



Ministero dell'Interno

CIE_CSP

GUIDA UTENTE

Versione 1.0

Data Preparazione 31.10.2001



Nota sul manuale

Le informazioni contenute in questo documento sono soggette a modifiche senza preavviso e non rappresentano un obbligo da parte di Siemens Informatica.

Tutti i nomi di aziende e di prodotti citati all'interno del manuale sono inventati e usati al solo scopo di documentare l'installazione e l'uso del modulo CIE_PKCS11. Questi nomi o parte di essi possono essere marchi commerciali appartenenti ai rispettivi proprietari.



INDICE

Descrizione Generale	4
Introduzione al CIE_CSP.....	5
Come usare il CIE_CSP in ambiente Microsoft.....	6
Scaricare il certificato della smart card sul registro di sistema.....	6
Come usare il certificato della Smart Card per l'autenticazione Client	7
Funzioni CIE_CSP	9
Architettura CIE_CSP.....	9
Funzioni di connessione del CIE_CSP.....	10
Funzioni di generazione di chiavi e di exchange	10
Funzioni di hashing e firma digitale	11
Distribuzione delle licenze	12



Descrizione Generale

Questo manuale guida all'uso del modulo CIE_CSP con i prodotti Microsoft come Internet Explorer.

Viene spiegato come effettuare l'autenticazione con l'impiego delle credenziali della smart card usando il browser Internet Explorer.

Prima di procedere nella lettura è necessario che il modulo CIE_CSP sia stato installato nell'ambiente sw del personal computer (a questo riguardo vedere la "Guida d'installazione del CIE_CSP").



Introduzione al CIE_CSP

Il CIE_CSP è un modulo compatibile con l'architettura PC/SC di Microsoft Windows. Può essere invocato da un'applicazione Crypto-API o usato con Internet Explorer per l'interfacciamento alla CIE smart card.

Si può usare CIE_CSP per accedere e autenticarsi a siti web sicuri con MS IE.

L'operazione più importante che esso realizza è l'impiego della chiave privata. Ogni volta che viene usata una chiave privata viene richiesto il PIN per il consenso all'uso della chiave stessa per qualche operazione "importante", ad esempio la firma di un messaggio o la prova di identità richiesta da un servizio remoto. Per questo motivo è molto importante proteggere attentamente sia la carta che il PIN da un uso non autorizzato.

Come usare il CIE_CSP in ambiente Microsoft

La procedura di setup include l'installazione del CIE_CSP in ambiente Microsoft (W9x, WNT 4.0 e W2k).

SCARICARE IL CERTIFICATO DELLA SMART CARD SUL REGISTRO DI SISTEMA

Il certificato contenuto sulla smart card deve essere introdotto nel sistema prima che possa essere usato da MS IE. A tale scopo è stato progettato un tool speciale (CIECardIntro) distribuito con il sw CIE_CSP e installato dalla procedura di setup.

Per usare CIECardIntro, seguire i seguenti passi:

1. Cliccare su Start Menu / Programs / <Install Dir>¹ / CIE_CSP / CIECardIntro.exe.

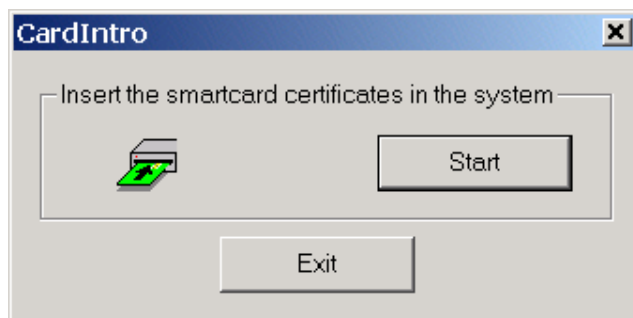


Figure 9 – Menu principale di CIECardIntro

2. Il certificato è associato ad un “Container Name”, identificato del numero della Carta d’Identità. Per introdurre nel sistema il certificato selezionare il ContainerName e cliccare su **Yes**. Cliccando su **NO** si annulla l’operazione. In fig. [10] il nome del ContainerName è esattamente “ContainerName”.

Nota: Un container name è associato non solo al certificato, ma anche alla corrispondente coppia di chiavi. Se sulla smart card è stata generata una coppia di chiavi, ma non è ancora presente un certificato per quella coppia di chiavi, il ContainerName esiste, ma non può essere usato per introdurre il certificato ancora non esistente. In questo caso, CIECardIntro mostra un messaggio di attenzione.

¹ Per default Install Dir = Siemens

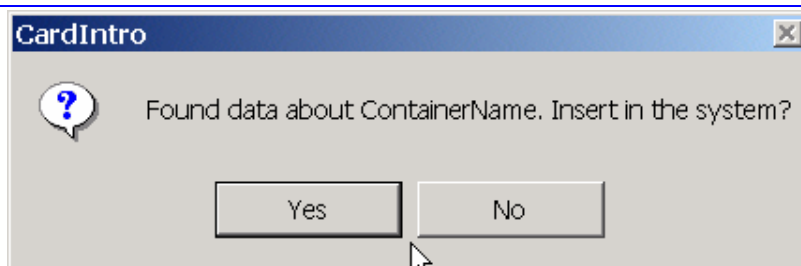


Figura 10 – Finestra del ContainerName

3. A questo punto viene visualizzato il messaggio di Fig. [11].

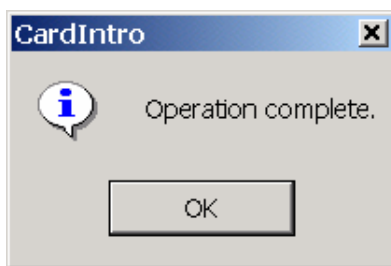


Figura 11 – Messaggio di chiusura di CIECardIntro

COME USARE IL CERTIFICATO DELLA SMART CARD PER L'AUTENTICAZIONE CLIENT

Per usare il protocollo di autenticazione client SSL, seguire i seguenti passi:

1. Introdurre nel sistema il certificato della Smart Card usando CIECardIntro (vedi par. 4.1).
2. Lanciare Microsoft Internet Explorer.
3. Inserire nella barra degli indirizzi l'url "<https://<server-name>>", dove "<server-name>" è il sito web che richiede l'autenticazione client SSL.
4. Durante l'handshake potrebbe apparire una finestra di autenticazione client (Fig. [13]). Selezionare il certificato di autenticazione SSL che si vuole usare, corrispondente con quello della carta inserita nel lettore. In Fig. [12], "SSL Authentication certificate" è solo un nome di fantasia, non il nome che verrà effettivamente visualizzato sullo schermo.

Nota: La finestra di autenticazione client appare solo se sono registrati sul sistema più di un certificato di autenticazione SSL.

5. Inserire il PIN della Smart Card
6. Se il certificato è accettato dal server del sito, è ammesso l'accesso alla pagina richiesta (Fig. [12]).

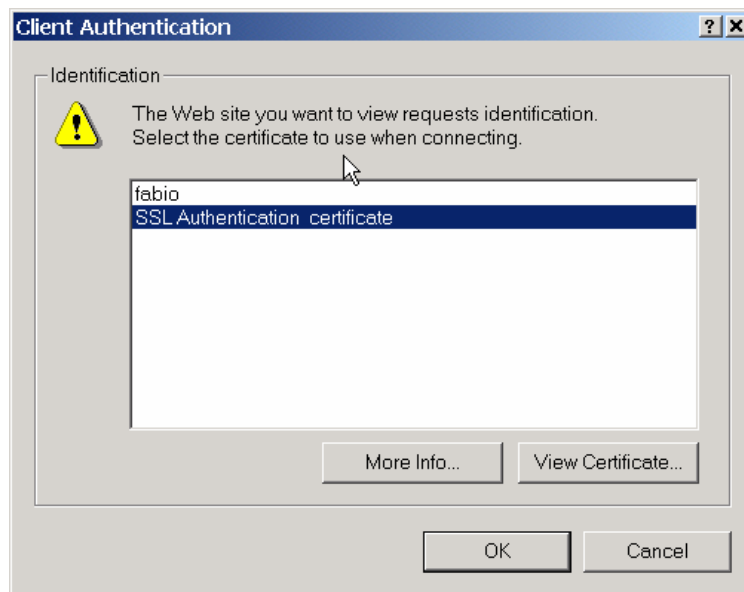


Figura 12– Finestra di autenticazione client di Internet Explorer

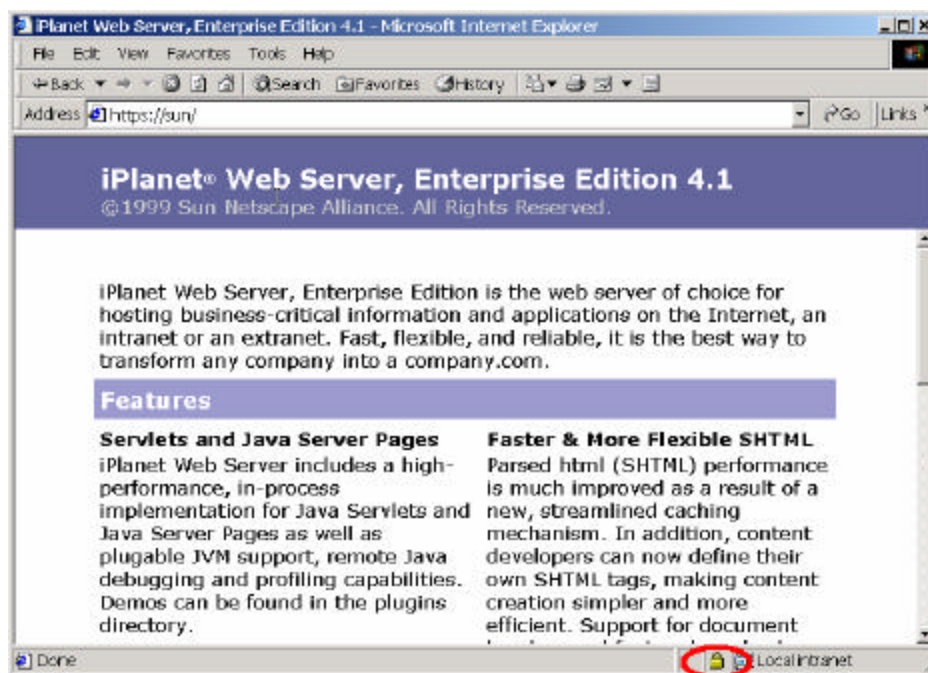


Figura 13 – Autenticazione client SSL riuscita

Funzioni CIE_CSP

Questo capitolo descrive l'architettura del modulo CIE_CSP, dove per CSP si intende "Cryptographic Service Provider".

Un Cryptographic Service Provider è un modulo usato in ambiente Microsoft Windows (Windows 9x, Windows NT, Windows 2000) per operazioni crittografiche.

In questo capitolo sono descritte anche le assunzioni fatte per questa implementazione e una lista degli algoritmi di hash supportati dal CIE_CSP.

ARCHITETTURA CIE_CSP

CIE_CSP è implementato come una DLL che usa una smart card CIE per le principali funzioni crittografiche, nel senso che genera e gestisce le chiavi degli utenti e memorizza il certificato dell'utente direttamente sulla smart card.

La procedura d'installazione include il CIE_CSP nella lista dei Provider Crittografici disponibili su una workstation windows. In questo modo tutte le applicazioni (come ad esempio MS Internet Explorer o Outlook) possono usarlo, generalmente attraverso le funzioni MS Crypto-API (ve di Fig. 14).

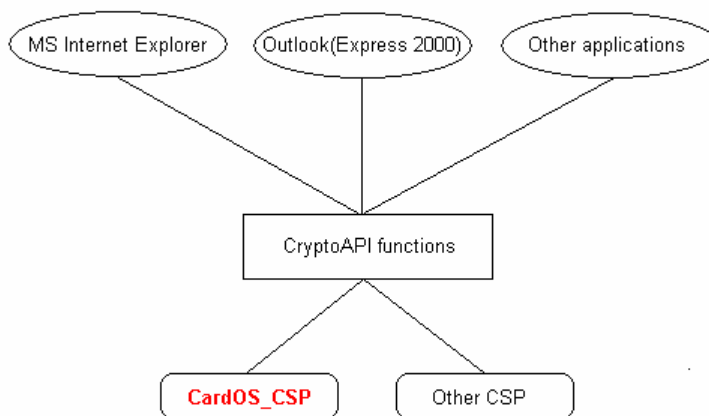


Figura 14 – Architettura CIE_CSP

Nota: Si possono usare direttamente le funzioni CIE_CSP, ma è preferibile usare le Crypto-API specificando CIE_CSP come Cryptographic Service Provider da usare.

Le funzioni implementate dal CIE_CSP possono essere divise nelle seguenti categorie:

1. Funzione di connessione
2. Generazione di chiavi e funzioni di Exchange
3. Funzioni di Hashing e di Firma Digitale

FUNZIONI DI CONNESSIONE DEL CIE_CSP

Queste funzioni sono usate per aprire e chiudere una connessione tra il CIE_CSP e le applicazioni chiamanti. Questo primo blocco di funzioni crea un collegamento tra le applicazioni e il Container Name, ovvero una chiave dell'utente.

Quando un'applicazione o un utente chiama la funzione CryptAcquireContext specificando CIE_CSP come il CSP da usare, il sistema operativo chiama la funzione del CIE_CSP CPAcquireContext per stabilire la connessione. A questo punto tutte le altre funzioni Crypto-API chiamano la funzione CP<funzione> del Provider di Servizi Cryptografici scelto.

Per esempio, se un programma chiama tutte le funzioni CryptGenkey il sistema operativo userà la CPGenkey del CSP precedentemente usato e così via.

La tabella seguente elenca tutte le funzioni di connessione disponibili:

Nome della funzione	Descrizione
CPAcquireContext	Questa funzione acquisisce un riferimento (handle) al CIE_CSP
CPGetProvParam	Restituisce gli attributi del CSP.
CPReleaseContext	Rilascia il contesto precedentemente acquisito dal CPAcquireContext
CPSetProvParam	Imposta attributi specifici del CSP

FUNZIONI DI GENERAZIONE DI CHIAVI E DI EXCHANGE

Le funzioni di generazione di chiavi e di exchange sono usate per creare chiavi in varie modalità (generazione randomica o derivazione di chiave key derivation), per memorizzarle in strutture di dati BLOB (export o import), per ricavare informazioni sulle chiavi e per impostare parametri delle chiavi.

La tabella seguente descrive queste funzioni:

Nome della funzione	Descrizione
CPDeriveKey	Crea una chiave a partire da una password
CPDestroyKey	Distrugge una chiave o rilascia un handle ad essa
CPExportKey	Esporta le chiavi, se possibile, in una struttura BLOB.
CPGenKey	Crea una chiave randomica nella smart card
CPGetKeyParam	Restituisce i parametri di una chiave
CPGetUserKey	Restituisce un handle alla chiave di exchange o alla chiave di firma
CPImportKey	Trasferisce una chiave da un BLOB a un CSP
CPSetKeyParam	Specifica i parametri di una chiave

FUNZIONI DI HASHING E FIRMA DIGITALE

Le funzioni di hash e di firma digitale calcolano gli hashe creano (e verificano) firme digitali. Gli algoritmi di hashing supportati sono:

1. MD2
2. MD5
3. SHA-1
4. SHA-1 MD5

La tabella seguente elenca tutte queste funzioni:

Nome della funzione	Descrizione
CPCreateHash	Crea un oggetto di hash e restituisce un handle ad esso
CPDestroyHash	Distrukge un oggetto di hash o rilascia l'handle all'oggetto di hash
CPGetHashParam	Restituisce un parametro di un oggetto di hash
CPHashData	Esegue l'hash di un blocco di dati, aggiungendolo all'oggetto di hash specificato
CPHashSessionKey	Effettua un hashing di una session key, aggiungendolo all'oggetto di hash specificato
CPSetHashParam	Imposta un parametro di un oggetto di hash
CPSignHash	Firma l'oggetto di hash specificato
CPVerifySignature	Verifica una firma digitale

Distribuzione delle licenze

Questo prodotto include del software crittografico scritto da Eric Young (ey@cryptsoft.com). Pertanto, CIE_PKCS11 V2.0 sottosta a una licenza doppia, ovvero la licenza CIE_PKCS11 e la licenza originale SSLeay.

Vedere di seguito la licenza originale SSLeay.

Original SSLeay License

```
/* Copyright (C) 1995-1998 Eric Young (ey@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (ey@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to. The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code. The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 * notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in the
 * documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 * must display the following acknowledgement:
 * "This product includes cryptographic software written by
 * Eric Young (ey@cryptsoft.com)"
 * The word 'cryptographic' can be left out if the routines from the library
 * being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 * the apps directory (application code) you must include an acknowledgement:
 * "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
```



* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS" AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/