

SERVIZI INFORMATICI E FORNITURA DI BENI CONNESSI ALLA REALIZZAZIONE,
DISTRIBUZIONE E GESTIONE DELLA CARTA NAZIONALE DEI SERVIZI (CNS)

Manuale Utente della CNS

Smartcard Manager

RAGGRUPPAMENTO TEMPORANEO DI IMPRESE

 <i>Società Mandataria</i>	
 <i>Società Mandante</i>	 <i>Società Mandante</i>
 <i>Società Mandante</i>	 <i>Società Mandante</i>

Codice documento:	213 – 01 - 03
-------------------	----------------------

Versione:	02
-----------	-----------

Distribuzione:	Pubblica
----------------	-----------------

ELENCO DELLE MODICHE APPORTATE			
Data	Versione.	Paragrafo	Modifiche
20 lug 2007	01		Prima versione del documento. Si riferisce alla versione 1.1.4.6 del software Universal Middleware
28 agosto 2009	02		E' stato modificato il nome del file a pag. 19 (C:\WINNT\System32\bit4opki.dll)

Sommario

1	COS'È UNIVERSAL MW?	5
1.1	SCOPO	5
1.2	ELEMENTI PRINCIPALI	5
1.3	TIPI DI CERTIFICATI	5
2	ACRONIMI	5
3	INSTALLAZIONE E RIMOZIONE	8
3.1	REQUISITI DI SISTEMA	8
3.2	PROCEDURA DI INSTALLAZIONE	8
3.3	PROCEDURA DI RIMOZIONE	10
4	GESTORE CARTA	11
4.1	SMARTCARD	12
4.2	CAMBIO PIN	12
4.3	SBLOCCA SMARTCARD	14
4.4	AVANZATE	15
4.5	INFORMAZIONI	16
5	CONFIGURAZIONE AVANZATA	17
6	USO DEL WEB BROWSER/MAILER	18
6.1	CONFIGURAZIONE DEI BROWSER	18
6.2	LETTURA DEI CERTIFICATI	19
6.3	FIRMA E CIFRATURA DI EMAIL	21
6.4	AUTENTICAZIONE WEB	22

Indice delle figure

FIGURA 1: AVVIO INSTALLAZIONE DI UNIVERSAL MIDDLEWARE.....	8
FIGURA 2: SPLASHSCREEN D'INSTALLAZIONE.....	9
FIGURA 3: ACCETTAZIONE LICENZA MU.....	9
FIGURA 4: MENÙ MIDDLEWARE UNIVERSALE.....	10
FIGURA 5: SPLASHSCREEN RIMOZIONE MU.....	10
FIGURA 6: CONTROLLI MU DALLA ICON TRAY.....	11
FIGURA 7: PANNELLO SMARTCARD SENZA CARTE INSERITE.....	12
FIGURA 8: PANNELLO SMARTCARD CON UNA CNS INSERITA.....	12
FIGURA 9: PANNELLO CAMBIO PIN.....	12
FIGURA 10: PANNELLO CAMBIO PIN DI FIRMA.....	13
FIGURA 11: PANNELLO SBLOCCO PIN.....	14
FIGURA 12: PANNELLO SBLOCCO PIN DI FIRMA.....	14
FIGURA 13: PANNELLO AVANZATE.....	15
FIGURA 14: PANNELLO INFORMAZIONI.....	16
FIGURA 15: CRYPTO MODULE IN MOZILLA.....	18
FIGURA 16: CARICAMENTO MODULO PKCS#11 DEL MU.....	19
FIGURA 17: VERIFICA FUNZIONAMENTO MU.....	19
FIGURA 18: STORE DEI CERTIFICATI DI EXPLORER.....	19
FIGURA 19: INSERIMENTO PIN.....	20
FIGURA 20: LISTA CERTIFICATI SULLA CNS.....	20
FIGURA 21: IMPOSTAZIONI PREDEFINITE INVIO MESSAGGI.....	21
FIGURA 22: OPZIONI DI INVIO MESSAGGIO.....	22
FIGURA 23: APERTURA CONNESSIONE PROTETTA.....	23
FIGURA 24: FINE CONNESSIONE PROTETTA.....	23
FIGURA 25: RICHIESTA PIN.....	24
FIGURA 26: SCELTA CERTIFICATO AUTENTICAZIONE SSL.....	24

1 Cos'è UNIVERSAL MW?

1.1 Scopo

UNIVERSAL MW⁴ (MU) è una soluzione completa che permette di eseguire in sicurezza comunicazioni elettroniche e transazioni on-line utilizzando la smartcard “Carta Nazionale dei Servizi”. Firme digitali, crittografie e certificati digitali assicurano l'autenticazione, il controllo degli accessi e la riservatezza.

L'insieme, carta CNS e UNIVERSAL MW⁴, è un passo verso la realizzazione dell'e-governement, cioè l'utilizzo delle nuove tecnologie dell'informazione e della comunicazione (ICT) per rendere la Pubblica Amministrazione sempre più veloce, efficiente e vicina al cittadino.

1.2 Elementi Principali

Gli elementi principali di UNIVERSAL MW⁴ sono:

- Gestione certificati
- Gestione PIN Login (cambio e sblocco)
- Gestione PIN Firma (cambio e sblocco)
- Autenticazione Web per aprire un canale sicuro SSL.
- Operazioni di browser (invio e ricezione di mail firmate e/o criptate)

1.3 Tipi di Certificati

Differenti certificati possono essere utilizzati con UNIVERSAL MW⁴. Un certificato è il passaporto digitale che contiene la chiave pubblica dell'utente ed è usato per:

- Autenticare il mittente
- Verificare l'integrità dei dati
- Provvedere al non ripudio dei dati
- Cifrare i dati spediti al possessore del certificato

Il certificato presente sulla CNS è un certificato di Autenticazione.

2 Acronimi

PKCS#11

Interfaccia di programmazione (API) standard, multi piattaforma, per l'accesso a generici token crittografici, quali le smartcard, 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 smartcard, 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; rappresenta 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 smartcard rappresenta 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 smartcard

PUK

Acronimo che sta per Pin Unblocking Key; nell'ambito delle smartcard 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 smartcard indica la struttura ed il formato dei file e dei dati presenti su una smartcard e che servono a implementare una determinata funzionalità/applicazione.

ATR

Acronimo che sta per **Answer To Reset**; è un codice restituito da una smartcard quando viene inserita nel lettore o resettata. Tale codice viene spesso utilizzato per identificare il tipo di smartcard 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 file system di firma digitale (in questo documento può indicare anche un file system non CNS)

3 Installazione e rimozione

3.1 Requisiti di sistema

UNIVERSAL MW⁴ è un software che richiede modiche risorse hardware e software:

- OS supportati: Windows 2000 SP4, Windows XP SP2, Windows Vista;
- 2 Mb liberi su disco fisso
- 16 Mb RAM
- Lettori Smartcard PC/SC
- Microsoft Internet Explorer 6.0, Mozilla Firefox 1.5, Netscape 7.1 o successivi
- Microsoft Outlook 2000 o Express

N.B.: Alcune diciture nelle figure riportate nel presente documento possono differire dalle schermate che si presentano sul pc, a causa dei vari release di software. Tali differenze non pregiudicano affatto l'installazione o l'utilizzo del prodotto.

3.2 Procedura di installazione

UNIVERSAL MW⁴ (MU) si presenta come un singolo file autoinstallante e autoestraente, denominato: **Universal Middleware.exe**

Per installare il MU, procedere come segue:

1. Uscire da tutti i programmi;
2. Eseguire il **bit4id.exe**. Compare la seguente schermata:

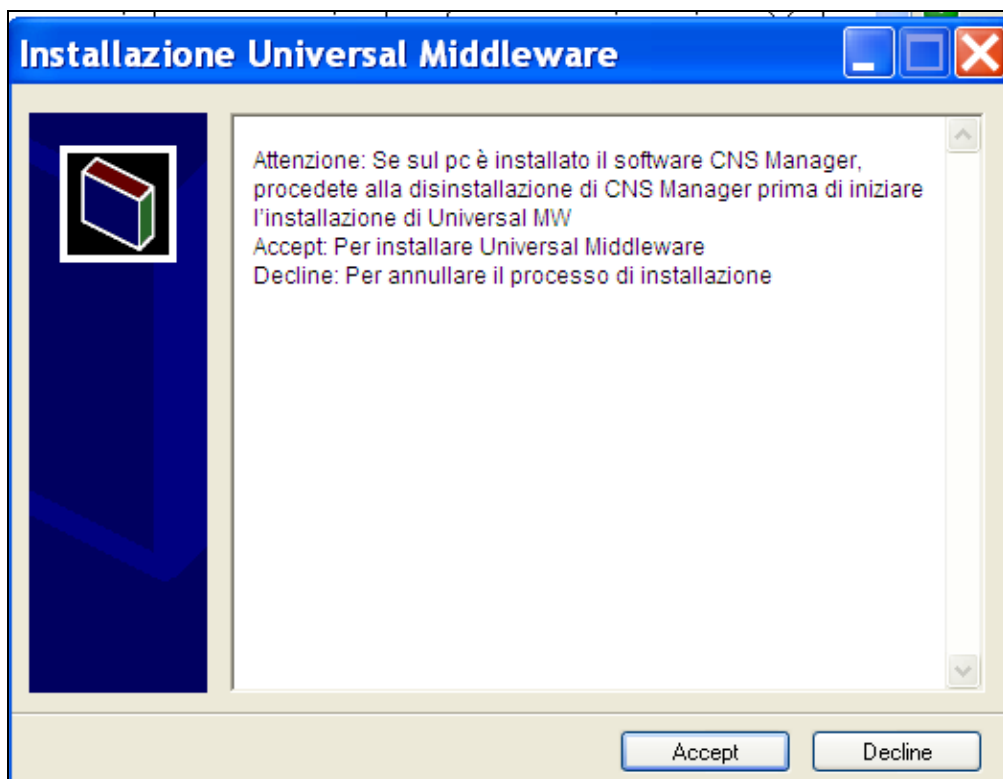


Figura 1: Avvio installazione di Universal Middleware

Verificare che non sia installato il software CNS Manager, nel qual caso chiudere l'installazione di MU (seleziona **Decline**) e procedere alla sua disinstallazione di CNS Manager.

Se CNS Manager non è installato, continuare con l'installazione selezionando **Accept**. Compare la seguente schermata:



Figura 2: Splashscreen d'installazione

3. Premere su “Avanti” per accedere alla schermata di accettazione della licenza d’uso:

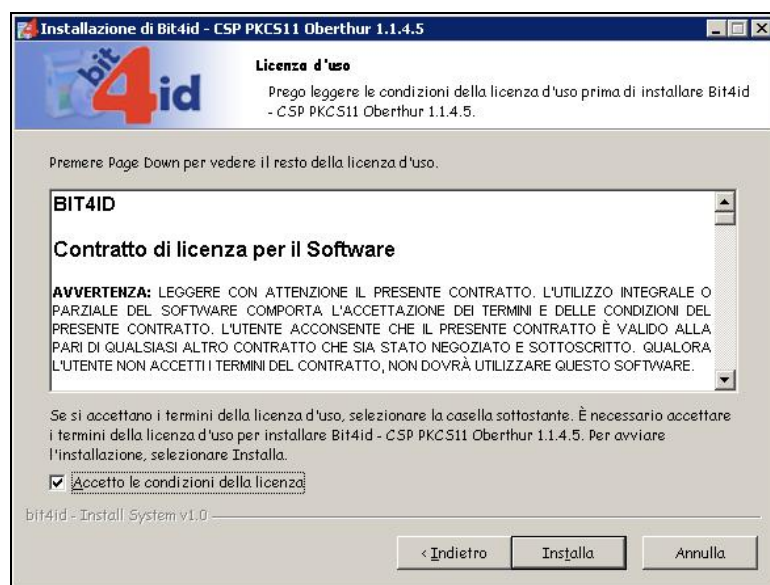



Figura 3: Accettazione licenza MU

4. Dopo aver letto la licenza, se si accetta di proseguire, selezionare la casella “**Accetto le condizioni della licenza**” e cliccare “**Installa**”;
5. A questo punto l'installazione si svolgerà automaticamente fino alla richiesta di riavviare la macchina;
6. Riavviare il computer. Compare l'icona  posizionata “in basso a destra”-

3.3 Procedura di rimozione

La procedura di rimozione è completamente automatica, occorre solo assicurarsi che il MU non sia in esecuzione (ovvero non sia presente il simbolo nella Icon Tray).

Per rimuovere il MU procedere come segue:

1. Accedere alla lista dei programmi e selezionare Bit4id, Bit4id – CSP PKCS11 Oberthur
2. e cliccare su “Disinstallazione”

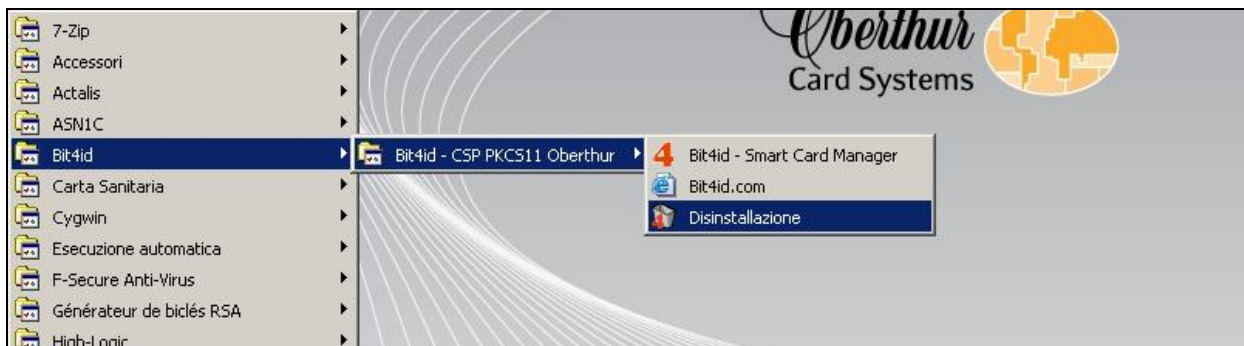


Figura 4: Menù Middleware Universale

3. Appirà la schermata di introduzione; cliccare su “Avanti”;



Figura 5: Splashscreen rimozione MU

4. Seguire le istruzioni di rimozione;
5. Il MU verrà rimosso automaticamente.

4 Gestore carta

Il gestore carta è un'applicazione dotata di interfaccia utente (GUI) che permette di gestire il PIN delle smartcard supportate dal MU.

L'applicazione permette di eseguire le seguenti operazioni:

- ottenere informazioni sulla smartcard inserita;
- cambiare il valore del PIN;
- sbloccare il PIN bloccato usando il codice PUK;
- configurazione avanzata del CSP.

Il gestore carta può essere caricato in automatico (esecuzione automatica) durante l'avvio del sistema oppure caricato esplicitamente selezionando l'icona relativa nel menu start.

Il gestore carta, quando la finestra principale non è visibile, è nascosto 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.

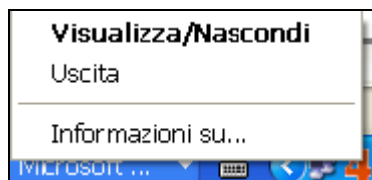


Figura 6: Controlli MU dalla Icon Tray

Il gestore carta rimarrà attivo in background e sarà riattivabile in due modi: lanciandolo nuovamente oppure facendo doppio click sull'icona che l'applicazione installa nella tray bar.

Per terminare completamente il gestore carta, 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 del gestore carta; se essa viene eseguita più volte verrà attivata la finestra dell'istanza precedente.

Il gestore carta è caratterizzato da un'interfaccia a pannelli (o tab), ognuna delle quali fornisce una funzionalità differente.

4.1 Smartcard

Il primo pannello offre all'utente un insieme di informazioni relative allo stato dei lettori e alla carta inserita al momento. E' possibile visualizzare le caratteristiche di una sola carta per volta.



Figura 7: Pannello Smartcard senza carte inserite



Figura 8: Pannello Smartcard con una CNS inserita

4.2 Cambio PIN

Il pannello di cambio PIN consente di gestire le due coppie di PIN-PUK di login e di firma.



Figura 9: Pannello cambio PIN

Il cambiamento di qualsiasi PIN è soggetto al previo inserimento dello stesso per comprovare l'identità dell'utilizzatore della carta.

Nella prima campo di input si richiede all'utente di inserire il vecchio valore del PIN di login e nei due campi restanti si deve digitare due volte (per evitare ogni errore di digitazione) il nuovo valore desiderato del PIN di login.

Tutti i valori inseriti sono offuscati dall'uso di asterischi per prevenire letture indebite di terzi. Non è nemmeno possibile effettuare "copia - incolla" sui campi di queste maschere.

Premendo su "Esegui", l'operazione di cambio PIN verrà concretamente eseguita sulla Smartcard e subito dopo, a seconda della configurazione, compariranno (o meno) le finestre di cambio PIN di firma.

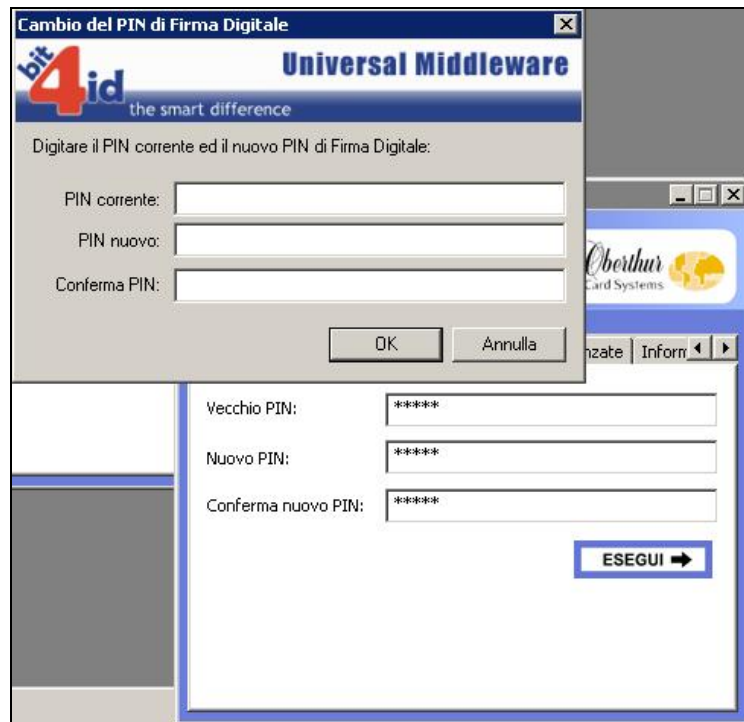


Figura 10: Pannello cambio PIN di firma

La maschera di cambio PIN di firma funziona esattamente come quella di cambio del PIN di login, salvo che va ad impattare sul valore del PIN che protegge le operazioni di firma digitale.

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 smartcard”
- “Il PIN è bloccato” (a causa dei troppi tentativi effettuati con un valore errato)
- “La smartcard 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.

4.3 Sblocca smartcard

La scheda denominata “Sblocca smartcard” 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).



Figura 11: Pannello sblocco PIN

L'operazione di sblocco PIN viene avviata cliccando sul pulsante “Esegui” oppure tramite tasto Invio battuto in uno qualsiasi dei campi.

Nel caso il MU sia stato configurato per gestire separatamente lo sblocco del PIN di firma digitale, comparirà una seconda maschera del tutto equivalente alla prima, ma riferita al PIN di firma.

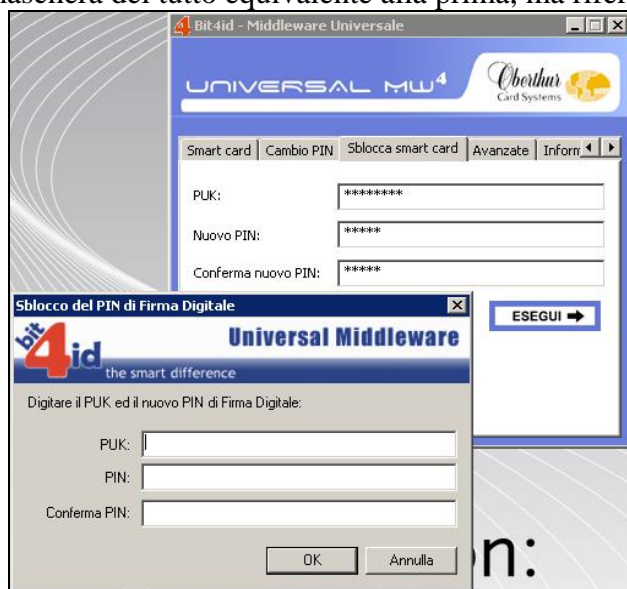


Figura 12: Pannello sblocco PIN di firma

Nel caso in cui si verificasse 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 smartcard”;
- “Il PUK è bloccato”(a causa dei troppi tentativi effettuati con un valore errato);
- “La smartcard 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.

4.4 Avanzate

Nella scheda “Avanzate” è possibile associare la smartcard 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 o Outlook Express. In questa scheda è inoltre possibile importare i certificati di ROOT CA presenti sulla smartcard nello store dei certificati di Windows “Autorità di certificazione attendibili”.



Figura 13: Pannello avanzate

4.5 Informazioni

Il pannello “Informazioni” riporta i riferimenti minimi alla versione del MU in uso, dati relativi al produttore della stessa e altre informazioni utili al supporto tecnico per risolvere eventuali problemi di funzionamento. In base alla versione di MU, compare una delle due seguenti schermate:

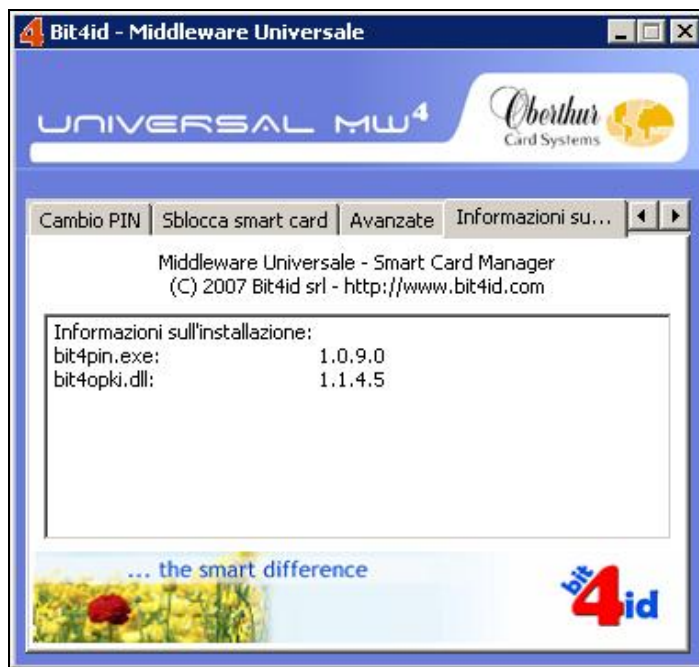


Figura 14: Pannello informazioni

5 Configurazione avanzata

Il MU ha un file di configurazione che permette di variarne il comportamento a seconda delle carte immesse.

Il file di configurazione, che si chiama bit4opki.dll.conf, si trova nella stessa cartella in cui si trova il modulo

principale bit4opki.dll, cioè in “System32”.

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.

Le impostazioni utilizzabili nel file di configurazione sono le seguenti:

Nome	Valori	Descrizione
DSPinIsCnsPin	true / false	Se impostato a “true” il MU suppone l’uguaglianza del PIN di login con quello di firma digitale (e non chiede il PIN di firma a login avvenuto).
DSPinUseGui	true / false	Se impostato a “false” il MU gestisce un eventuale PIN di firma in maniera compliant con 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 utilizzata l’interfaccia grafica (GUI) per recuperare dall’utente il valore del PIN di firma. Il parametro è ignorato quando DSPinIsCnsPin è impostato a “true”. Valore di default: true
HideCacheDsPinCheck	true / false	Se impostato a “true” viene nascosto dall’interfaccia utente che richiede il PIN di firma forte la checkbox che permette di utilizzare lo stesso PIN per più operazioni di firma in sequenza, fino al logout dalla carta. Valore di default: false

6 Uso del web browser/mailer

In questo capitolo sono contenute tutte le informazioni necessarie per utilizzare il MU con i browser più diffusi (Explorer e Mozilla) e per firmare digitalmente i documenti.

Argomenti Principali

In questo capitolo sono trattati i seguenti argomenti:

- Configurazione dei Browser (Internet Explorer e Mozilla FireFox)
- Lettura dei certificati
- Firma e cifratura di email
- Autenticazione Web

6.1 Configurazione dei browser

Internet Explorer

Dopo la corretta installazione del MU, non è necessario fare nulla.

Mozilla FireFox

In questo paragrafo viene descritta la procedura da seguire per configurare Mozilla FireFox in modo che legga automaticamente i certificati contenuti nelle carte riconosciute dal MU.

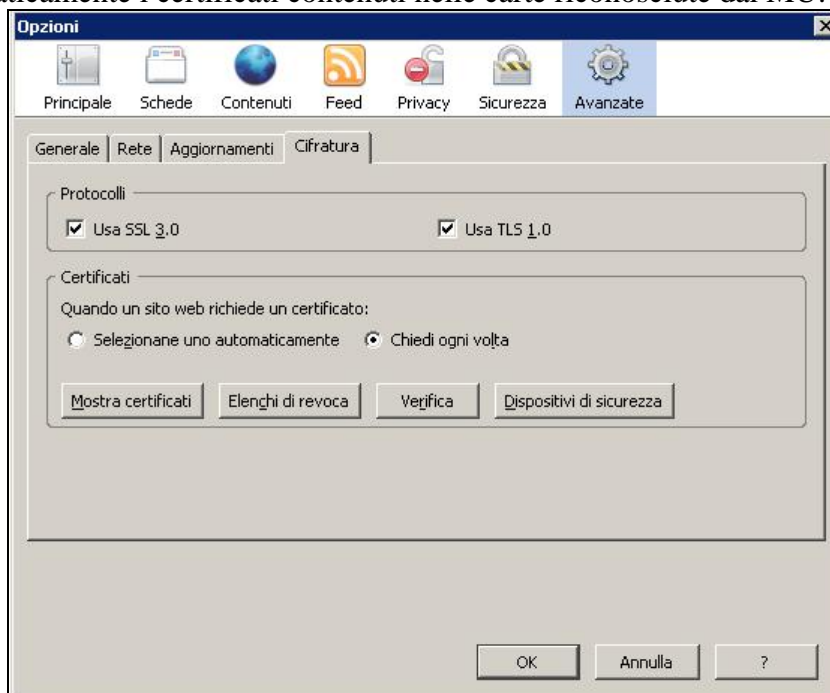


Figura 15: Crypto module in Mozilla

Procedere come segue:

1. Avviare Mozilla FireFox;
2. Aprire il menu “Strumenti -> Opzioni”;
3. Selezionare il sottomenù “Avanzate”;
4. Selezionare il pannello “Cifratura” e cliccare sul pulsante “Dispositivi di sicurezza” (v. Figura 15);
5. Il menù “Dispositivi di sicurezza” permette di gestire i tipi diversi di smartcard supportati sul PC: cliccare su “Carica”;

6. Digitare “Oberthur Crypto Module” come nome per il modulo MU;
7. Selezionare il file C:\WINNT\System32\bit4opki.dll nel campo “Nome file modulo” e cliccare su OK (v. Figura 16)
8. A questo punto il modulo è stato correttamente registrato da Mozilla. Per verificare il corretto funzionamento inserire una CNS e constatare la visualizzazione dei dati essenziali della carta (v. Figura 17)

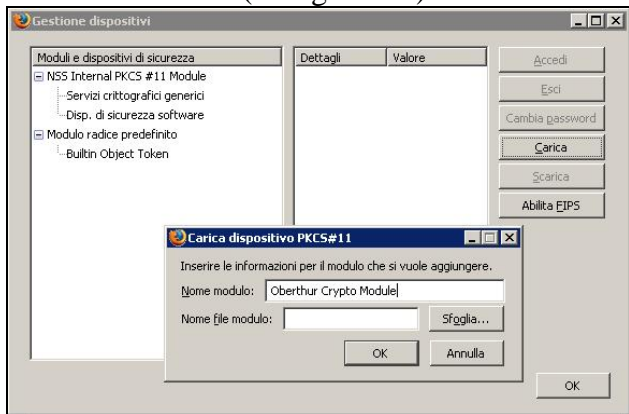


Figura 16: Caricamento modulo PKCS#11 del MU

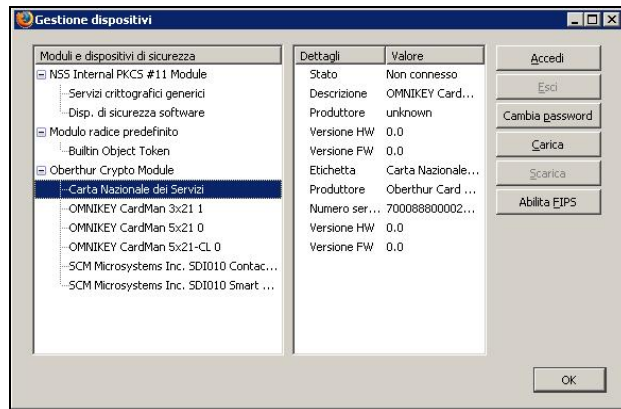


Figura 17: Verifica funzionamento MU

6.2 Lettura dei Certificati

Internet Explorer

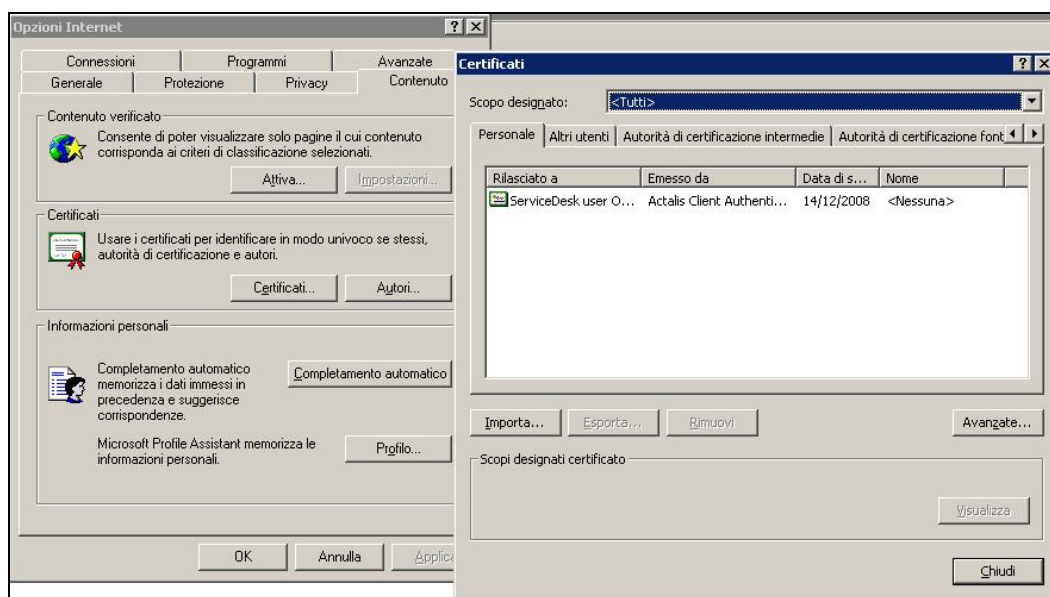


Figura 18: Store dei certificati di Explorer

Per poter leggere un certificato contenuto sulla CNS su Internet Explorer, si proceda nel modo seguente:

1. Inserire la smartcard CNS nel lettore;
2. Avviare Internet Explorer;
3. Nel menu Strumenti, cliccare Opzioni Internet;
4. Selezionare il pannello “Contenuto”;

5. Nell'area Certificati, cliccare il pulsante Certificati per vedere i certificati installati;
6. Apparirà la finestra Certificate Manager (v. Figura 18);
7. Selezionare il certificato e cliccare View;
8. Apparirà la finestra Certificate (v. Figura 18);
9. Cliccare OK, e, una volta terminato il tutto, Close.

Mozilla FireFox

Per poter leggere un certificato su Mozilla FireFox, si proceda nel modo seguente:

1. Inserire la smartcard CNS nel lettore;
2. Avviare Mozilla FireFox;
3. Selezionare Strumenti, Opzioni;
4. Selezionare la sottofinestra Avanzate;
5. Cercare la sezione Certificati;
6. Cliccare sul pulsante Gestione Certificati;
7. Apparirà la finestra Richiesta PIN (v. Figura 19)
8. Inserire il PIN di Login e cliccare OK;
9. Apparirà la finestra Gestione Certificati;
10. Selezionare il pannello "Certificati personali";
11. Cliccare con il tasto sinistro sul certificato corrispondente per selezionarlo e cliccare il pulsante Visualizza (v. Figura 20). Apparirà una descrizione dettagliata del certificato;
12. Cliccare OK per chiudere.

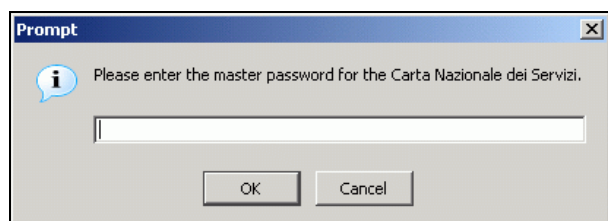


Figura 19: Inserimento PIN

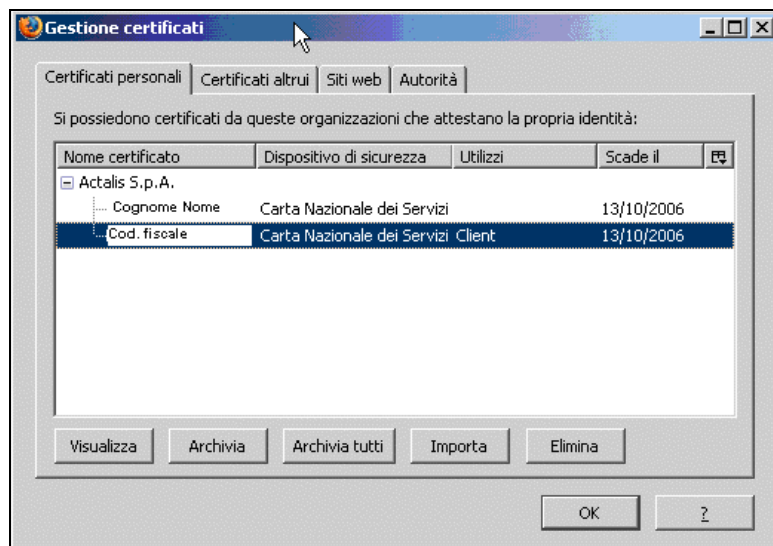


Figura 20: Lista certificati sulla CNS

6.3 Firma e cifratura di email

Questa sezione descrive come spedire e-mail cifrate o firmate utilizzando Microsoft Outlook 2000..

IMPORTANTE: Prima di spedire un messaggio cifrato, è necessario aver ricevuto via email una copia della chiave pubblica del destinatario.

In questo paragrafo si vedrà in primo luogo come selezionare il corretto certificato e successivamente come utilizzarlo per firmare e/o cifrare i messaggi.

Per selezionare il certificato, si proceda come segue:

1. Avviare Outlook;
2. Sulla barra menu Outlook, selezionare Strumenti e Opzioni;
3. Selezionare il tab Protezione. Apparirà la seguente finestra:

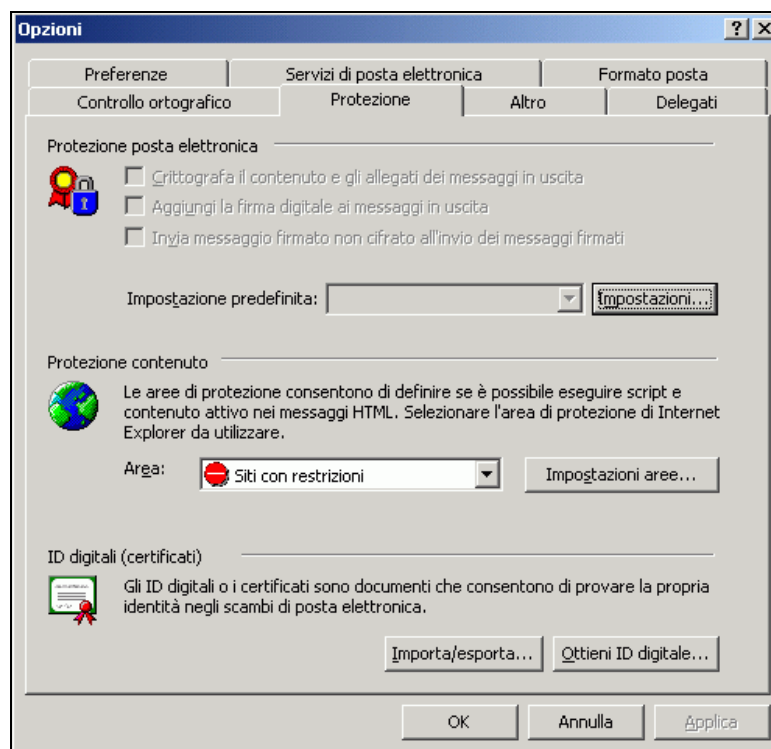


Figura 21: Impostazioni predefinite invio messaggi

4. Cliccare il pulsante Impostazioni;
5. Apparirà la finestra Modifica impostazioni di protezione;
6. Cliccare il pulsante Scegli desiderato (a seconda che si voglia firmare o cifrare il messaggio);
7. Apparirà la finestra Scegli Certificato;
8. Selezionare il certificato e cliccare OK per tornare al pannello “Protezione”;
9. Cliccare OK per tornare alla finestra principale di Outlook.

IMPORTANTE: La procedura di selezione va eseguita solo la prima volta
Dopo aver selezionato il certificato come descritto sopra, si proceda nel modo seguente per cifrare e/o firmare il messaggio e, successivamente, procedere alla spedizione.

1. Scrivere un nuovo messaggio senza spedirlo.
2. Cliccare Options nel menu View.

Apparirà la finestra Message Options:

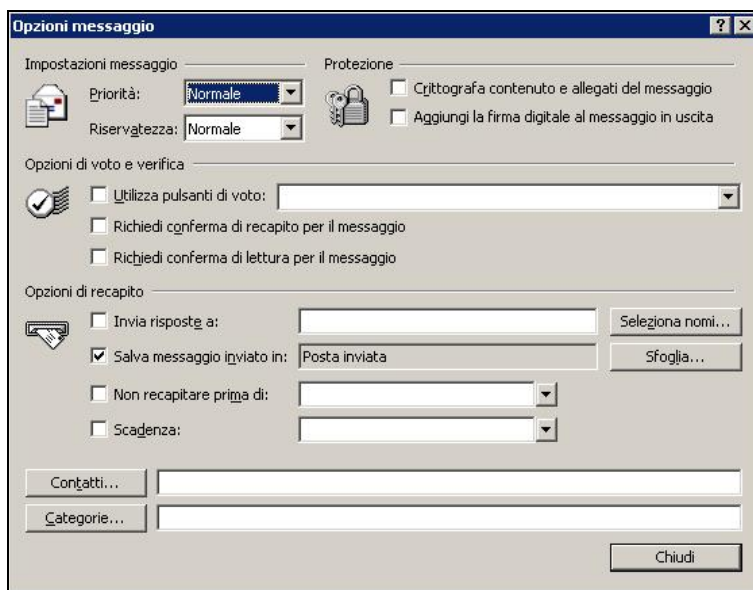


Figura 22: Opzioni di invio messaggio

Per...	Verificare...
Cifrare un messaggio	Il box “Crittografa contenuto e allegati del messaggio”
Firmare un messaggio	Il box “Aggiungi la firma digitale al messaggio in uscita”
Cifrare e firmare un messaggio contemporaneamente	Sia il box “Crittografa contenuto e allegati del messaggio” che il box “Aggiungi la firma digitale al messaggio in uscita”

3. Cliccare Chiudi.
4. Spedire il messaggio.

Il messaggio è stato spedito cifrato e/o firmato come richiesto.

6.4 Autenticazione WEB

La CNS dispone di certificati che permettono l'autenticazione WEB. Normalmente i dati scambiati via internet sono “in chiaro” e un intruso potrebbe indebitamente accedere a informazioni confidenziali. E' possibile, tramite il protocollo SSL (Secure Socket Layer), stabilire un canale di comunicazione criptato e sicuro.

Oltre a questo primo livello di sicurezza, l'autenticazione web è un meccanismo che, grazie alla smartcard CNS, permette al server web di assicurarsi dell'identità dell'utente che cerca di connettersi. Le informazioni riservate comunicate dal server web saranno protette per due ragioni:

1. Sono criptate e firmate, quindi nessuno può né leggerle né modificarle
2. Sono trasmesse solo se l'utente è stato validamente identificato

IMPORTANTE: Se non si importano i certificati ROOT delle certification authorities che hanno emesso il proprio certificato CNS, il browser non permette l'uso dei certificati SSL client.

Qui di seguito la procedura da seguire per autenticarsi su richiesta di un server web che voglia stabilire una sessione SSL.

Internet Explorer

Aperto una connessione sicura con un server web, Explorer avverte che si sta per aprire una sessione protetta:

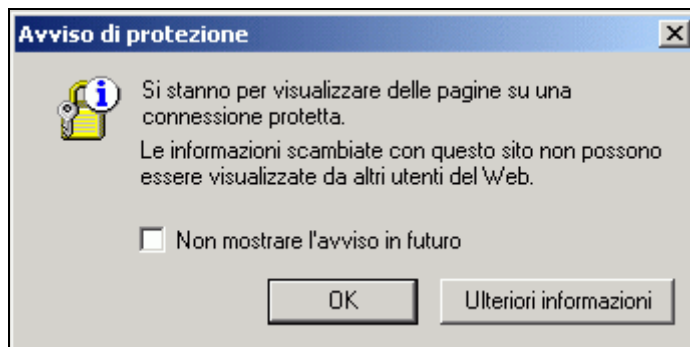



Figura 23: Apertura connessione protetta

Seguire la procedura specificata qui di seguito:

1. Cliccare su OK;
2. Apparirà la finestra di Autenticazione Client dove poter scegliere il certificato di autenticazione desiderato;
3. Scegliere il certificato di autenticazione desiderato e cliccare OK;
4. Da questo momento in avanti la connessione è sicura, cioè nessuno potrà leggere i dati intercorrenti tra server e client. Internet Explorer segnala lo stato di connessione sicura visualizzando  nella sua status bar.

Terminando la connessione sicura, Microsoft Explorer visualizzerà la seguente finestra che avvisa il cambiamento di stato di connessione.

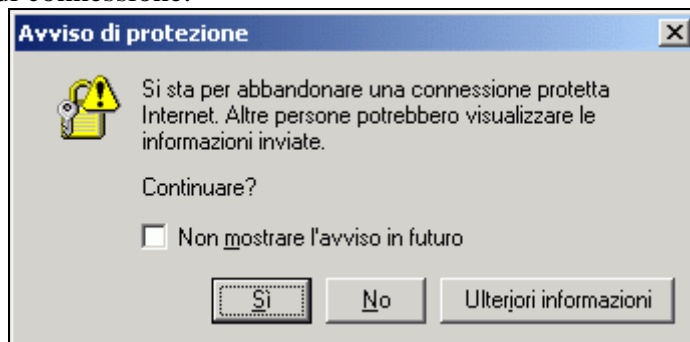


Figura 24: Fine connessione protetta

Mozilla FireFox

Aperto una connessione sicura con un server web, Mozilla FireFox avverte che si sta per aprire una sessione protetta.

Seguire la procedura specificata qui di seguito:

1. Apparirà un prompt di PIN di Login per la CNS:

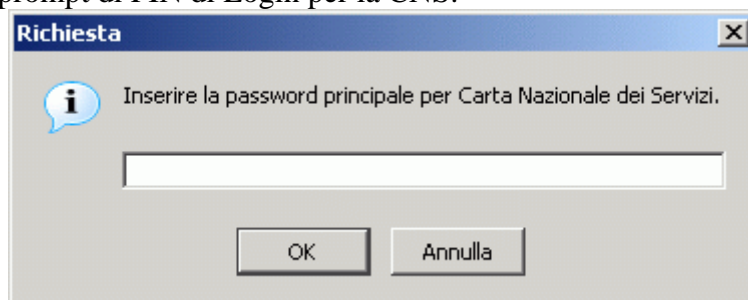


Figura 25: Richiesta PIN

2. Inserire il PIN di Login e cliccare su OK
3. Apparirà la finestra di Richiesta identificazione Utente dove poter scegliere il certificato di autenticazione desiderato

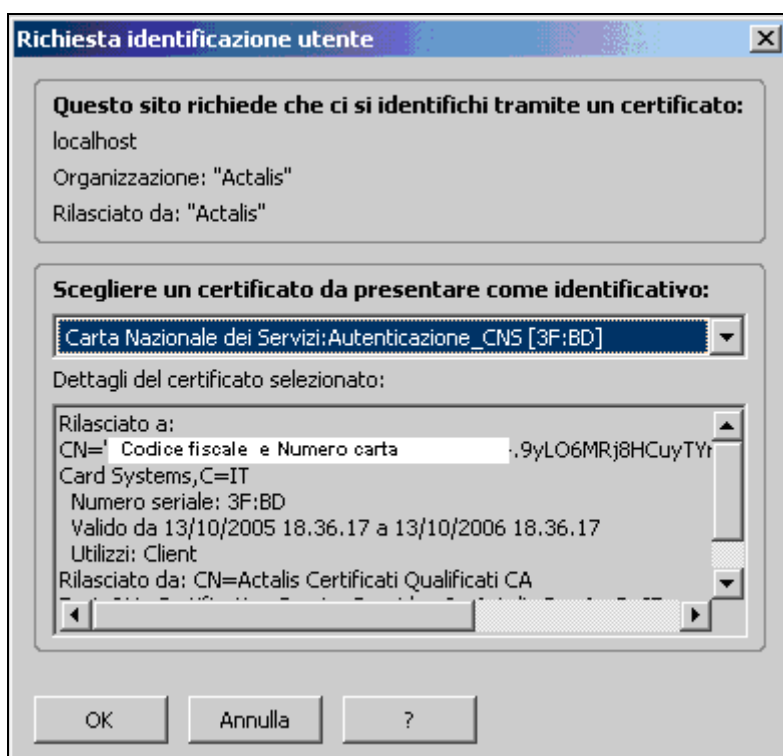



Figura 26: Scelta certificato autenticazione SSL

4. Scegliere il certificato di autenticazione desiderato e cliccare OK

Da questo momento in avanti la connessione è sicura, cioè nessuno potrà leggere i dati intercorrenti tra server e client. Mozilla FireFox segnala lo stato di connessione sicura visualizzando  nella sua status bar e ombreggiando in giallo la barra degli indirizzi.