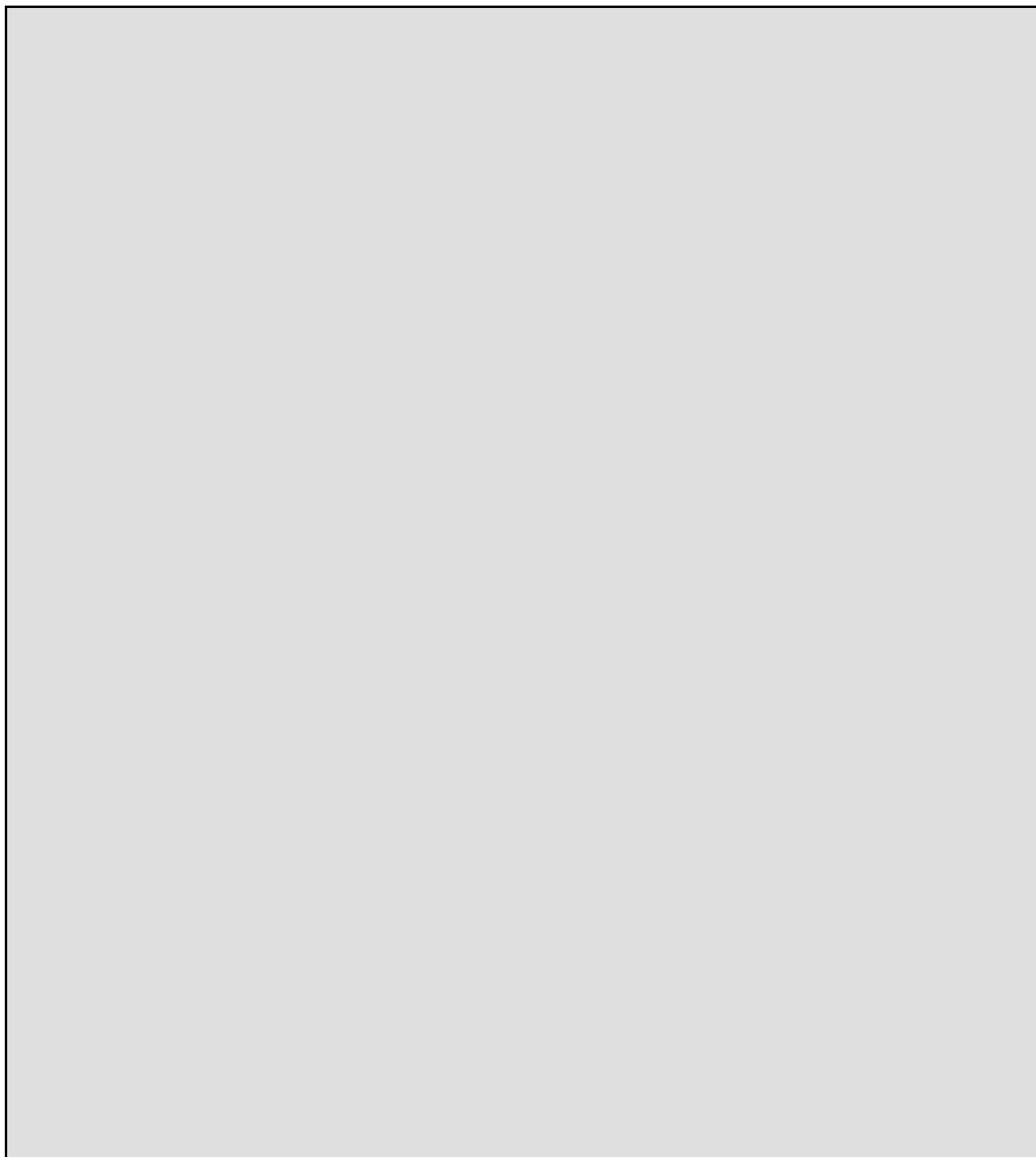


CardOS API V3.3 CNS per Windows

Manuale Utente

Edizione 12/2010



**© Siemens IT Solutions and Services GmbH, 2004 - 2010
All Rights Reserved**

The reproduction, transmission or use of this document or its contents is not permitted without express written authority. Offenders will be liable for damages. All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Siemens IT Solutions and Services GmbH
Otto-Hahn-Ring 6
D-81739 Munich
Germany

Contact:

Siemens IT Solutions and Services GmbH
Smartcard Solutions
Otto-Hahn-Ring 6
D-81739 Munich

Germany

<http://www.siemens.com/cardos>

Disclaimer of Liability

We have checked the contents of this manual for agreement with the hardware and software described. Since deviations cannot be precluded entirely, we cannot guarantee full agreement. However, the data in this manual is reviewed regularly and any necessary corrections are included in subsequent editions. Suggestions for improvement are welcome.

Some of the specifications described herein may not be currently available in all countries. Please contact your local Siemens IT Solutions and Services GmbH sales representative for the most current information.

Subject to change without notice

© Siemens IT Solutions and Services GmbH, 2004 - 2010

CardOS is a registered trademark of
Siemens IT Solutions and Services GmbH.

Contenuti

1	INFORMAZIONI SU QUESTO MANUALE	4
1.1	Destinatari	4
1.2	Schermate	4
1.3	Documentazione	4
2	PANORAMICA DI CARDOS API	5
3	LETTORI A PIN PAD CON INSERIMENTO SICURO DI PIN	6
4	AVVIARE CARDOS API	7
5	MODIFICA PIN	9
6	SBLOCCO PIN	12
7	MODIFICA PUK	15
8	MODIFICA PIN AUT. SEC. (PIN DI FIRMA)	18
9	SBLOCCO PIN SEC. AUT. (SBLOCCO PIN DI FIRMA)	21
10	INFORMAZIONI SU CARDOS API	24
11	NUOVO AVVIO	25
12	CHIUDI	26
13	PROPAGAZIONE DEI CERTIFICATI	27
13.1	Propagazione Automatica dei Certificati	28
13.2	Propagazione Manuale dei Certificati	29
13.3	Propagazione Interattiva dei Certificati	31
14	RISOLUZIONE DEI PROBLEMI	34
15	GLOSSARIO	36

1 Informazioni su questo Manuale

Questo documento contiene una descrizione dettagliata sulle funzioni del CardOS API. Questa sezione comprende dei riferimenti utili nell'utilizzo del manuale utente.

1.1 Destinatari

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

1.2 Schermate

Tutti gli esempi e le schermate mostrate in questo manuale sono state catturate su un sistema Microsoft Windows 7.

Se si sta utilizzando un sistema operativo diverso o una versione differente di CardOS API, le finestre mostrate sullo schermo potrebbero essere leggermente differenti.

Le icone usate nelle schermate hanno il seguente significato:



Nota

Indica un'operazione riuscita o un messaggio importante per l'utente.



Domanda

L'interazione con l'utente è richiesta per completare l'operazione con successo.



Avviso

Indica un evento che non è immediatamente importante, ma che potrebbe causare problemi se lo si ignora.



Errore

Indica un'operazione fallita.

1.3 Documentazione

Fare riferimento alla documentazione seguente per informazioni dettagliate su CardOS API:

- **CardOS API – Note di rilascio**
Questo documento descrive i requisiti di sistema per Windows, Mac OS X, e Linux. Così come, fornisce informazioni sulle applicazioni supportate, nuove funzionalità e problemi noti.
- **CardOS API – Manuale di installazione**
Questo documento fornisce la descrizione dettagliata dei requisiti hardware e software così come le informazioni dettagliate su come installare, aggiornare, riparare, configurare e disinstallare CardOS API in ambiente Windows.
- **CardOS API – Viewer – Manuale utente**
Questo documento fornisce informazioni dettagliate su come usare il tool chiamato Viewer in ambiente Windows.

2 Panoramica di CardOS API

Questo manuale descrive come usare CardOS API nelle attività di tutti i giorni in ambiente Windows.

CardOS API fornisce le seguenti funzionalità:

- **Gestione del PIN**
Modifica del PIN utente, del PUK utente e del PIN di Secondary Authentication, sblocco del PIN utente e del PIN Secondary Authentication.
- **Accesso alla Smart Card tramite PKCS#11**
Accesso alle smart card CardOS attraverso l'interfaccia PKCS#11 Cryptographic Token Interface. Questo permette a tutte le applicazioni che fanno uso di PKCS#11 per le operazioni crittografiche (ad esempio Firefox) di usare i certificati e le chiavi immagazzinate sulle smart card CardOS.
- **Accesso alla Smart Card Access tramite CSP**
Accesso alle smart card CardOS attraverso l'interfaccia Microsoft Cryptographic Service Provider (CSP). La maggiorparte delle applicazioni Microsoft (ad esempio Internet Explorer, Outlook) e le applicazioni di terze parti per piattaforma Microsoft utilizzano questa interfaccia per le operazioni crittografiche.
- **Propagazione dei Certificati**
Propagazione automatica dei certificati immagazzinati sulla smart card CardOS nello store dei certificati Microsoft. Questo permette a tutte le applicazioni che cercano i certificati personali nello store dei certificati Microsoft di utilizzare i certificati e le chiavi immagazzinati sulle smart card CardOS.

Riferirsi al documento CardOS API – Note di rilascio per la lista completa delle applicazioni supportate.

Gestione del PIN utente attraverso l'interfaccia CSP (per esempio Outlook):

CardOS API richiede l'inserimento del PIN utente per ogni operazione di firma.

Per le operazioni di cifra e decifra, tuttavia, CardOS richiede il PIN utente solo la prima volta, in quanto CardOS API il the user is prompted for the User PIN only for the first time, because CardOS API si basa sulla prima autenticazione per tutte le operazioni di decifra.

Gestione del PIN utente attraverso l'interfaccia PKCS#11 (per esempio Firefox):

L'applicazione controlla completamente la richiesta di PIN utente. Tuttavia, se si apre una sessione crittografica, dipende dall'applicazione se viene richiesto il PIN utente ogni volta che bisogna eseguire un'operazione crittografica.

3 Lettori a PIN Pad con inserimento sicuro di PIN

Soprattutto per le applicazioni ad alta sicurezza, il cosiddetto Inserimento Sicuro del PIN (Secure PIN Entry (SPE)) è soggetto a regolamentazioni sulle tastiere. Queste particolari tastiere sono dette PIN pad. I lettori di smart card dotati di PIN pad integrato sono chiamati lettori a PIN pad. Essi sono protetti meccanicamente e crittograficamente, così che il PIN non può essere intercettato durante l'inserimento.

A seconda dei requisiti di sicurezza dell'applicazione, la postazione deve essere connessa con un lettore di smart card che sia conforme alle seguenti classi qui elencate:

- **Lettore Classe 1**
Un lettore classe 1 collega semplicemente la postazione alla smart card. Questi lettori non forniscono alcuna funzionalità per esser conformi a requisiti di sicurezza.
- **Lettore Classe 2**
Un lettore classe 2 consiste di un lettore di smart card con un PIN pad integrato. E' impossibile intercettare il PIN durante il suo inserimento tramite PIN pad.
- **Lettore Classe 3**
Un lettore classe 3 consiste di un lettore di smart card con integrati un PIN pad e un display su cui sono mostrate informazioni, come ad esempio l'ammontare economico, prima che la transazione sia firmata.
- **Lettore Classe 4**
Oltre alle caratteristiche di un lettore classe 3, questa classe di lettori include un modulo che firma ogni transazione. Questo assicura che solo i lettori certificati possono comunicare con le applicazioni corrispondenti.

Se la workstation è connessa con un lettore a PIN pad (Classe 2 o superiore), durante le operazioni di sicurezza, la tastiera viene bypassata, ad esempio ogni volta che si esegue una firma digitale. In questo caso l'applicazione richiede l'inserimento del PIN di Secondary Authentication attraverso il PIN pad del lettore di smart card.

Nota



- A seconda del lettore usato, le finestre visualizzate e il rispettivo comportamento possono essere differenti, ma il numero e il tipo di inserimenti di PIN rimane lo stesso.
- A seconda del lettore usato, gli inserimenti di PIN che eccedono la lunghezza massima configurata, sono considerati come inserimenti scorretti o sono troncati alla lunghezza massima senza messaggi di avviso.

4 Avviare CardOS API

CardOS API è avviato automaticamente durante l'accesso a Windows. Nel caso lo si volesse avviare manualmente, l'icona può essere trovata nel menu *Start* del sistema operativo.

➤ *Start* → *Programmi* → *Esecuzione automatica* → *CardOS API*

Alternativamente usare:

➤ *Start* → *Programmi* → *Siemens* → *CardOS API* → *CardOS API*

CardOS API opera in background. Quando il CardOS API è in esecuzione, un'icona viene mostrata in basso a destra nella barra degli strumenti di Windows.

Questa icona mostra lo stato della carta inserita per ultima.

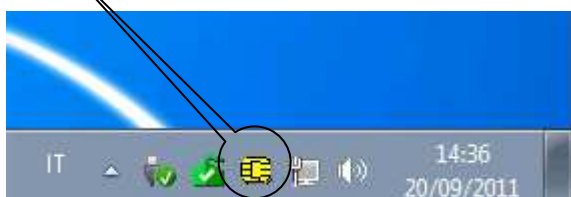







Figura 1

Se si mantiene il puntatore del mouse sull'icona di CardOS API, apparirà un tooltip con le informazioni sulla versione e, quando applicabile, apparirà un messaggio di errore seguito da un codice di errore.

Nella barra delle applicazioni possono apparire le seguenti icone di CardOS API:

 Figura 2	Una icona grigia indica che CardOS API è in attesa di una smart card. L'icona rimane grigia per tutto il tempo in cui alcuna smart card viene inserita nel lettore.
 Figura 3	Una clessidra sta a indicare che una smart card è stata inserita e CardOS API sta propagando i certificati dalla carta allo store dei certificati Microsoft sul computer. Riferirsi alla sezione 13 <i>Propagazione dei Certificati</i> a pagina 27 per maggiori informazioni sull'argomento.
 Figura 4	Una icona gialla è mostrata appena CardOS API ha terminato il processo di propagazione dei certificati. I certificati propagati e le chiavi, che rimangono sempre sulla smart card, possono ora essere utilizzati da qualunque applicazione utilizzi il CSP Microsoft o l'interfaccia PKCS#11 per eseguire le operazioni di firma digitale, cifra e decifra.
 Figura 5	CardOS API ha riconosciuto una smart card nel lettore, ma CardOS API non supporta la carta inserita. Riferirsi alla sezione 14 <i>Risoluzione dei problemi</i> a pagina 34 per maggiori dettagli su cosa fare se questa icona viene mostrata.
 Figura 6	Si è verificato un errore critico. Riferirsi alla sezione 14 <i>Risoluzione dei problemi</i> a pagina 34 per maggiori dettagli su cosa fare se questa icona viene mostrata.

**Avviso**

Se un altro Cryptographic Service Provider (CSP) è installato sul computer, apparirà una finestra simile a quella mostrata in Figura 7 appena si lancia CardOS API. In questo caso è necessario contattare il proprio amministratore di sistema per assistenza.

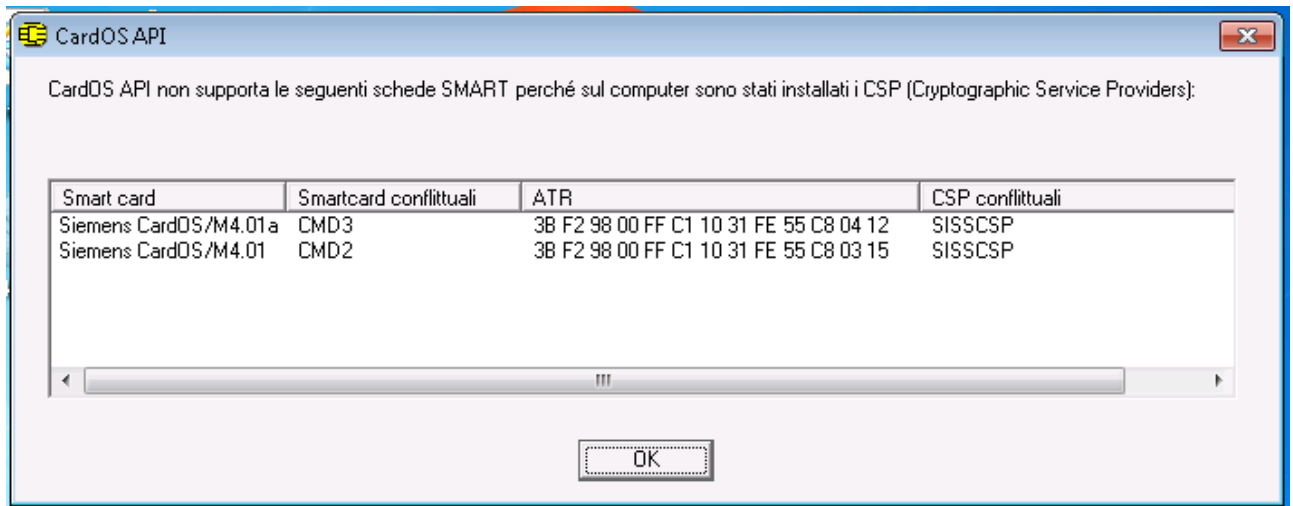


Figura 7

5 Modifica PIN

Se il PIN della smart card è stato compromesso, è consigliabile cambiarlo immediatamente. Un'altra ragione per cambiare il PIN può essere dovuto alle policy di sicurezza della propria azienda che obbligano a cambiare il PIN a intervalli prefissati.

- Passo 1** ➤ Cliccare l'icona del CardOS API nella barra delle applicazioni e selezionare: *Modifica PIN...* (vedere la Figura 8).

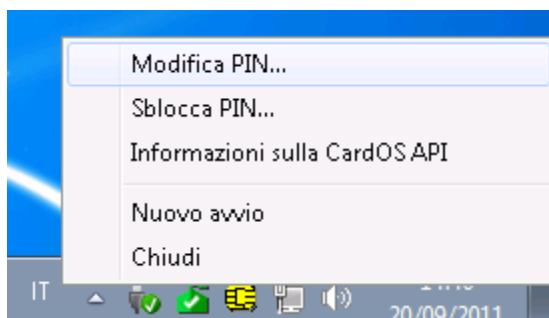


Figura 8

- Alternativamente selezionare: *Start* → *Programmi* → *Siemens* → *CardOS API* → *Modifica PIN*

- Passo 2** Se al PC sono collegati più lettori di smart card con più di una carta inserita, CardOS API chiederà su quale lettore lavorare (vedere la Figura 9).

- Selezionare la smart card con cui lavorare.



Nota

Ogni elemento della lista in Figura 9 consiste del nome del lettore e dell'etichetta della carta inserita. I due elementi sono separati da una virgola.

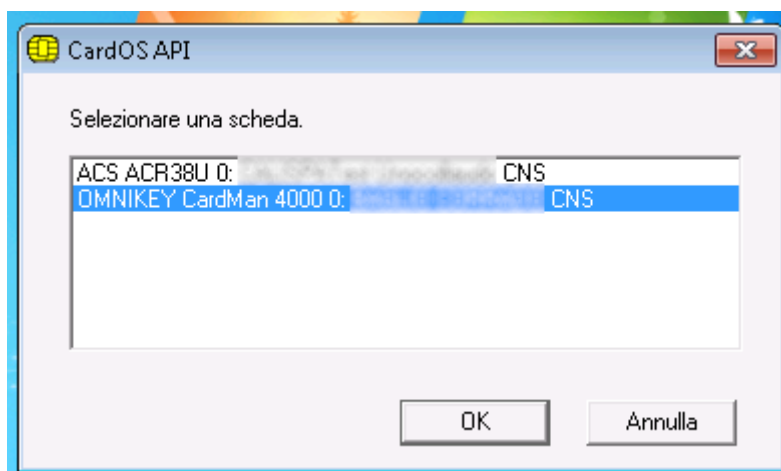


Figura 9

- Cliccare *OK* per confermare la scelta.

- Passo 3** La finestra di *Modifica PIN* viene mostrata (vedere la Figura 10). Le informazioni sull'etichetta della carta (mostrata come *Scheda*) e il lettore di smart card collegato (mostrato come *Lettore*) assicura quale smart card si sta utilizzando.

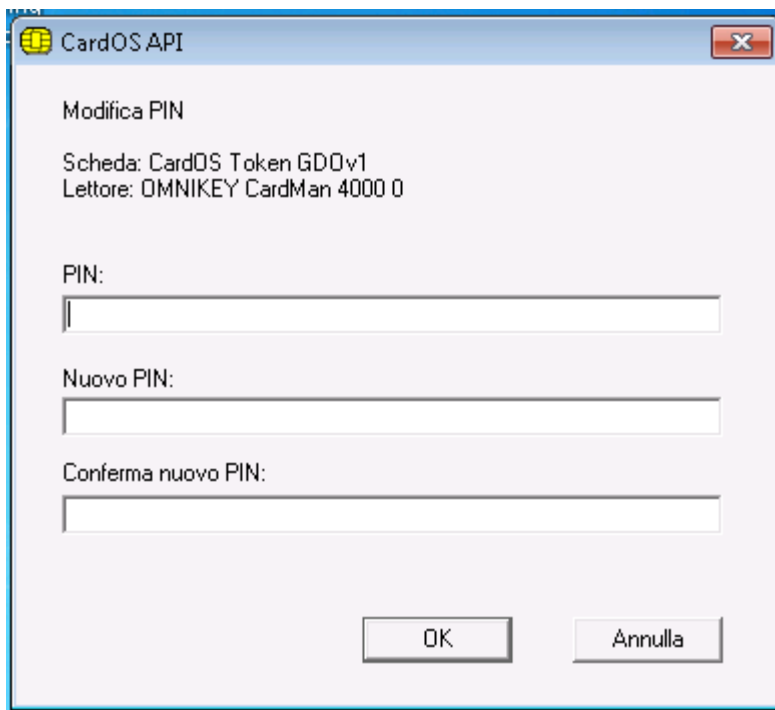


Figura 10








Avviso

Per ragioni di sicurezza, il numero di inserimenti consecutivi errati di PIN è limitato. Il numero massimo¹ di inserimenti errati dipende dalle policy locali policy. Se viene raggiunto il numero massimo di inserimenti errati, il PIN viene bloccato.

- Inserire il PIN attuale.
- Inserire il nuovo PIN.
- Re-inserire il nuovo PIN una seconda volta a scopo di verifica.
- Cliccare *OK* quando le informazioni sono complete.

¹ Il valore di default per il contatore di errori è 3 per il PIN e 10 per il PUK e il PIN aut. sec. Le lunghezze di default vanno da 4 a 16 caratteri.

Passo 4 A seconda delle informazioni inserite, viene mostrato uno dei seguenti messaggi:

Icona	Messaggio mostrato	Cosa si può fare...
	<i>Modifica PIN riuscita.</i>	
	<i>I nuovi PIN inseriti non coincidono. Riprovare.</i>	
	<i>Modifica PIN fallita. Lunghezza PIN non valida.</i>	
	<i>Modifica PIN fallita. Il PIN inserito è sbagliato.</i>	
	<i>Modifica PIN fallita. PIN bloccato.</i>	A seconda delle proprie policy locali, potrebbe essere possibile sbloccare il PIN tramite il PUK. Se non è possibile sbloccare il PIN contattare il proprio amministratore di sistema per maggiore assistenza.

6 Sblocco PIN

Nel caso in cui il PIN si fosse bloccato a causa di troppi tentativi errati consecutivi (3 volte di solito), è necessario sbloccare il PIN tramite il PUK.

- Passo 1** ➤ Cliccare l'icona CardOS API nella barra delle applicazioni e selezionare: *Sblocca PIN...* (Vedere Figura 11).

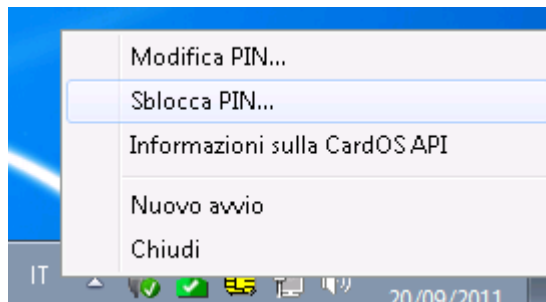



Figura 11

- Alternativamente selezionare: *Start* → *Programmi* → *Siemens* → *CardOS API* → *Sblocco PIN*

- Passo 2** Se al PC sono collegati più lettori di smart card con più di una carta inserita, CardOS API chiederà su quale lettore lavorare (vedere la Figura 12).

- Selezionare la smart card con cui lavorare.

Nota

 Ogni elemento della lista in Figura 12 consiste del nome del lettore e dell'etichetta della carta inserita. I due elementi sono separati da una virgola.

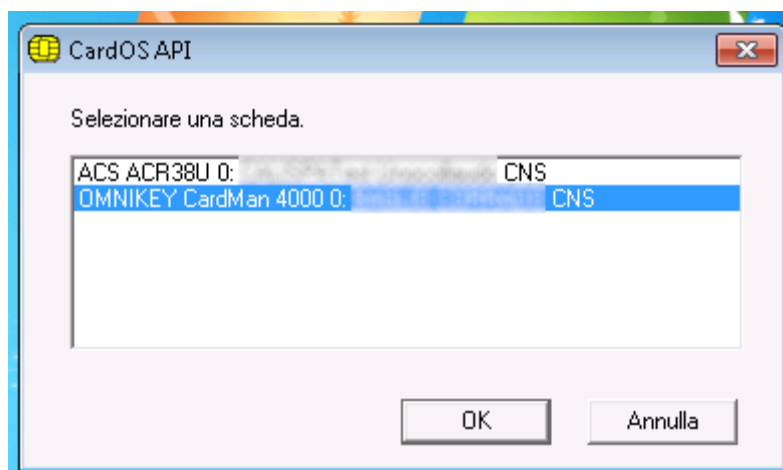


Figura 12

- Cliccare *OK* per confermare la scelta.

- Passo 3** La finestra di *Sblocco PIN* viene mostrata (vedere la Figura 10).
Le informazioni sull'etichetta della carta (mostrata come *Scheda*) e il lettore di smart card collegato (mostrato come *Lettore*) assicura quale smart card si sta utilizzando.

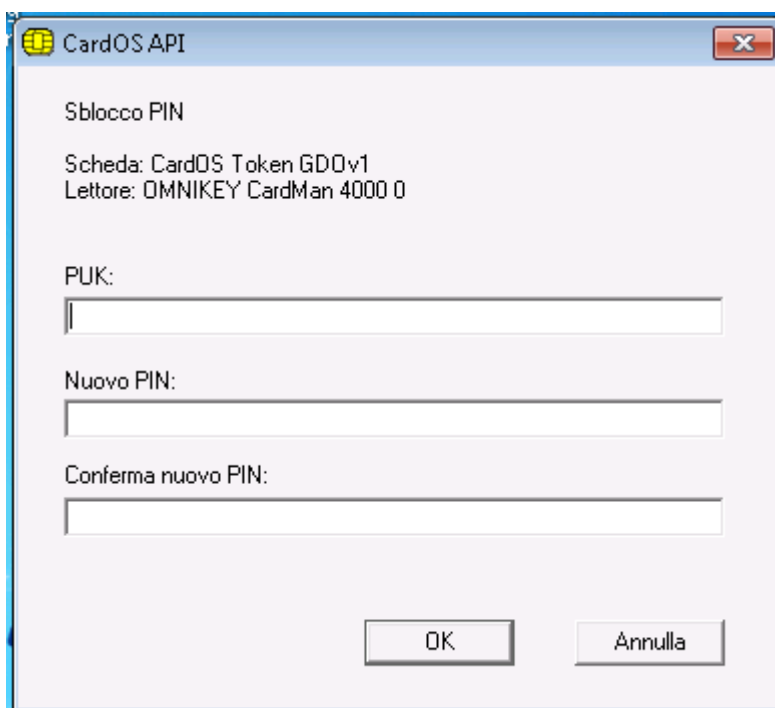


Figura 13






**Avviso**

Per ragioni di sicurezza, il numero di inserimenti consecutivi errati di PUK è limitato. Il numero massimo² di inserimenti errati dipende dalle policy locali policy. Se viene raggiunto il numero massimo di inserimenti errati, la smart card viene irreversibilmente bloccata.

- Inserire il PUK attuale.
- Inserire il nuovo PIN.
- Re-inserire il nuovo PIN una seconda volta a scopo di verifica.
- Cliccare *OK* quando le informazioni sono complete.

² Il valore di default per il contatore di errori è 3 per il PIN e 10 per il PUK e il PIN aut. sec. Le lunghezze di default vanno da 4 a 16 caratteri.

Passo 4 A seconda delle informazioni inserite, viene mostrato uno dei seguenti messaggi:

Icona	Messaggio mostrato	Cosa si può fare...
	<i>Sblocco PIN riuscito.</i>	
	<i>I nuovi PIN inseriti non coincidono. Riprovare.</i>	
	<i>Sblocco PIN fallito. Lunghezza PIN non valida.</i>	
	<i>Sblocco PIN fallito. Il PUK inserito è sbagliato</i>	
	<i>Sblocco PIN fallito. PUK bloccato.</i>	Il numero massimo di inserimenti scorretti del PUK è stato raggiunto, la carta è irreversibilmente bloccata. Contattare il proprio amministratore di sistema per maggiore assistenza.


7 Modifica PUK

Se il PUK della smart card è stato compromesso, è consigliabile cambiare immediatamente il PUK.

Passo 1 ➤ Selezionare: *Start* → *Programmi* → *Siemens* → *CardOS API* → *Modifica PUK*

Passo 2 Se al PC sono collegati più lettori di smart card con più di una carta inserita, CardOS API chiederà su quale lettore lavorare (vedere la Figura 14).

➤ Selezionare la smart card con cui lavorare.

 **Nota**
Ogni elemento della lista in Figura 14 consiste del nome del lettore e dell'etichetta della carta inserita. I due elementi sono separati da una virgola.

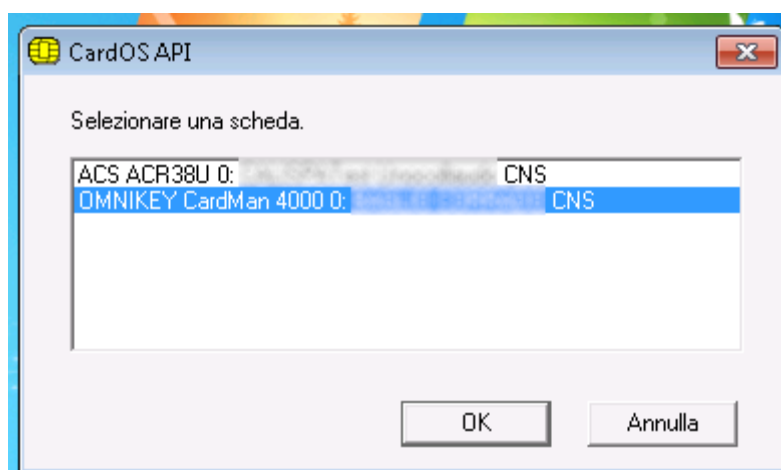


Figura 14

➤ Cliccare *OK* per confermare la scelta.

- Passo 3** La finestra di *Modifica PUK* viene mostrata (vedere la Figura 15). Le informazioni sull'etichetta della carta (mostrata come *Scheda*) e il lettore di smart card collegato (mostrato come *Lettore*) assicura quale smart card si sta utilizzando.

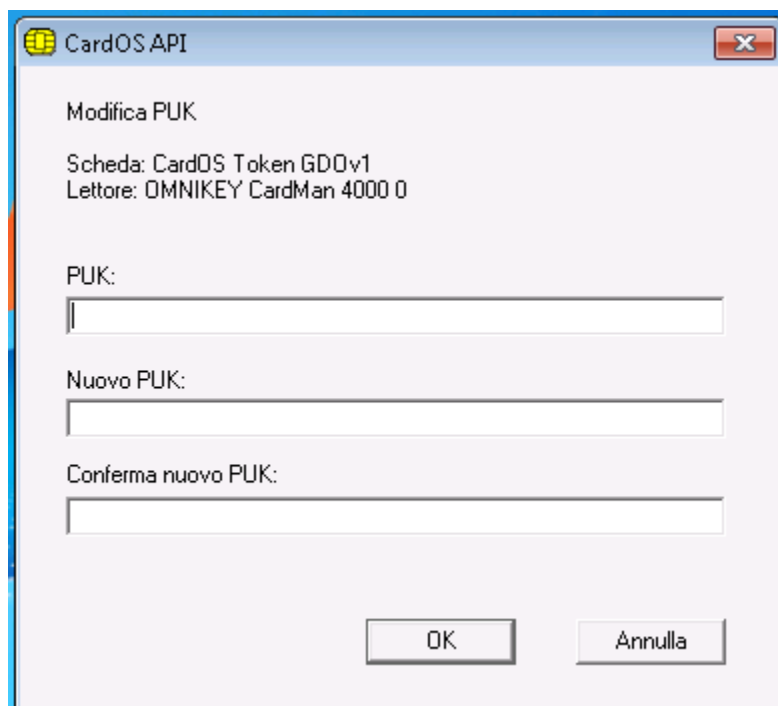



Figura 15








Avviso
Per ragioni di sicurezza, il numero di inserimenti consecutivi errati di PUK è limitato. Il numero massimo³ di inserimenti errati dipende dalle policy locali policy. Se viene raggiunto il numero massimo di inserimenti errati, la smart card viene irreversibilmente bloccata.

- Inserire il PUK attuale.
- Inserire il nuovo PUK.
- Re-inserire il nuovo PUK una seconda volta a scopo di verifica.
- Cliccare *OK* quando le informazioni sono complete.

³ Il valore di default per il contatore di errori è 3 per il PIN e 10 per il PUK e il PIN aut. sec. Le lunghezze di default vanno da 4 a 16 caratteri.

Passo 4 A seconda delle informazioni inserite, viene mostrato uno dei seguenti messaggi:

Icona	Messaggio mostrato	Cosa si può fare...
	<i>Modifica PUK riuscita.</i>	
	<i>I nuovi PUK inseriti non coincidono. Riprovare.</i>	
	<i>Modifica PUK fallita. Lunghezza PUK non valida.</i>	
	<i>Modifica PUK fallita. Il PUK inserito è sbagliato.</i>	
	<i>Modifica PUK fallita. PUK bloccato.</i>	Il numero massimo di inserimenti scorretti del PUK è stato raggiunto, la carta è irreversibilmente bloccata. Contattare il proprio amministratore di sistema per maggiore assistenza.


8 Modifica Pin aut. sec. (PIN di Firma)

Se il Secondary Authentication PIN (PIN di Firma) della smart card è stato compromesso, è consigliabile cambiarlo immediatamente.

Passo 1 ➤ Selezionare: *Start* → *Programmi* → *Siemens* → *CardOS API* → *Modifica PIN aut. sec.*

Passo 2 Se al PC sono collegati più lettori di smart card con più di una carta inserita, CardOS API chiederà su quale lettore lavorare (vedere la Figura 16).

➤ Selezionare la smart card con cui lavorare.

 **Nota**
Ogni elemento della lista in Figura 16 consiste del nome del lettore e dell'etichetta della carta inserita. I due elementi sono separati da una virgola.

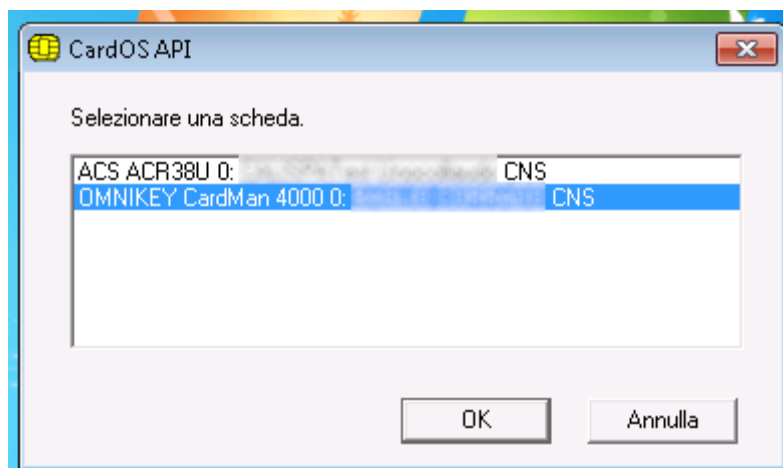


Figura 16

➤ Cliccare *OK* per confermare la scelta.

- Passo 3** La finestra di *Modifica PIN DS* viene mostrata (vedere la Figura 17). Le informazioni sull'etichetta della carta (mostrata come *Scheda*) e il lettore di smart card collegato (mostrato come *Lettore*) assicura quale smart card si sta utilizzando.

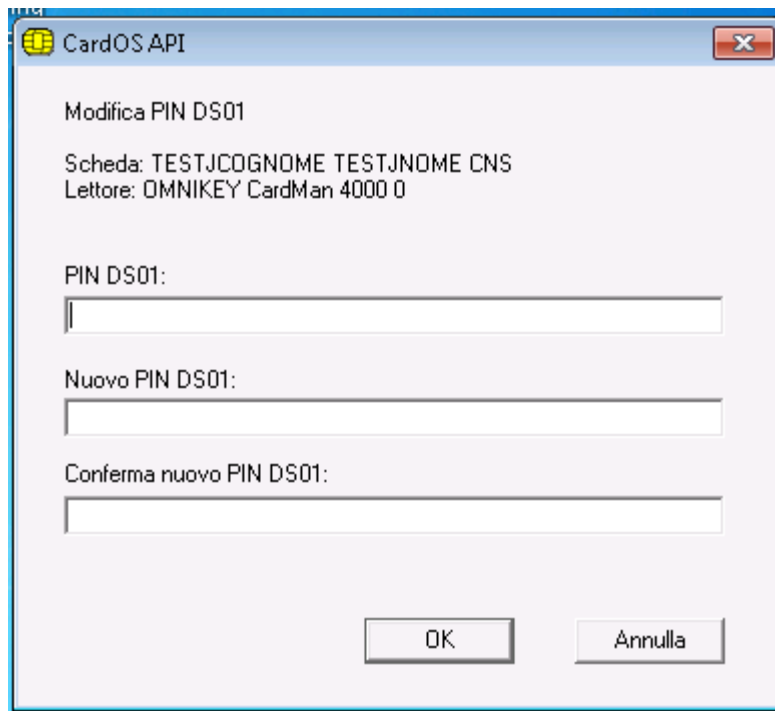


Figura 17






**Avviso**

Per ragioni di sicurezza, il numero di inserimenti consecutivi errati di PIN aut. sec. è limitato. Il numero massimo⁴ di inserimenti errati dipende dalle policy locali policy. Se viene raggiunto il numero massimo di inserimenti errati, il PIN aut. sec. viene bloccato.

- Inserire il PIN DS attuale.
- Inserire il nuovo PIN DS.
- Re-inserire il nuovo PIN DS una seconda volta a scopo di verifica.
- Cliccare *OK* quando le informazioni sono complete.

⁴ Il valore di default per il contatore di errori è 3 per il PIN e 10 per il PUK e il PIN aut. sec. Le lunghezze di default vanno da 4 a 16 caratteri.

Passo 4 A seconda delle informazioni inserite, viene mostrato uno dei seguenti messaggi:

Icona	Messaggio mostrato	Cosa si può fare...
	<i>The Secondary Auth PIN has been successfully changed.</i>	
	<i>I nuovi PIN DS inseriti non coincidono. Riprovare.</i>	
	<i>Modifica PIN DS fallita. Lunghezza PIN DS non valida.</i>	
	<i>Modifica PIN DS fallita. Il PIN DS inserito è sbagliato.</i>	
	<i>Modifica PIN DS fallita. PIN DS bloccato.</i>	

A seconda delle proprie policy locali, potrebbe essere possibile sbloccare il PIN aut. sec. tramite il PUK aut. sec. Se non è possibile sbloccare il PIN aut. sec. contattare il proprio amministratore di sistema per maggiore assistenza.


9 Sblocco PIN sec. aut. (Sblocco PIN di Firma)

Nel caso in cui il Secondary Authentication PIN (PIN di Firma) si fosse bloccato a causa di troppi tentativi errati consecutivi (3 volte di solito), è necessario sbloccare il Secondary Authentication PIN tramite il Secondary Authentication PUK.

Passo 1 ➤ Selezionare: *Start* → *Programmi* → *Siemens* → *CardOS API* → *Sblocco PIN aut. sec.*

Passo 2 Se al PC sono collegati più lettori di smart card con più di una carta inserita, CardOS API chiederà su quale lettore lavorare (vedere la Figura 18).

➤ Selezionare la smart card con cui lavorare.

 **Nota**
Ogni elemento della lista in Figura 18 consiste del nome del lettore e dell'etichetta della carta inserita. I due elementi sono separati da una virgola.

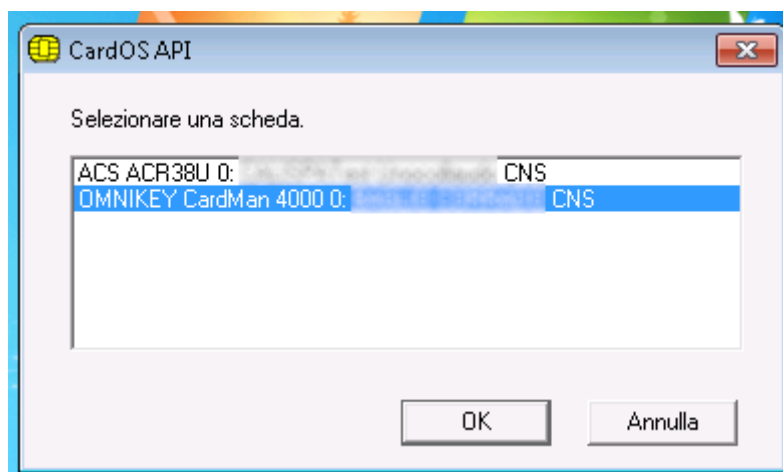


Figura 18

➤ Cliccare *OK* per confermare la scelta.

Passo 3 La finestra di *Sblocco PIN DS* viene mostrata (vedere la Figura 19).
Le informazioni sull'etichetta della carta (mostrata come *Scheda*) e il lettore di smart card collegato (mostrato come *Lettore*) assicura quale smart card si sta utilizzando.

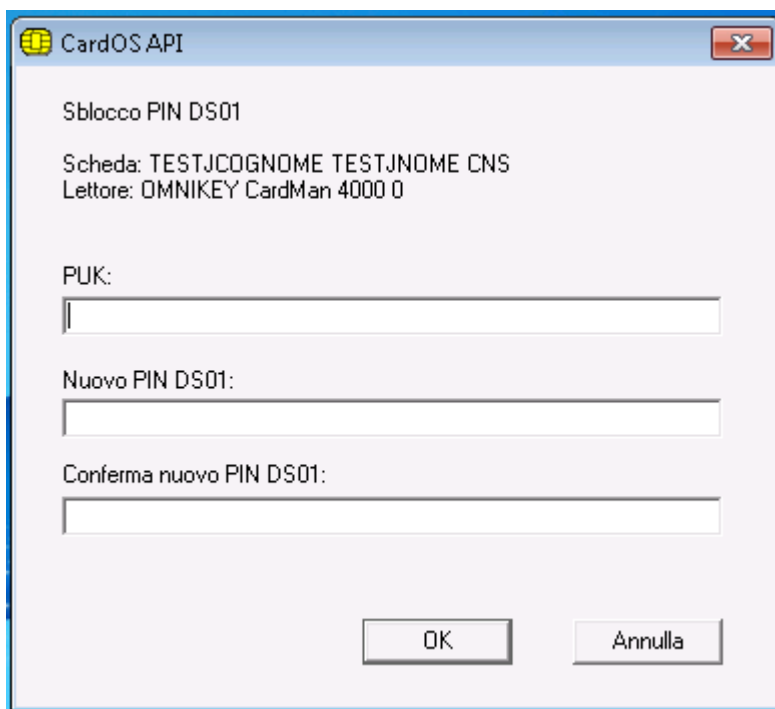


Figura 19








Avviso

Per ragioni di sicurezza, il numero di inserimenti consecutivi errati di PUK è limitato. Il numero massimo⁵ di inserimenti errati dipende dalle policy locali policy. Se viene raggiunto il numero massimo di inserimenti errati, la smart card viene irreversibilmente bloccata.

- Inserire il PUK DS attuale.
- Inserire il nuovo PIN DS.
- Re-inserire il nuovo PIN DS una seconda volta a scopo di verifica.
- Cliccare *OK* quando le informazioni sono complete.

⁵ Il valore di default per il contatore di errori è 3 per il PIN e 10 per il PUK e il PIN aut. sec. Le lunghezze di default vanno da 4 a 16 caratteri.

Passo 4 A seconda delle informazioni inserite, viene mostrato uno dei seguenti messaggi:

Icona	Messaggio mostrato	Cosa si può fare...
	<i>Sblocco PIN DS riuscito.</i>	
	<i>I nuovi PIN DS inseriti non coincidono. Riprovare.</i>	
	<i>Sblocco PIN DS fallito. Lunghezza PIN DS non valida.</i>	
	<i>Sblocco PIN DS fallito. Il PUK DS inserito è sbagliato</i>	
	<i>Sblocco PIN DS fallito. PUK DS bloccato.</i>	Il numero massimo di inserimenti scorretti del PUK è stato raggiunto, la carta è irreversibilmente bloccata. Contattare il proprio amministratore di sistema per maggiore assistenza.

10 Informazioni su CardOS API

La funzione *Informazioni sulla CardOS API* fornisce informazioni sui file, le versioni, i copyright e i marchi registrati utilizzati in CardOS API.

- Passo 1** ➤ Cliccare l'icona *CardOS API* nella barra degli strumenti e selezionare: *Informazioni sulla CardOS API*

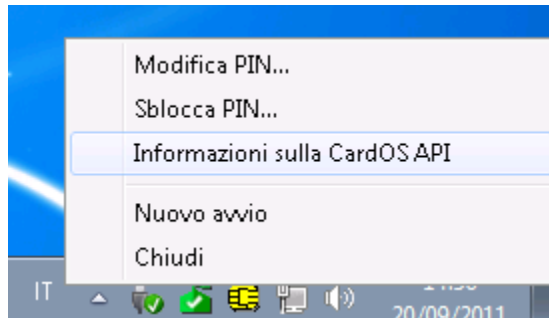


Figura 20

- Passo 2** La finestra *Informazioni su CarOS API* è mostrata in Figura 21. Essa mostra le componenti di CardOS API e le loro versioni. L'elemento Build xx indica il numero di Build della propria installazione. Quest'informazione può essere necessaria per un report di errore o una richiesta di cambiamento.

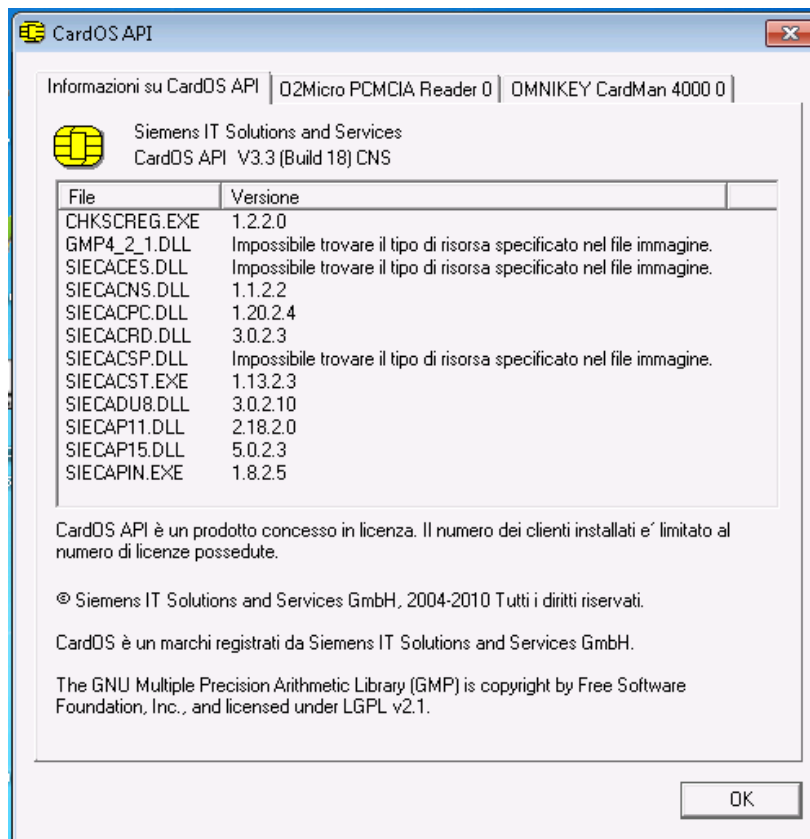


Figura 21

- Premere il tasto *OK* per chiudere la finestra.

11 Nuovo avvio

In alcuni casi può essere necessario riavviare CardOS API, ad esempio dopo aver installato un nuovo lettore di smart card sul sistema.

- Cliccare l'icona CardOS API sulla barra delle applicazioni e selezionare l'opzione *Nuovo avvio* dal menu contestuale come mostrato in Figura 22.

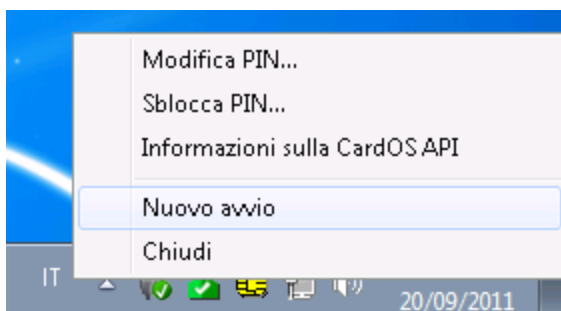



Figura 22

12 Chiudi

- Per chiudere CardOS API cliccare l'icona di CardOS API sulla barra delle applicazioni e selezionare la funzione *Chiudi* dal menu contestuale.

 **Avviso**
Se si chiude CardOS API, i certificati personali che erano stati originariamente propagati durante l'inserimento della carta, verranno rimossi dallo store dei certificati Microsoft⁶. Le applicazioni non potranno accedere ai certificati propagati e alle chiavi sulla smart card.

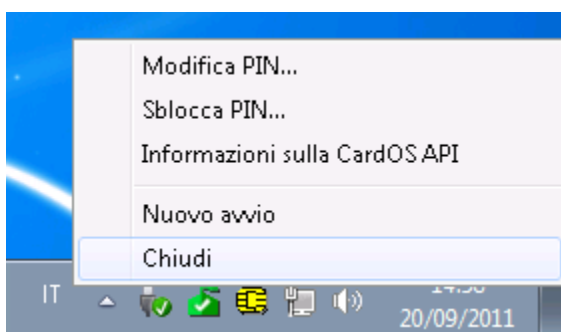


Figura 23

Fare riferimento alla sezione 4 *Avviare CardOS API* a pagina 7 per maggiori informazioni su come riavviare CardOS API.

⁶ A meno che non sia configurato diversamente. Riferirsi refer to CardOS API - Installation Manual for more details.

13 Propagazione dei Certificati

La propagazione dei certificati permette alle applicazioni, dotate di supporto dell'architettura Microsoft CSP, di utilizzare i certificati e le chiavi immagazzinate sulla smart card.

Come spiegato in breve qui nel seguito, CardOS API offre tre diversi modi per propagare i certificati collocati su una smart card:

- **Propagazione Automatica dei Certificati**
Se una smart card è inserita, tutti i certificati sono copiati automaticamente dalla smart card al corrispondente store dei certificati sul computer. I certificati personali sono cancellati appena si rimuove la smart card dal lettore⁷.
- **Propagazione Manuale dei Certificati**
Solo i certificati personali sono copiati nello store dei certificati del computer. I certificati personali rimangono nello store del computer anche se la smart card è rimossa.
- **Propagazione Interattiva dei Certificati**
L'utente è in grado di selezionare i certificati collocati sulla smart card così come i certificati immagazzinati negli store del computer. I certificati personali rimangono nello store del computer se la smart card viene rimossa.

Per verificare i certificati propagati, utilizzare il menu di Internet Explorer:

Strumenti → *Options Internet...* → Tab: *Contenuto* → Pulsante: *Certificati...*

Riferirsi alle sezioni seguenti per una descrizione dettagliata dei diversi tipi di propagazione dei certificati.

⁷ A meno che sia configurato diversamente dall'amministratore di sistema. Riferirsi al document CardOS API – Manuale di Installazione per maggiori dettagli.

13.1 Propagazione Automatica dei Certificati

Utilizzare la propagazione automatica dei certificati per copiare tutti i certificati dalla smart card all'appropriato store dei certificati Microsoft appena CardOS API riconosce che una smart card è stata inserita in un lettore.

A seconda del tipo di certificato, questi vengono propagati in un diverso store di certificati.

- **Autorità di certificazione radice attendibili (Root Certificates)**

I certificati radice sono certificati auto-firmati. Appena si inserisce una smart card che include un certificato radice, il computer mostra un Avviso di sicurezza che chiede se si vuole installare questo certificato radice. Leggere attentamente il messaggio mostrato.

Se si clicca *Sì*, il certificato radice è copiato nel seguente store dei certificati:

Radice console\Certificati – Utente corrente\Autorità di certificazione radice attendibile\Certificati

Questi certificati rimangono nello store dei certificati anche se si rimuove la smart card.

- **Autorità di certificazione intermedie (CA Certificates)**

Se il bit CA di un certificato è impostato, il certificato è chiamato di CA intermedia. Se una smart card è inserita, i certificati di CA intermedia sono copiati automaticamente nel seguente store dei certificati:

Radice console\Certificati – Utente corrente\Autorità di certificazione intermedie\Certificati

Questi certificati rimangono nello store dei certificati anche se si rimuove la smart card.

- **Personale (Personal Certificates)**

Tutti gli altri certificati sulla smart card sono trattati come certificati personali. Questi certificati sono copiati automaticamente nel seguente store dei certificati:

Radice console\Certificati – Utente corrente\Personale\Certificati

Rimuovendo la smart card si cancellano tutti i certificati personali propagati⁸.

⁸ A meno che sia configurato diversamente dall'amministratore di sistema. Riferirsi al document CardOS API – Manuale di Installazione per maggiori dettagli.

13.2 Propagazione Manuale dei Certificati

La propagazione manuale dei certificati è usata solo in casi eccezionali, ad esempio se non si vuole lanciare CardOS API in background per migliorare le prestazioni del sistema.

La propagazione manuale dei certificati copia solo i certificati personali dalla smart card inserita nel seguente store dei certificati Microsoft:

Radice console\Certificati – Utente corrente\Personale\Certificati

Rispetto alla propagazione automatica dei certificati, i certificati personali non sono cancellati quando si rimuove la smart card dal lettore. Se necessario, rimuoverli manualmente, utilizzando il menu di Internet Explorer → *Strumenti* → *Opzioni Internet* → *Contenuto* tab → *Certificati* tasto → selezionare uno o più certificati e premere il tasto *Rimuovi*.

**Nota**

CardOS API deve essere chiuso prima di lanciare la funzione di *Propagazione Manuale dei Certificati*.

Passo 1 ➤ Cliccare *Start*, e poi *Esegui*.

Passo 2 La finestra Esegui viene mostrata.

- Cliccare Sfoglia... per selezionare il programma *siecacst.exe* dell'installazione di CardOS API
Default: C:\Programmi\Siemens\CardOS API\bin\siecacst.exe
- Aggiungere l'opzione /m alla riga di comando come mostrato in Figura 24.

Nota

In caso si inserisca manualmente il percorso, è necessario aggiungere le virgolette a tutto il percorso assoluto del file se il percorso di installazione contiene dei caratteri di spaziatura.
Esempio: "C:\Program Files\Siemens\CardOS API\bin\siecacst.exe" /m

Se si lancia *siecacst.exe* senza alcun parametro, viene avviata la propagazione automatica.

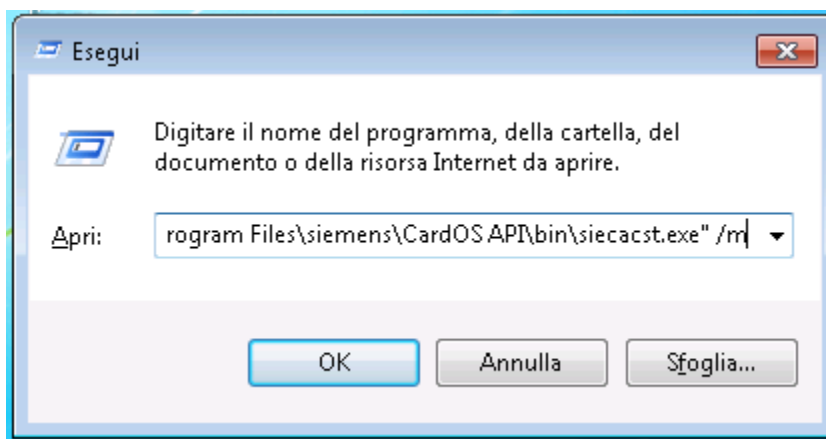


Figura 24

- Premere *OK* per lanciare la *Propagazione Manuale dei Certificati*.

Passo 3 Nel caso non si fosse ancora inserita la smart card, viene chiesto di inserire la carta.

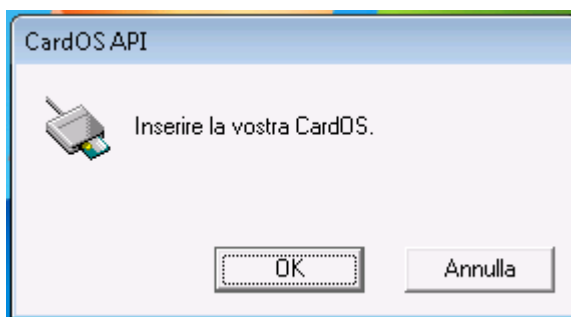


Figura 25

- Inserire la propria smart card e cliccare *OK* per copiare tutti i certificati personali nello store dei certificati appropriato di Microsoft.

13.3 Propagazione Interattiva dei Certificati

La propagazione interattiva dei certificati permette di selezionare i certificati personali e lo store dei certificati dove copiare questi certificati. I certificati copiati non vengono cancellati quando si rimuove la smart card dal lettore.

Nota



- La propagazione interattiva è supportata solo su piattaforma Microsoft XP o se si è installata l'estensione Microsoft CAPICOM.
- E' necessario chiudere CardOS API prima di poter avviare la propagazione interattiva dei certificati.

Passo 1 ➤ Cliccare *Start*, e poi *Esegui*.

Passo 2 La finestra *Esegui* viene mostrata.

- Cliccare *Sfoggia...* per selezionare il programma *siecacst.exe* dell'installazione di CardOS API Default: C:\Programmi\Siemens\CardOS API\bin\siecacst.exe
- Aggiungere l'opzione */m* e */i* alla riga di comando come mostrato in Figura 26.

Nota



In caso si inserisca manualmente il percorso, è necessario aggiungere le virgolette a tutto il percorso assoluto del file se il percorso di installazione contiene dei caratteri di spaziatura.

Esempio: "C:\Program Files\Siemens\CardOS API\bin\siecacst.exe" /m /i

Se si lancia *siecacst.exe* senza alcun parametro, viene avviata la propagazione automatica.

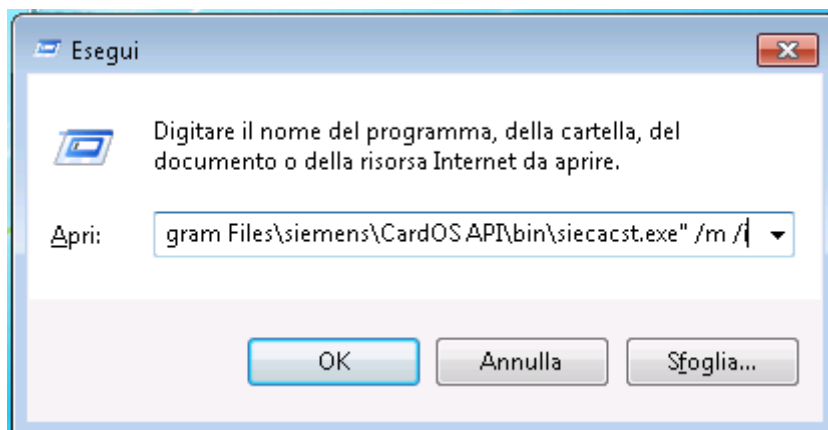


Figura 26

- Premere *OK* per continuare.

Passo 3 Nel caso non si fosse ancora inserita la smart card, viene chiesto di inserire la carta.

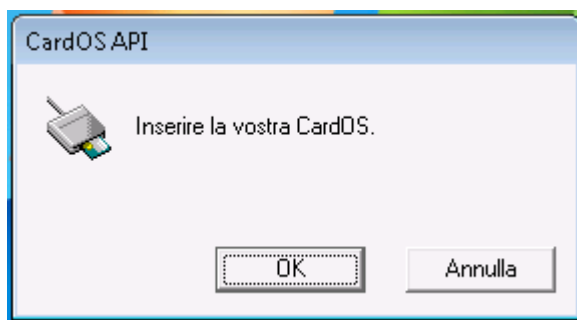


Figura 27

- Inserire la propria smart card e cliccare *OK* per copiare tutti i certificati personali nello store dei certificati appropriato di Microsoft.

Passo 4 Per ogni certificato personale sulla smart card, apparirà la finestra Microsoft di importazione dei certificati (vedere Figura 28).

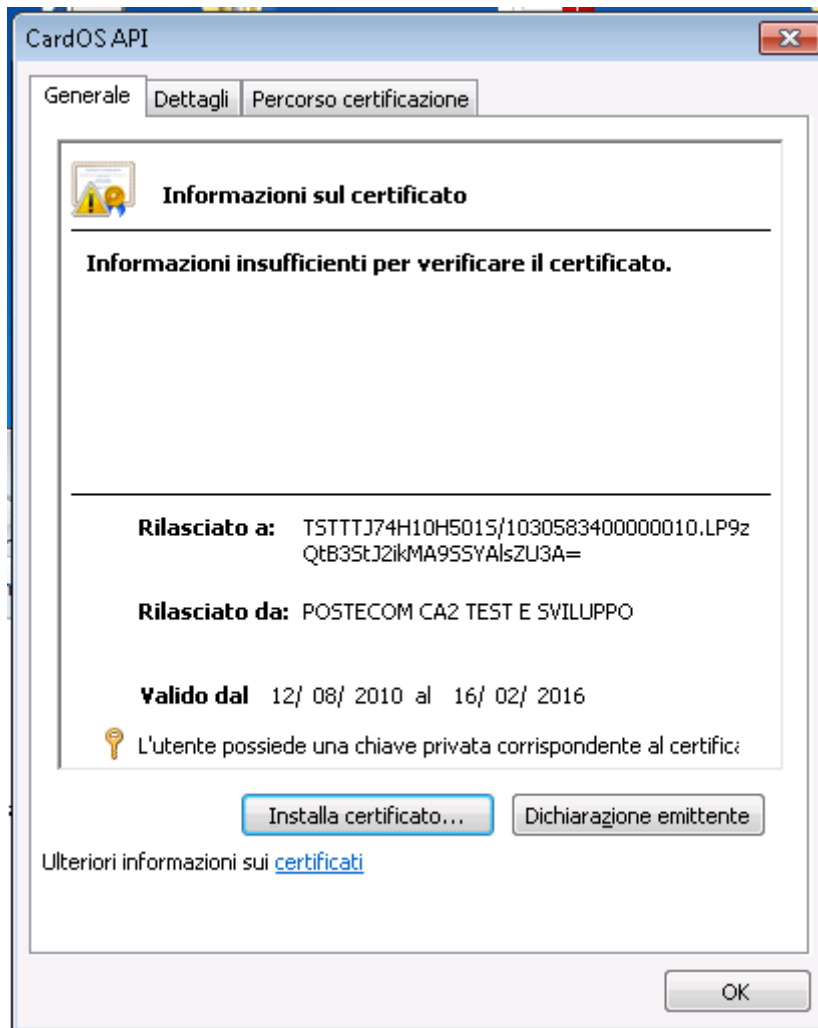




Figura 28

- Se si vuole installare il certificato mostrato, premere il tasto *Instala! Certificato*. Il wizard Microsoft di importazione certificato la guiderà attraverso i passi successivi richiesti per l'installazione del certificato, oltre a scegliere lo store dei certificati.
- Premere invece *OK* per procedere con il prossimo certificato disponibile senza installare il certificato mostrato.

14 Risoluzione dei problemi

Confronti i seguenti scenari prima di contattare il suo amministratore di sistema:

 Figura 29	<p>CardOS API non può riconoscere la smart card inserita:</p> <ol style="list-style-type: none"> 1. Il sistema operativo della sua smart card non è supportato. Riferirsi al documento CardOS API – <i>Note di rilascio</i> per una lista della carte supportate. 2. Il sistema operativo della smart card è supportato, ma CardOS API non riconosce il file system della smart card.
 Figura 30	<p>CardOS API ha identificato un errore critico. In questo caso il codice di errore è mostrato nel tooltip dell'icona. I possibili passi per risolvere il problema possono essere:</p> <ol style="list-style-type: none"> 1. Assicurarsi che il proprio lettore di smart card e i driver corrispondenti siano installati correttamente sul proprio sistema. La maggiorparte dei lettori è dotato di un piccolo programma che permette di ricavare alcune informazioni di base sulla carta (ad esempio l'answer to reset (ATR)). Ciò può essere di aiuto per capire se tutto è stato installato correttamente. 2. Assicurarsi che il servizio Microsoft Smart Card sia avviato. <i>Gestione attività Windows (Task Manager) → Processi → scardsvr.exe</i> 3. Riavviare CardOS API. <p>Se la condizione di errore persiste, contattare il proprio amministratore di sistema.</p>
	<p>L'applicazione XYZ non è in grado di utilizzare le chiavi e i certificati sulla carta</p> <ol style="list-style-type: none"> 1. Nel caso si stesse utilizzando un'applicazione che utilizza Microsoft CSP, assicurarsi che i certificati siano propagati nello store dei certificati di Microsoft (refer to the section 13 <i>Propagazione dei Certificat</i> a pagina 27 per maggiori informazioni). 2. Assicurarsi che l'applicazione giri utilizzando i certificati e le chiavi immagazzinate in un PSE. Se la funzione gira correttamente, riprovare nuovamente utilizzando la propria smart card.
	<p>Lo Smart Card Logon fallisce con '0x80090006 – Firma non valida.' o '0x8009001D – Impossibile inizializzare correttamente la DLL del provider.' (Event log).</p> <p>L'Enrollment conto terzi non riconosce la smart card e chiede continuamente all'utente di inserire la smart card.</p> <p>Assicurarsi che CardOS API sia installato correttamente. Tutte le cartelle sotto la voce di registro: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Calais\SmartCards devono contenere un parametro ATR impostato al valore di una carta CardOS in uso. Il parametro <i>Crypto Provider</i> deve essere impostato a Siemens Card API CSP.</p>

Internet Explorer: “La pagina non può essere visualizzata”

1. Controllare che il certificato personale sia immagazzinato nello store dei certificati di Microsoft. Per maggiori informazioni consultare la sezione 13 *Propagazione dei Certificat* a pagina 27.
2. Riavviare Internet Explorer se il certificato personale è disponibile.

Se CardOS API viene lanciato due volte, apparirà il seguente messaggio di errore (Figura 31).

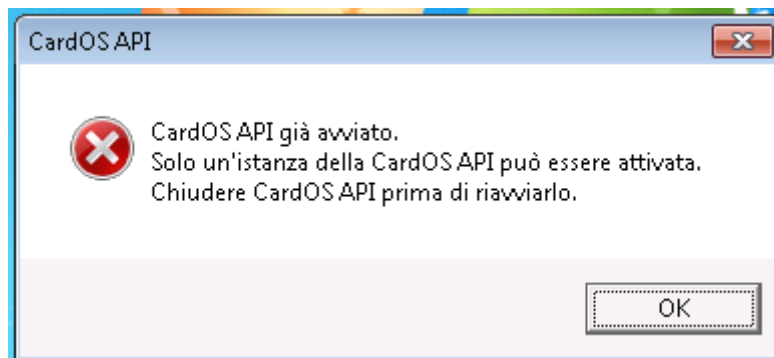


Figura 31

Accettare il messaggio di errore premendo il tasto *OK* e terminare CardOS API (riferirsi alla sezione 12 *Chiudi* a pagina 26) prima di rilanciarlo.

15 Glossario

All'interno dei documenti della distribuzione di CardOS API, sono utilizzate le seguenti abbreviazioni:

API	Application Programming Interface (API) è un'interfaccia che può essere usata da programmi per controllare dispositivi hardware o funzioni del sistema operativo.
CA	Una certification authority, o CA, emette certificati che si legano all'identità di una persona o computer.
CAPI	Microsoft Cryptographic API; anche chiamate Crypto API
CardOS	Sistema Operativo per smart card, sviluppato da Siemens IT Solutions and Services GmbH.
Certificate	Un certificato digitale è un file che include il nome del titolare del certificato, le date di validità, una Chiave Pubblica e il nome della CA emittitrice.
CNS	Carta Nazionale dei Servizi
Cryptoki	Lo standard PKCS#11 specifica la Cryptographic Token Interface (Cryptoki) per i dispositivi che immagazzinano informazioni crittografiche e che eseguono funzioni crittografiche.
CSP	Cryptographic Service Provider (CSP). Un CSP è responsabile della creazione di chiavi e del loro utilizzo per vari compiti. Su un PC possono essere installati differenti e innumerevoli CSP, i quali differiscono per esempio per la lunghezza delle chiavi, algoritmi per la cifra for encryption, o le smart card supportate.
Data Object	Un Data Object è un file che può essere importato o esportato da una smart card.
DF	Un DF (dedicated file) è una directory nel file system di una Smart Card.
Digital Signature Application	Una Digital Signature Application (DSA) consiste di una struttura di file of appropriata e degli oggetti su una smart card, che abilitano l'esecuzione di una firma digitale.
Digital Signature PIN	Un PIN di Firma Digitale è un PIN di Secondary Authentication conforme alle leggi tedesche sulla firma digitale SigG and SigV.
Digital Signature PUK	Un PUK di Firma Digitale è usato per sbloccare il PIN di Firma Digitale.
DIN NI 17-4	Specifiche dell'interfaccia alle smart card con Digital Signature Application conforme alle leggi SigG e SigV.
HPC	Health Professional Card
ICC	Integrated Circuit Card. Descrizione conforme ISO per una Smart Card.
ICCSP	Un Integrated Circuit Card Service Provider (ICCSP) è responsabile per l'allocazione delle funzionalità di una smart card, indipendentemente dal sistema operativo della carta (ICC).
Minidriver	I Minidriver forniscono alle smart card un'interfaccia consistente con il Microsoft Smart Card Base Cryptographic Service Provider.
MF	Un MF (master file) è la directory radice nel file system di una smart card.
PC/SC	Interoperability Specification for ICCs and Personal Computer Systems.
PDC	Patient Data Card
PIN	Il Personal Identification Number (PIN) è usato per autenticare l'utente come possessore della carta. Ogni volta che un PIN corretto viene immesso, il suo contatore di errori viene resettato.

PIN pad	Specialmente su applicazioni ad alta sicurezza (ad esempio transazioni economiche) l'inserimento di un PIN è soggetto a regolamenti sulle tastiere. Queste specifiche tastiere sono chiamate PIN pad. Sono protette meccanicamente e crittograficamente, in modo che il PIN non può essere intercettato durante l'inserimento. I lettori di smart card con un PIN pad integrato sono chiamati lettori a PIN pad.
PKCS#11	I Public-Key Cryptography Standard (PKCS) sono specifiche sviluppate da RSA Security in associazione con gli sviluppatori a livello mondiale. PKCS#11 definisce una tecnologia indipendente dall'interfaccia di programmazione per dispositivi crittografici come le smart card.
PSE	Personal Security Environment – Le informazioni rilevanti per la sicurezza sono immagazzinate in un PSE. Tra le altre cose, esso contiene il certificato e la chiave privata del titolare di una carta e può contenere uno o più certificati di CA. Il PSE può prendere la forma di un file cifrato su una smart card ed è protetto da password.
PUK	Il Personal Unblocking Key (PUK), anche noto come Super-PIN o SO PIN (nello standard PKCS#11), viene utilizzato per cambiare o sbloccare il PIN Utente.
Secondary Authentication PIN	Lo scopo della secondary authentication è di fornire un modo alla smart card di produrre firme digitali per il non-ripudio con ragionevole certezza che solo l'utente autorizzato può essere stato l'appositore della firma. Un Secondary Authentication PIN deve essere fornito ogni volta che una chiave di firma deve essere utilizzata per eseguire una operazione di firma digitale. A seconda dei requisiti di sicurezza di una applicazione, un Secondary Authentication PIN deve essere inserito tramite un lettore a PIN pad in modo da bypassare il PC.
SigG	Germany's Electronic Signature Act, entrata in vigore il 22 Maggio 2001, definisce le condizioni del framework per la firma elettronica. La Signature Ordinance (SigV) è stata sviluppata per governare l'utilizzo delle firme elettroniche.
SigV	Germany's Signature Ordinance. Supplemento alla SigG riguardo le procedure delle certification authority; effettiva da 22 Novembre 2001.
SO PIN	Security Officer PIN. Questa definizione è utilizzata nello standard PKCS#11 → PUK.
SPE	Secure PIN Entry (SPE) ottenuto utilizzando un lettore PIN pad.
Super-PIN	→ PUK
Token	Un token è un oggetto contenente le informazioni di sicurezza per una sessione crittografica. Una smart card è quindi un token.
Transport PIN	Il Transport PIN (PIN di Trasporto) è comunemente fornito da un Trust Center tramite un canale sicuro (ad esempio una busta cieca). Prima di utilizzare una Digital Signature Application il possessore della smart card deve inizializzare il proprio Digital Signature PIN sulla carta. Per eseguire questa inizializzazione, è necessario inserire il cosiddetto PIN di Trasporto, per poter quindi assegnare un Digital Signature PIN e un Digital Signature PUK sulla carta.
WinSCard API	Windows Smart Card client API