Middleware Universale

Bit4id srl
sede legale ed operativa:
Via Coroglio, 57
Città della Scienza
80124 Napoli – Italia
Tel. +39 081 7625600
Fax. +39 081 19731930
N.iscriz. CCIAA, c.f. e P.IVA:
IT-04741241212
Iscritta al Registro Imprese di Napoli
(REA 711203)
Capitale sociale: 600.000 EUR

Ufficio Roma:
Via Tirone,11
00146 Roma
Tel +39 06 45213431
Fax +39 06 99335481

Ufficio Milano:
Tel. +39 02 40042990
Fax. +39 02 45500675

www.bit4id.com
info@bit4id.com

Ufficio Spagna: Bit4id Iberica s.l.
C/ Marie Curie, 8-14
Forum Nord de Tecnología
08042 Barcellona - Spagna
Tel. +34 902 602030
Fax +34 932 917730

Ufficio UK: Bit4id Ltd.
2 London Wall Buildings
London Wall, London EC2M 5UU - UK
Tel. +44 (0)2 03 3973166
Fax +44 (0)2 07 8553780

qualityaustria
SYSTEM CERTIFIED
ISO 9001:2008 No.07974/0
ISO 14001:2004 No.01608/0

ISO 9001:2008
ISO 14001:2004
ISO 27001:2005

INDICE

Definizioni, Acronimi, abbreviazioni 4
Middleware Universale 5
Caratteristiche del modulo CSP 6
Caratteristiche del modulo PKCS#11 7
Caratteristiche del modulo di gestione del PIN (Bit4Id – Smart Card Manager) 8
Gestione del PIN di firma forte 11
File di configurazione del MU 12
Installazione 13
Microsoft Windows 13
Apple OSX 14
Distribuzioni Linux 15
Guida alla configurazione di Firefox 16

Revisione	Autori	Note
A (29/01/2016)	Vincenzo Cinque	

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.
- 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 Filesystem:
  - 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
- CNS Incard Touch & Sign (T&S) con doppio Filesystem:
  - Filesystem CNS conforme alla specifica CNS del CNIPA (v.1.1.3)
  - Filesystem di firma proprietario Incard
- CNS Incard Java Sign (JSign) con doppio Filesystem::
  - Filesystem CNS conforme alla specifica CNS del CNIPA (v.1.1.3)
  - Filesystem di firma proprietario Incard
- CNS Siemens:
  - Filesystem CNS conforme alla specifica CNS del CNIPA (v.1.1.3)
- CNS Atena:
  - Filesystem CNS conforme alla specifica CNS del CNIPA (v.1.1.3)

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 scrittura del certificato di autenticazione CNS,
- Generazione di una coppia di chiavi RSA di autenticazione CNS
- Generazione di una coppia di chiavi RSA di Firma forte

Per il filesystem proprietario di firma:

- Firma digitale e decifra tramite la chiave RSA di autenticazione
- Lettura e scrittura dei certificati di autenticazione o di firma forte,
- Generazione di una coppia di chiavi RSA di autenticazione
- Generazione di una coppia di chiavi RSA 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 , OSX e Linux.

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 dalle applicazioni.

Il modulo "certificate store" si occupa di aggiungere e rimuovere i certificati nello store "My store", quando viene inserita una smart card riconosciuta. 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 XP SP3, intel 32 e 64bit
- Windows Vista SP2, intel 32 e 64bit
- Windows 7 , intel 32 e 64bit
- Windows 8.1, intel 32 e 64bit
- Windows 10, intel 32 e 64bit
- Distribuzioni Linux Debian-Ubuntu, Fedora-Redhat, intel 32 e 64bit
- OSX da 10.10 a 10.11, intel 32 e 64bit

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. Supporto della smart card InCard Touch & Sign e Java Sign con doppio Filesystem: Filesystem CNS conforme alla specifica CNS del CNIPA (v.1.1.3) e Filesystem di firma proprietario InCard
4. Supporto della smart card CNS Siemens con Filesystem CNS conforme alla specifica CNS del CNIPA (v.1.1.3)
5. Supporto della smart card CNS Atena con Filesystem CNS conforme alla specifica CNS del CNIPA (v.1.1.3)
6. Funzionamento del CSP limitato all'utilizzo nei seguenti contesti applicativi:
    a. autenticazione SSL V3/TLS con Microsoft IE, Google Chrome
    b. funzione di "Firma leggera per Attestazione" per applicazioni web
    c. funzione di "Firma Forte" per applicazioni di firma digitale
7. Sistemi operativi sui quali Bit4id certifica il pieno funzionamento ed il superamento dei propri test prima del rilascio:
    a. Windows XP SP3
    b. Windows 7
    c. Windows 8.1
    d. Window 10
8. Rilascio libreria in formato binario sotto form adi libreria a "link dinamico".
9. Applicazione con la quale Bit4id certifica il pieno funzionamento con il superamento dei propri test prima del rilascio: Microsoft IE vers. 10,11 , Google Chrome. E' in via di sviluppo il supporto a Windows Edge.
10. 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. Supporto della smart card InCard Touch & Sign e Java Sign con doppio Filesystem: Filesystem CNS conforme alla specifica CNS del CNIPA (v.1.1.3) e Filesystem di firma proprietario InCard
4. Supporto della smart card CNS Siemens con Filesystem CNS conforme alla specifica CNS del CNIPA (v.1.1.3)
5. Supporto della smart card CNS Atena con Filesystem CNS conforme alla specifica CNS del CNIPA (v.1.1.3)
6. Funzionamento del PKCS#11 limitato all'utilizzo nei seguenti contesti applicativi:
    a. autenticazione SSL V3 con il browser Mozilla FireFox 41.0.2 e precedenti,
    b. funzione di "Firma leggera per Attestazione" per applicazioni web
    c. funzione di "Firma Forte" per applicazioni di firma digitale
    d. funzione di enrollment di credenziali CNS, di firma forte, di autenticazione tramite Software CA di Infocamere
    e. Lettura della smart card tramite Token Manager Alladin eToken View ver. 3.50.138
7. Sistemi operativi sui quali Bit4id certifica il pieno funzionamento ed il superamento dei propri test prima del rilascio:
    a. Windows XP SP3, Windows 7 , Windows 8.1, Windows 10,
    b. OSX 10.10, OSX 10.11,
    c. Distribuzioni Linux Debian-Ubuntu , Fedora-Redhat
8. Rilascio del modulo PKCS#11 in formato binario come libreria a "link dinamico".
9. Applicazione con la quale Bit4id certifica il pieno funzionamento con il superamento dei propri test prima del rilascio: Browser Mozilla Firefox vers. 41.0.2 (Vedi paragrafo - Guida alla configurazione di Firefox - come guida alla configurazione)

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, RSA_SHA_256_PKCS)
- C_Sign
- C_DecryptInit (meccanismo RSA_PKCS)
- C_Decrypt
- C_DigestInit (meccanismo SHA_1, SHA_256)

- 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)
- RSA_SHA1_PKCS (firma)
- RSA_SHA_256_PKCS (firma)
- CKM_SHA_1 (digest)
- CKM_SHA_256 (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:

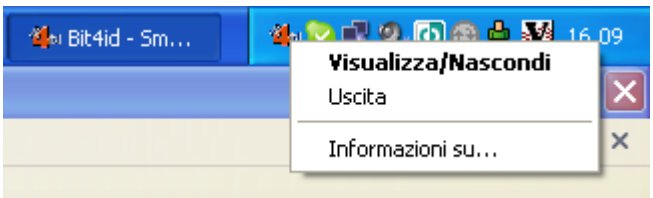
- Quando il CKA_ID di un oggetto ha come valore '**CNS0**' viene creato un oggetto nel filesystem CNS; se l'oggetto che si vuole creare esiste già viene generato un errore.
- Quando CKA_LABEL di un data object (un oggetto per cui CKA_CLASS=CKO_DATA) è impostato a 'PDATA' viene creato il file dati personali del filesystem CNS. Il valore dei dati personali va specificato come attributo CKA_VALUE.
- Quando il CKA_ID è 'DS<X>' viene creato un oggetto di firma forte. DS0,DS1,DS2 per oggetti a 1024 bit , DS3,DS4,DS5 per oggetti a 2048 bit.
- In tutti gli altri casi viene creato un oggetto di autenticazione non CNS.

Caratteristiche del modulo di gestione del PIN (Bit4Id – Smart Card Manager)

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 supporta le lingue: Inglese, Italiano, Spagnolo e Tedesco selezionandola automaticamente secondo il local della macchina.
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.

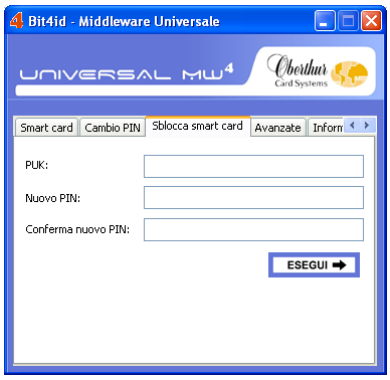
La scheda richiede il valore del vecchio PIN (primo campo); il valore da assegnare al nuovo PIN viene richiesto per due volte, quale conferma del valore inserito (secondo e terzo campo). Tutti i valori richiesti sono offuscati ed al loro posto sullo schermo appariranno degli asterischi (o altri simboli, 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 scheda è inoltre possibile importare i certificati di ROOT CA presenti sulla smart card nello store dei certificati di Windows "Autorità di certificazione attendibili".

Gestione Smart Card Contactless

Il MU è in grado di gestire l'interfaccia contactless di smart card duali, previa installazione e configurazione di un adeguato lettore PCSC v2.0.

Tutte le operazioni (CSP o PKCS#11) disponibili tramite l'interfaccia a contatti sono disponibili anche tramite l'interfaccia contactless, senza differenza alcuna.

Occorre sottolineare comunque che, a causa del funzionamento del protocollo di comunicazione contactless (ISO 14443-A/B), l'ATR ritornato da ciascun modello di lettore senza contatti dipende dalle sue caratteristiche interne ed è pertanto impossibile associare ad una carta un ATR "contactless".

Per tale ragione, in ambiente Windows, il primo uso di una qualunque smart card contactless determina l'attivazione della ricerca automatica di driver su Windows Update, anche se la smart card è stata precedentemente registrata tramite l'interfaccia a contatti.

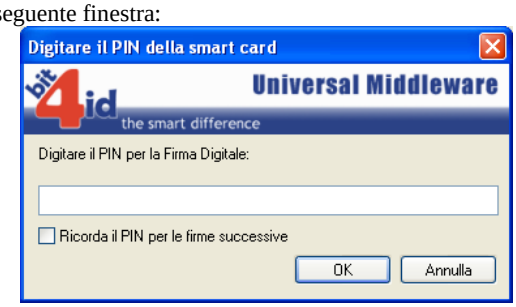
Per evitare ripetute connessioni ai server di Windows Update ad ogni uso dell'interfaccia contactless, è necessario registrare la Smart Card contactless tramite lo Smart Card Manager nella sezione "Avanzate" (vedi pag. 9)

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 (opzione di default)
- 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:

File di configurazione del MU

Il MU ha un file di configurazione che permette di variarne il comportamento.
Il file di configurazioneha lo stesso nome della libreria con aggiunta dell'enstensione "**.conf**". Il file DEVE sempre trovarsi nella stessa cartella in cui si trova il il modulo principale.

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

Installazione

Microsoft Windows

Il MU è distribuito sotto forma di installer per Windows. La procedura guidata multilingue (Italiano, Inglese, Tedesco, Spagnolo) consente, previa accettazione del contratto di licenza, di installare automaticamente il middlware e il software di gestione del pin con tutte le sue dipendenze permettendo all'utente l'immediato utilizzo. Il software di gestione del pin (Bit4Id – Smart Card Manager) viene installato nel seguente percorso C:\Program Files (x86)\Bit4id\Universal MW\bit4pin.exe

Moduli installati e configurati automaticamente dall'installer sia per i sistemi a 32 che a 64 bit :

Nome	Destinazione
bit4xpki.dll	%WINDIR%\System32 e %WINDIR%\SysWOW64
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 e %WINDIR%\SysWOW64
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 bit4xpki.dll** .	

Nome	Destinazione
bit4upki-store.dll	%WINDIR%\System32 e %WINDIR%\SysWOW64
Descrizione	
Modulo per 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 bit4upki-store.dll** La deregistrazione del modulo si può invece ottenere con: **regsvr32.exe /u bit4upki-store.dll** La disattivazione del "certificate store" si ottiene tramite la sua deregistrazione.	

Nome	Destinazione
bit4pin.exe	C:\Program Files (x86)\Bit4id\Universal MW\bit4pin.exe
Descrizione	
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.

Nome	Destinazione
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. Tale procedura è effettuata in automatico all'atto dell'installazione per le SmartCard supportate.
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)	"bit4xpki.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".

Apple OSX

La versione OSX del MU è distribuita sotto forma di pacchetto di installazione Apple (**PKG**), contenuto in un file immagine disco (**DMG**). La procedura guidata multilingue (Italiano, Inglese, Tedesco, Spagnolo) consente, previa accettazione del contratto di licenza, di installare automaticamente il middlware e il software di gestione del pin con tutte le sue dipendenze permettendo all'utente l'immediato utilizzo. Il software di gestione del pin (Bit4Id – Smart Card Manager) viene inserito tra le applicazioni del sistema.
Il MU include il modulo per l'iterazione con il servizio di SmartCard dei sistemi Apple denominato TokenD

Caratteristiche del modulo TokenD

1. Libreria compatibile con la specifica TokenD di Apple
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. Supporto della smart card InCard Touch & Sign e Java Sign con doppio Filesystem: Filesystem CNS conforme alla specifica CNS del CNIPA (v.1.1.3) e Filesystem di firma proprietario InCard
4. Supporto della smart card CNS Siemens con Filesystem CNS conforme alla specifica CNS del CNIPA (v.1.1.3)
5. Supporto della smart card CNS Atena con Filesystem CNS conforme alla specifica CNS del CNIPA (v.1.1.3)
6. Funzionamento limitato all'utilizzo nei seguenti contesti applicativi:
    a. autenticazione SSL V3/TLS con Safari, Google Chrome
    b. funzione di "Firma leggera per Attestazione" per applicazioni web
    c. funzione di "Firma Forte" per applicazioni di firma digitale
7. Sistemi operativi sui quali Bit4id certifica il pieno funzionamento ed il superamento dei propri test prima del rilascio:
    a. 10.10
    b. 10.11
8. Rilascio libreria in formato binario sotto form adi libreria a "link dinamico".
9. Applicazione con la quale Bit4id certifica il pieno funzionamento con il superamento dei propri test prima del rilascio: Safari, KeyChain.
10. Caricamento dei certificati presenti sulla smart card in maniera trasparente per l'utente all'inserimento nel lettore.

Su sistema Apple OSX il MU è composto dai seguenti moduli:

Nome	Destinazione
libbit4xpki.dylib	/Library/bit4id/pkcs11/libbit4xpki.dylib'
Descrizione	
Il modulo principale del MU. Tale modulo contiene l'interfaccia PKCS#11.	

Nome	Destinazione
PinManager.app	Area “Applicazioni” di OSX
Descrizione	
E' il modulo per la gestione del PIN.	

Distribuzioni Linux

La versione Linux del MU è distribuita o sotto forma di librerie sciolte oppure sotto forma di pacchetti specifici per la distribuzione.
In particolare sono distribuiti i pacchetti in formato DEB, per distribuzioni Debian/Ubuntu e compatibili. Ed in formato RPM, per distribuzioni Fedora/RedHat e compatibili.

Poichè non tutte le distribuzioni sono pensate per installare direttamente dei pacchetti DEB, potrebbe essere necessario installare le dipendenze in maniera manuale. Fare riferimento alla documentazione della distribuzione per le istruzioni precise.
Qui di seguito elenchiamo i passi necessari sui sistemi Debian ed Ubuntu. Da terminale, come **root** eseguire:
#> apt-get install libccid
#> apt-get install pcscd

Per distribuzioni Fedora e Redhat

#> yum install ccid
#> yum install pcsc-lite

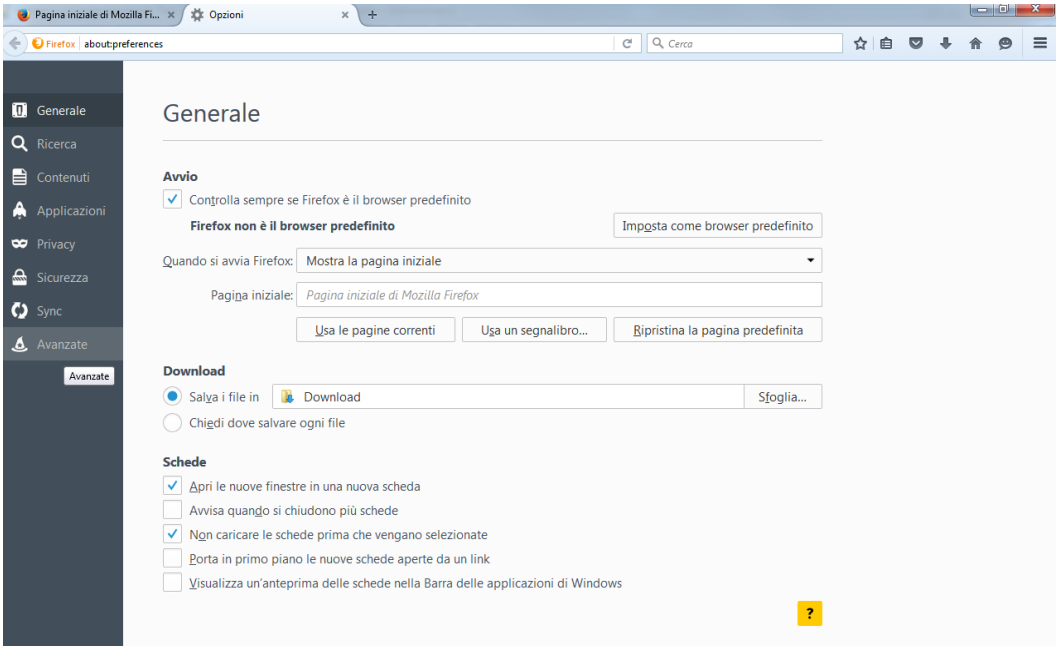
Su Linux il MU è composto dai seguenti moduli:

Nome	Destinazione
libbit4xpki.so	/usr/lib/bit4id/ /usr/lib/
Descrizione	
Il modulo principale del MU. Tale modulo contiene l'interfaccia PKCS#11.	

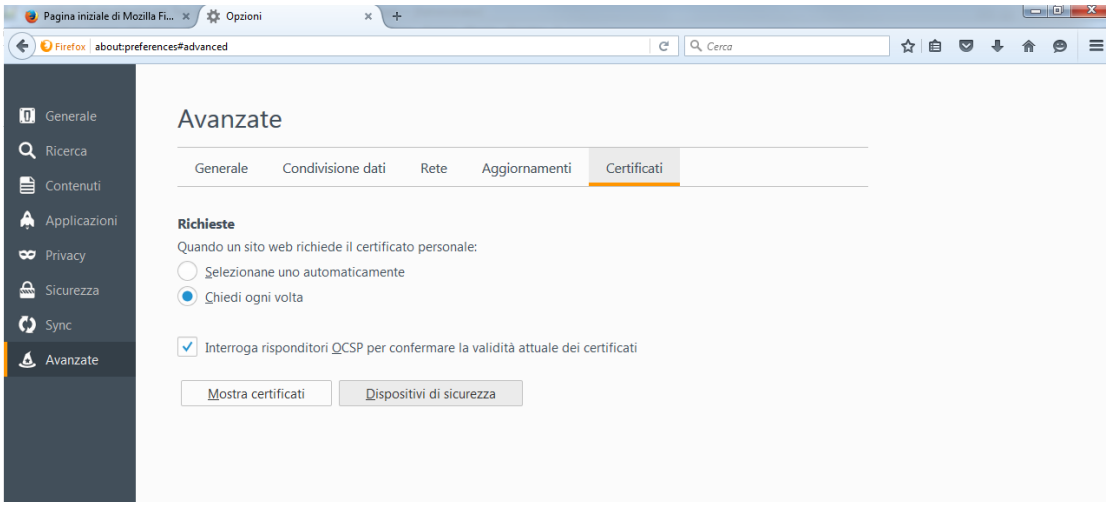
Guida alla configurazione di Firefox

Per permettere l'autenticazione attraverso Mozilla Firefox è necessario caricare il modulo PKCS11 all'interno del browser seguendo i seguenti passi:

- Dal menù "Strumenti \ Opzioni" del browser, selezionare l'icona "Avanzate"

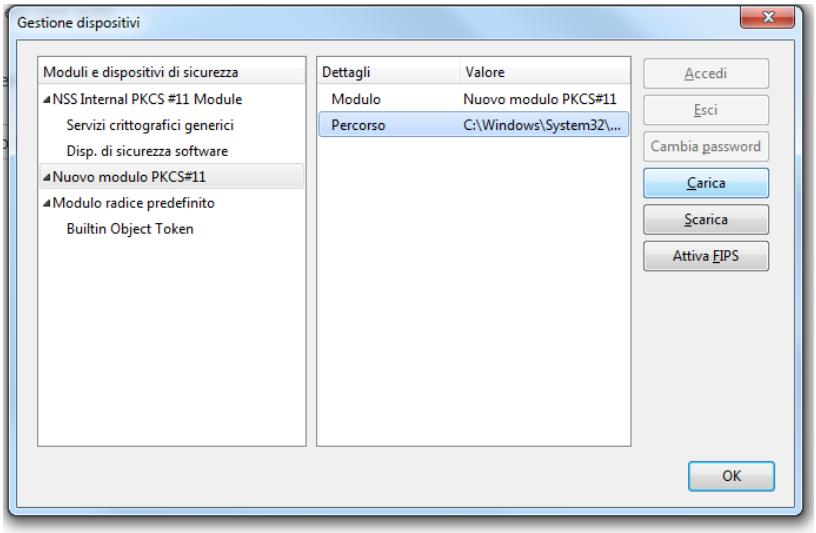


- Cliccare su "Dispositivi di sicurezza"



- Cliccare su "Carica", assegnare un nome modulo a piacere (es. CNS) quindi cliccare su sfoglia e selezionare il modulo PKCS11. Il file bit4xpki.ddl per i sistemi windows, libbit4xpki.dylib per i sistemi osx o libbit4xpki.so per i sistemi linux.

Al termine dell'operazione cliccare OK.


Gestione dispositivi
Moduli e dispositivi di sicurezza
NSS Internal PKCS #11 Module
Servizi crittografici generici
Disp. di sicurezza software
Nuovo modulo PKCS#11
Modulo radice predefinito
Builtin Object Token
Dettagli
Valore
Modulo
Nuovo modulo PKCS#11
Percorso
C:\Windows\System32\...
Accedi
Esci
Cambia password
Carica
Scarica
Attiva FIPS
OK