

- Windows 2000 SP4
- Windows XP SP2
- Windows Vista

Caratteristiche del modulo CSP

1. Libreria compatibile con la specifica CSP di Microsoft
2. Supporto della smart card CNS Oberthur COSMO ID/ONE con doppio Filesystem: Filesystem CNS conforme alla specifica CNS del CNIPA (v.1.1.3) e Filesystem di firma proprietario Oberthur
3. Funzionamento del CSP limitato all'utilizzo nei seguenti contesti applicativi:
    1. autenticazione SSL V3 con Microsoft IE,
    2. funzione di "Firma leggera per Attestazione" per applicazioni web
    3. funzione di "Firma Forte" per applicazioni di firma digitale
4. Sistemi operativi sui quali Bit4id certifica il pieno funzionamento ed il superamento dei propri test prima del rilascio:
    1. Windows 2000 SP4, XP SP2
5. Rilascio libreria in formato binario sotto form adi libreria a "link dinamico".
6. Applicazione con la quale Bit4id certifica il pieno funzionamento con il superamento dei propri test prima del rilascio: Microsoft IE vers. 6
7. Caricamento dei certificati presenti sulla smart card in maniera trasparente per l'utente all'inserimento nel lettore.

L'interfaccia CSP implementa le seguenti funzioni:

- CryptGetProvParam (PP_NAME, PP_CONTAINER, PP_UNIQUE_CONTAINER)
- CryptSetProvParam (PP_SIGNATURE_PIN)
- CryptAcquireContext
- CryptReleaseContext
- CryptCreateHash
- CryptSetHashParam
- CryptGetHashParam (HP_ALGID, HP_HASHSIZE, HP_HASHVAL)
- CryptHashData,
- CryptDestroyHash
- CryptSignHash
- CryptGetUserKey
- CryptDestroyKey
- CryptGetKeyParam (KP_CERTIFICATE)
- CryptExportKey (PUBLICKEYBLOB)

CSP Default container

Per l'uso con applicazioni di logon (ad esempio l'accesso alla workstation con smart card) il sistema operativo richiede la presenza sulla smart card di un container di default.
Il modulo CSP considera il primo container che viene trovato sulla carta come quello di default. Nel caso venga importato tramite l'interfaccia CSP un certificato che contiene le estensioni X509 specifiche per smart card logon, il container corrispondente viene marcato come quello di default.
Internamente la libreria crea un oggetto dati PKCS#11 (CKA_CLASS=CKO_DATA) con attributo CKA_LABEL "default_container" ed il cui contenuto (CKA_VALUE) coincide con il nome del container di default.

Caratteristiche del modulo PKCS#11

1. Libreria compatibile con la specifica PKCS#11 di RSA (v. 2.11)
2. Supporto della smart card CNS Oberthur COSMO ID/ONE con doppio Filesystem: Filesystem CNS conforme alla specifica CNS del CNIPA (v.1.1.3) e Filesystem di firma proprietario Oberthur.

3. Funzionamento del PKCS#11 limitato all'utilizzo nei seguenti contesti applicativi:
   1. autenticazione SSL V3 con il browser Mozilla FireFox 2.0,
   2. funzione di "Firma leggera per Attestazione" per applicazioni web
   3. funzione di "Firma Forte" per applicazioni di firma digitale
   4. funzione di enrollment di credenziali CNS, di firma forte, di autenticazione tramite Software CA di Infocamere
   5. Lettura della smart card tramite Token Manager Alladin eToken View ver. 3.50.138
4. Sistemi operativi sui quali Bit4id certifica il pieno funzionamento ed il superamento dei propri test prima del rilascio:
   1. Windows 2000 SP4, XP SP2
5. Rilascio del modulo PKCS#11 in formato binario come libreria a "link dinamico".
6. Applicazione con la quale Bit4id certifica il pieno funzionamento con il superamento dei propri test prima del rilascio: Browser Mozilla Firefox vers. 2.0

L'interfaccia PKCS#11 implementa le seguenti funzioni:

- C_Initialize
- C_Finalize
- C_GetInfo
- C_GetSlotList
- C_GetSlotInfo
- C_GetTokenInfo
- C_GetMechanismList
- C_GetMechanismInfo
- C_OpenSession
- C_CloseSession
- C_CloseAllSessions
- C_GetSessionInfo
- C_Login
- C_Logout
- C_SetPIN
- C_FindObjectsInit
- C_FindObjects
- C_FindObjectsFinal
- C_GetAttributeValue
- C_GetObjectSize
- C_SignInit (meccanismi RSA_PKCS e RSA_SHA1_PKCS)
- C_Sign
- C_DecryptInit (meccanismo RSA_PKCS)
- C_Decrypt
- C_DigestInit (meccanismo SHA_1)
- C_Digest
- C_DigestUpdate
- C_DigestFinal
- C_CreateObject
- C_GenerateKeyPair
- C_SetAtttributeValue
- C_DestroyObject

Mechanisms supportati:
CKM_RSA_PKCS_KEY_PAIR_GEN
CKM_RSA_PKCS (firma, decifra)
CKM_SHA_1 (digest)

Creazione dei diversi tipi di oggetti: CNS, Firma Forte, Autenticazione

Per stabilire la tipologia di oggetto da creare vengono utilizzati alcuni attributi specificati alla creazione o generazione degli oggetti:

- Quando il CKA_ID di un oggetto ha come valore '**CNS0**' viene creato un oggetto nel filesystem CNS; se l'oggetto che si vuole creare esiste già viene generato un errore.
- Quando CKA_LABEL di un data object (un oggetto per cui CKA_CLASS=CKO_DATA) è impostato a 'PDATA' viene creato il file dati personali del filesystem CNS. Il valore dei dati personali va specificato come attributo CKA_VALUE.
- Quando il CKA_ID è 'DS', oppure 'DS0', 'DS1', 'DS2'; ovvero quando CKA_LABEL è 'Firma_CNS' oppure 'Firma_CNS0'..'Firma_CNS2': viene creato un oggetto di firma forte

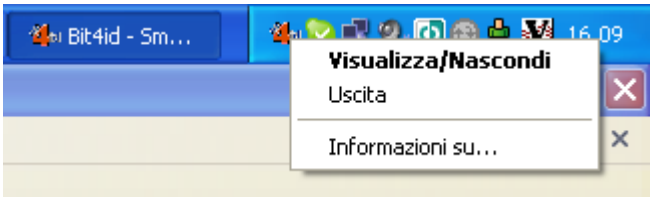
- In tutti gli altri casi viene creato un oggetto di autenticazione non CNS.

Caratteristiche del modulo di gestione del PIN

Il modulo di gestione PIN è un'applicazione dotata di interfaccia utente (GUI) che permette di gestire il PIN delle smart card supportate dal MU.
L'applicazione permette di eseguire le seguenti operazioni:

- Ottenere informazioni sulla smart card inserita, quali il numero di serie, il modello e il lettore in uso.
- Cambiare il valore del PIN
- Sbloccare il PIN bloccato usando il codice PUK

Tutte le operazioni sono eseguite utilizzando l'interfaccia PKCS#11 messa a disposizione dal MU.
L'applicazione può essere caricata in automatico durante l'avvio del sistema ed in tal caso non verrà mostrata una finestra.
L'applicazione, quando la finestra principale non è visibile, è nascosta e mostrerà esclusivamente un'icona nella barra delle applicazioni, accanto all'orologio (tray bar). Facendo doppio click su tale icona si attiva/disattiva la finestra principale dell'applicazione, l'applicazione rimarrà attiva in background e sarà riattivabile in due modi: lanciando nuovamente l'applicazione oppure facendo doppio click sull'icona che l'applicazione installa nella tray bar; per terminare completamente l'applicazione si può usare la voce "*Uscita*" presente nel menu contestuale che appare cliccando sull'icona che l'applicazione visualizza nella tray-bar.



Per ogni sessione utente può esistere una singola istanza dell'applicazione; se essa viene eseguita più volte verrà attivata la finestra dell'istanza precedente.
L'applicazione è caratterizzata da un'interfaccia a schede (o tab), ognuna delle quali fornisce una funzionalità; la prima scheda è la principale e fornisce le informazioni sulla smart card.

Quando non è inserita nessuna smart card oppure se l'unica smart card inserita non è riconosciuta la scheda principale sarà l'unica visibile.

Nel caso in cui non siano installato un lettore di smart card l'applicazione mostrerà la sola scheda delle informazioni indicando che non è stato rilevato alcun lettore.

Cambio del PIN

La scheda denominata "Cambio PIN" permette di modificare il valore del PIN della smart card inserita.

La scheda richiede il valore del vecchio PIN (primo campo); il valore da assegnare al nuovo PIN viene richiesto per due volte, quale conferma del valore inserito (secondo e terzo campo). Tutti i valori richiesti sono offuscati ed al loro posto sullo schermo appariranno degli asterischi (o altri simboli, a seconda del sistema operativo in uso).
L'operazione di cambio PIN viene avviata cliccando sul pulsante Esegui oppure tramite tasto Invio battuto in uno qualsiasi dei campi.

Nel caso in cui si verifichi un errore durante l'operazione di cambio PIN, questo verrà segnalato tramite una "message box" che spiegherà l'errore all'utente.
Gli errori che possono verificarsi sono:
“Il valore del nuovo PIN è troppo lungo o troppo corto”
“Il nuovo PIN è stato ridigitato in maniera diversa”
“Il vecchio PIN non è corretto ed è stato rifiutato dalla smart card”
“Il PIN è bloccato” (a causa dei troppi tentativi effettuati con un valore errato)
“La smart card ha restituito un errore inatteso”

Alla fine di un cambio PIN avvenuto con successo, oppure cambiando scheda, i valori dei campi sono azzerati.
Se uno dei campi è responsabile di un errore esso viene automaticamente selezionato e diventa il campo che riceve l'input dall'utente.

Sblocco del PIN

La scheda denominata “Sblocca smart card” permette di sbloccare un PIN bloccato, mediante l'uso del codice di sblocco (PUK), e di assegnare dunque un nuovo valore al PIN.
La scheda richiede il valore del PUK (primo campo); il valore da assegnare al nuovo PIN viene richiesto per due volte, quale conferma del valore inserito (secondo e terzo campo). Tutti i valori richiesti sono offuscati ed al loro posto sullo schermo appariranno degli asterischi (o altri simboli, a seconda del sistema operativo in uso).
L'operazione di sblocco PIN viene avviata cliccando sul pulsante Esegui oppure tramite tasto Invio battuto in uno qualsiasi dei campi.

Nel caso in cui si verifichi un errore durante l'operazione di sblocco PIN, questo verrà segnalato tramite una "message box" che spiegherà l'errore all'utente.
Gli errori che possono verificarsi sono:
“Il valore del nuovo PIN è troppo lungo o troppo corto”
“Il nuovo PIN è stato ridigitato in maniera diversa”
“Il PUK non è corretto ed è stato rifiutato dalla smart card”
“Il PUK è bloccato”(a causa dei troppi tentativi effettuati con un valore errato)
“La smart card ha restituito un errore inatteso”

Alla fine di uno sblocco del PIN avvenuto con successo, oppure cambiando scheda, i valori dei campi sono azzerati.
Se uno dei campi è responsabile di un errore esso viene automaticamente selezionato e diventa il campo che riceve l'input dall'utente.

Impostazioni avanzate

Nella scheda “Avanzate” è possibile associare la smart card inserita al CSP del Middleware Universale: è infatti necessario che l'ATR della carta inserita si correttamente associato al CSP perché possa essere riconosciuta da applicazioni come Internet Explorer e Outlook Express.
In questa shceda è inoltre possibile importare i certificati di ROOT CA presenti sulla smart card nello store dei certificati di Windows “Autorità di certificazione attendibili”.

Gestione del PIN di firma forte

Il PIN di Firma forte può essere gestito in due modalità:

- Il suo valore è identico al PIN CNS ed i due PIN vanno considerati come se fossero uno solo
- Il PIN di firma forte ha un valore diverso da quello CNS e va richiesto all'utente tramite interfaccia grafica (finestra di popup)

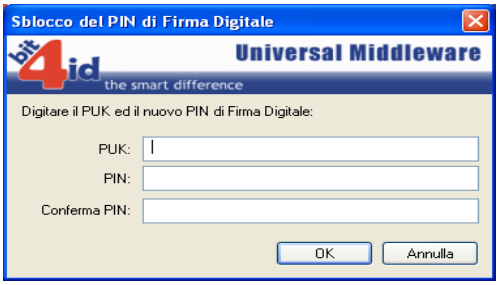
La scelta del tipo di comportamento delle librerie può essere deciso tramite il file di configurazione che segue la libreria e che viene descritto più avanti.

Nel caso di gestione separata di PIN, quando viene richiamata funzioni che richiedono il PIN di firma forte verrà visualizzata la seguente finestra:

Nel caso di cambio del PIN:

NOTA: nel caso di cambio del PUK la finestra è identica, cambiano esclusivamente le descrizioni dei campi.

Nel caso di sblocco del PIN:



Installazione

Il MU è composto dai seguenti moduli:

Nome	Destinazione
bit4opki.dll	%WINDIR%\System32
Descrizione	
Il modulo principale del MU, va installato nella cartella **System32**. Tale modulo contiene l'interfaccia PKCS#11, l'interfaccia Smart Card per l'uso tramite "Microsoft Base smart card CSP", che fornisce l'interfaccia CSP, e il “certificate store” per l'importazione automatica e temporanea dei certificati dalla smart card al sistema operativo. Quando si vuole utilizzare la sola interfaccia PKCS#11 è possibile installare tale modulo anche in directory diverse dalla System32.	

Nome	Destinazione
bit4extplg.dll	%WINDIR%\System32
Descrizione	
Il modulo per la richiesta PIN utilizzato dal MU per richiedere il PIN DS, va installato nella **stessa cartella in cui si trova il modulo principale bit4opki.dll** .	

Nome	Destinazione
bit4opki-store.dll	%WINDIR%\System32
Descrizione	
Modulo epr l'importazione automatica dei certificati negli store dei certificati di Windows. Per attivare la funzionalità del “certificate store” è necessario eseguire la registrazione nel sistema operativo tramite il comando: **regsvr32.exe bit4opki-store.dll** La deregistrazione del modulo si può invece ottenere con: **regsvr32.exe /u bit4opki-store.dll** La disattivazione del “certificate store” si ottiene tramite la sua deregistrazione.	

Nome	Destinazione
bit4pin.exe	Una directory a propria scelta
Descrizione	
E' il modulo per la gestione del PIN e può essere installato in una directory qualsiasi. L'applicazione può ricevere alcuni parametri che permettono di eseguire alcune funzioni aggiuntive: /kill — permette di terminare un'istanza dell'applicazione già in esecuzione; questo parametro è utile ad esempio in un programma di disinstallazione per evitare di dover cancellare il file del programma al successivo riavvio del computer. /hide — permette di eseguire l'applicazione in maniera nascosta; tale parametro può essere usato per eseguire in maniera silente l'applicazione durante l'avvio del sistema. Se l'applicazione viene eseguita senza alcun parametro ma un'istanza precedente è in esecuzione, l'istanza precedente verrà attivata e la nuova istanza terminerà immediatamente. **NOTA**: poiché l'applicazione usa il MU per poter svolgere le sue funzioni occorre installare tutti i suoi moduli in System32.	

Registrazione di un ATR per il CSP

Affinché una carta sia utilizzabile tramite l'interfaccia CSP del MU è necessario che l'ATR della carta sia configurato nel sistema.
Per registrare una carta nel sistema occorre creare delle chiavi di registro, simili a quelle che seguono:

percorso nel registro	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\smart cards\Nome_Della_Carta

Nome valore e tipo	Valore
Crypto Provider (valore stringa)	"Bit4id Universal Middleware Provider"
80000001 (valore stringa)	"bit4opki.dll"
ATR (valore binario)	ATR_DELLA_CARTA
ATRMASK (valore binario)	bitmask dell'ATR della carta

La chiave "**Nome_Della_Carta**" rappresenta il nome con il quale la carta è conosciuta dal sistema operativo.
Il sistema enumererà le carte in ordine alfabetico; affinché una carta sia valutata prima delle altre potrebbe essere necessario preporre una o più caratteri di spazio (" ") prima del suo nome; ad esempio " Nome_Della_Carta".

File di configurazione del MU

Il MU ha un file di configurazione che permette di variarne il comportamento.
Il file di configurazione, che si chiama **bit4opki.dll.conf** DEVE sempre trovarsi nella stessa cartella in cui si trova il il modulo principale bit4opki.dll.

Formato del file di configurazione

Il file di configurazione è composto da una serie di righe ed ogni riga contiene una stringa del tipo NomeValore=Valore; sono ammesse righe vuote.

Contenuto del file di configurazione

Le impostazioni utilizzabili nel file di configurazione sono le seguenti:

Nome	Possibili Valori	Descrizione
DSPinIsCnsPin	true o false	Se impostato a "true" viene indicato forzata l'uguaglianza del pin primario con il pin di firma. Valore di default: false
DSPinUseGui	true o false	Se impostato a "false" la libreria PKCS#11 gestisce un eventuale PIN secondario che protegge gli oggetti di firma in maniera compliant col la specifica PKCS#11, restituendo dunque l'errore CKR_USER_NOT_LOGGED_IN in seguito ad una chiamata alla funzione C_Sign su una chiave protetta da quel PIN, aspettandosi immediatamente dopo una chiamata a C_Login(CKU_CONTEXT_SPECIFIC) col PIN di firma. Se impostato a "true" verrà utilizzato il plugin per la richiesta del PIN secondario tramite interfaccia grafica (GUI). Il parametro è ignorato quando DSPinIsCnsPin è impostato a "true". Valore di default: true
HideCacheDsPinCheck	true o false	Se impostato a true viene nascosto dall'interfaccia utente che richiede il PIN di firma forte il checkbox che permette di utilizzare lo stesso PIN per più operazioni di firma in sequenza, fino al logout dalla carta. Valore di default: false