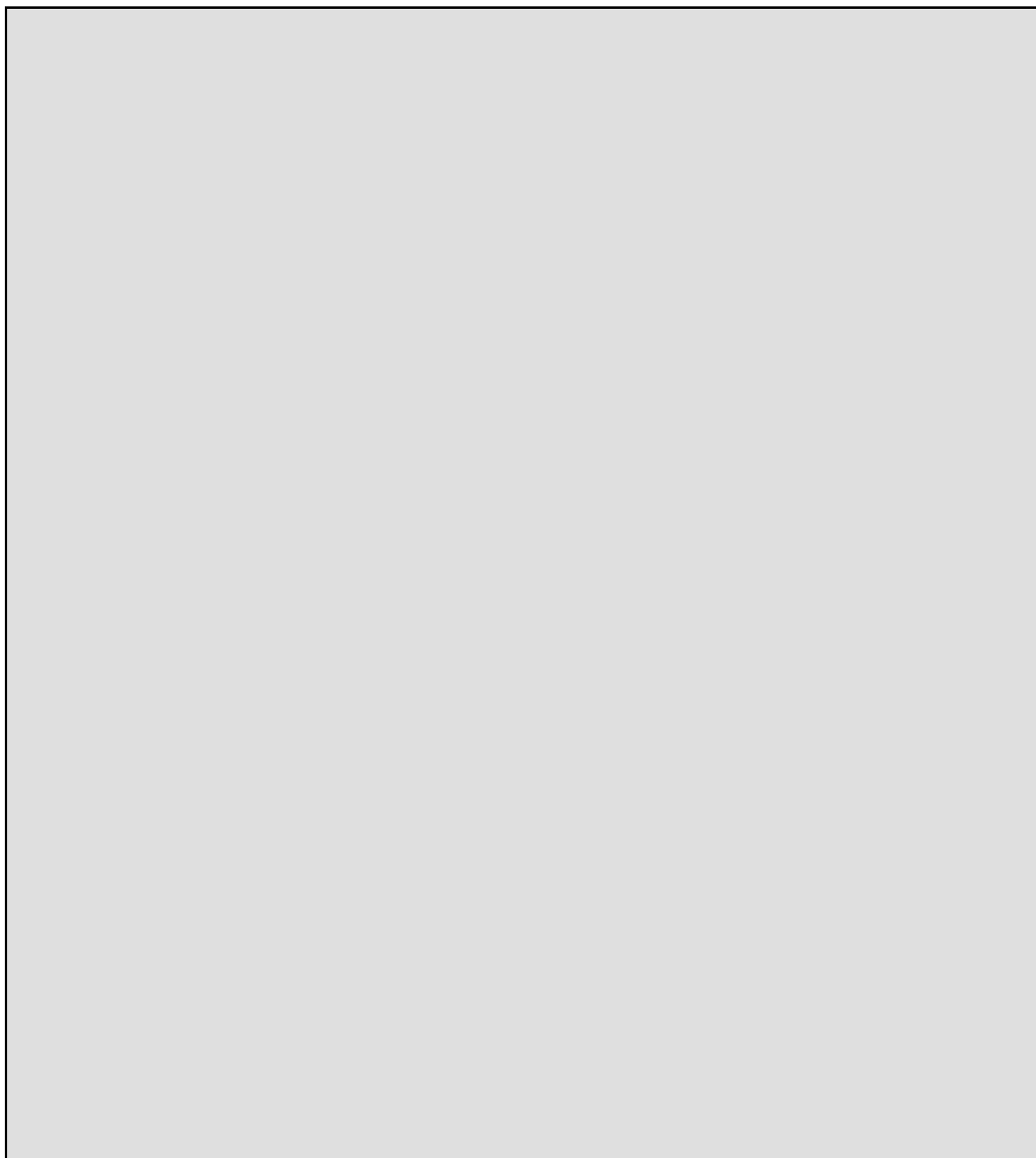


# **CardOS API V3.3 CNS per Windows**

**Manuale di Installazione**

**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.

# Contents

<b>1</b>	<b>INFORMAZIONI SU QUESTO MANUALE</b>	<b>4</b>
1.1	Destinatari	4
1.2	Schermate	4
1.3	Documentazione	4
1.4	Copyright di terze parti	5
<b>2</b>	<b>PANORAMICA DI CARDOS API</b>	<b>6</b>
<b>3</b>	<b>REQUISITI HARDWARE E SOFTWARE</b>	<b>7</b>
<b>4</b>	<b>INSTALLAZIONE DI CARDOS API</b>	<b>8</b>
<b>5</b>	<b>INSTALLAZIONE DI CARDOS API SENZA INTERAZIONE UTENTE</b>	<b>18</b>
<b>6</b>	<b>MODIFICARE O RIPARARE CARDOS API</b>	<b>19</b>
<b>7</b>	<b>PROPAGAZIONE DEI CERTIFICATI MICROSOFT VS CARDOS API</b>	<b>26</b>
7.1	Propagazione dei certificati di CardOS API	26
7.2	Propagazione dei certificati di Windows XP e Windows Server 2003/2008	26
7.3	Propagazione dei certificati di Windows Vista e Windows 7	27
<b>8</b>	<b>CONFIGURARE CARDOS API</b>	<b>28</b>
8.1	Abilitare i log di CardOS API	28
8.1.1	Log PKCS#11	29
8.1.2	Log CSP	31
8.1.3	Log della propagazione dei certificati	32
8.1.4	Log dell'interfaccia con la Smart Card	32
8.2	Opzioni PKCS#11	33
8.3	Opzioni CSP	34
8.4	Opzioni della propagazione dei certificati	35
8.5	Opzioni dell'inserimento sicuro del PIN	37
<b>9</b>	<b>CONFIGURAZIONE DI CARDOS API - VIEWER</b>	<b>38</b>
<b>10</b>	<b>REGISTRARE LA LIBRERIA PKCS#11 CON APPLICAZIONI DI TERZE PARTI</b>	<b>40</b>
<b>11</b>	<b>CONFIGURARE CARDOS API SU CITRIX METAFRAME</b>	<b>41</b>
11.1	Configurazione lato Server	41
11.1.1	Abilitare Citrix Smart Card Hooking per CardOS API	41
11.1.2	Abilitare l'accesso remoto tramite Smart Card per le applicazioni singole	42
11.2	Configurazione lato Client	42
<b>12</b>	<b>RIMUOVERE CARDOS API</b>	<b>43</b>
<b>13</b>	<b>GLOSSARIO</b>	<b>44</b>

# 1 Informazioni su questo Manuale

Questo manuale contiene una guida passo-passo per installare, aggiornare, riparare e disinstallare CardOS API V3.3 CNS per Windows in ambiente Windows così come le informazioni di configurazione.

Leggere questa sezione per ricavare le informazioni generali per l'uso di questo documento.

## 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.



**Avviso**

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

## 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.

## 1.4 Copyright di terze parti

Lo standard Cryptographic Token Interface “RSA Security Inc. Public Key Cryptography Standard (PKCS)” è copyright di RSA Security Inc. ([www.rsasecurity.com](http://www.rsasecurity.com)).

CardOS API utilizza routine di decompressione del *lab* project (<http://www.gzip.org/zlib>). Il software zlib è copyright di Jean-loup Gailly e Mark Adler.

CardOS API utilizza la libreria GNU Multiple Precision Arithmetic Library per le operazioni con i bignum operations (<http://gmplib.org/>). La libreria GMP è copyright di Free Software Foundation, Inc., e licenziata sotto LGPL v2.1 e v3.0

CardOS API utilizza il porting di GMP per Microsoft Windows gestito da Brian Gladman (<http://gladman.plushost.co.uk/oldsite/computing/gmp4win.php>).

Riferirsi al documento informativo Open Source Software distribuito sul CD per maggiori informazioni sulle componenti software Open Source utilizzate da CardOS API.

## 2 Panoramica di CardOS API

CardOS API è il nome della famiglia di strumenti e documenti, che trattano le Application Programming Interface (API) per le smart card CardOS.

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 maggior parte 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.

## 3 Requisiti Hardware e Software

Assicurarsi che il proprio computer soddisfi le condizioni minime del sistema operativo date da Microsoft e che abbia almeno 20 MB di spazio disco libero prima dell'installazione.

Riferirsi al documento CardOS API – Note di rilascio per i dettagli sul supporto di smart card, lettori di smart card, lettori PIN pad, applicazioni e sistemi operativi.

## 4 Installazione di CardOS API

La distribuzione di CardOS API fornisce un pacchetto di setup a 32-bit e a 64-bit. Assicurarsi di selezionare il pacchetto corrispondente al proprio sistema.



### Nota

La distribuzione di CardOS API fornisce un pacchetto di setup a 32-bit e a 64-bit. Per un sistema operativo a 32-bit è necessario installare CardOS API 32-bit. Per un sistema operativo a 64-bit è necessario installare CardOS API 64-bit. Dopo l'installazione di CardOS API 64-bit sarà possibile utilizzare le applicazioni a 32-bit su ambiente Windows 64-bit.

Durante l'installazione è possibile scegliere se eseguire un'installazione completa o personalizzata. L'installazione completa installa il seguente software e documenti:

- **CardOS API**  
Librerie ed eseguibili necessari per la gestione del PIN, la propagazione dei certificati e l'accesso alla smart card.
- **CardOS API – Viewer**  
Applicazione per la gestione degli oggetti sulla smart card, la gestione dei PIN, l'inizializzazione delle smart card, e la visualizzazione delle informazioni PKCS#11 della smart card.
- **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, problemi noti
- **CardOS API – Manuale utente**  
Questo documento fornisce informazioni dettagliate su come usare CardOS API nel lavoro di tutti i giorni in ambiente Windows.
- **CardOS API – Viewer – Manuale utente**  
Questo documento fornisce informazioni dettagliate su come usare il Viewer in ambiente Windows.
- **License Agreement**  
Questo documento fornisce le clausole della licenza applicabili a CardOS API.

L'applicazione Viewer e il relativo manuale utente può essere escluso dall'installazione selezionando una installazione di tipo personalizzato.

Al termine dell'installazione, il software e la documentazione possono essere acceduti tramite il menu *Start* di Windows.

Seguire i passi successivi per installare CardOS API in un ambiente Windows.

**Passo 1** ➤ E' consigliato chiudere tutti i programmi Windows prima di avviare l'installazione.



- Passo 2** ➤ Inserire il CD CardOS API nel lettore CD-ROM o DVD del computer. Internet Explorer si aprirà automaticamente sulla pagina iniziale di CardOS API come mostrato in Figura 1 a pagina successiva.




**Nota**

Nel caso non si usi Internet Explorer o la funzione di AutoRun sia disattivata sul PC, posizionarsi sulla directory `Setup` sul CD di installazione e avviare, a seconda del sistema operativo, uno dei due pacchetti di setup: `CardOS_API_Setup.exe` (32-bit) o `CardOS_API_Setup_x64.exe` (64-bit).

Saltare il **Passo 3** e procedere con il **Passo 4**.

**Passo 3** La Figura 1 mostra la pagina iniziale di CardOS API.

- Per cambiare lingua, selezionare una lingua nel menu in alto alla pagina.



**Nota**  
La lingua dell'interfaccia grafica durante il processo di installazione e l'esecuzione di CardOS API è la stessa del sistema operativo.



**SIEMENS**

IT Solutions and Services

English Deutsch Español Français Italiano Português

### CardOS API V3.3 CNS for Windows

#### Installazione Windows

La distribuzione di CardOS API viene fornita con la routine di installazione de 32 bits i una de 64 bits para configurazione Microsoft Windows. Su un sistema Windows 32 bit installa solamente la version CardOS API 32 bit i su un sistema Windows 64 bit installa la version CardOS API 64 bit. Si raccomanda di fare riferimento al documento [CardOS API - Release Notes](#) prima di installare il software.

- **Installazione: CardOS API 32 bit**  
Seguire le istruzioni passo per passo descritte in [CardOS API - Installation Manual](#) per installare CardOS API su un sistema Windows 32 bit. Il programma Card Viewer può essere installato additionally su richiesta.
- **Installazione: CardOS API 64 bit**  
Seguire le istruzioni passo per passo descritte in [CardOS API - Installation Manual](#) per installare CardOS API su un sistema Windows 64 bit. Il programma Card Viewer può essere installato additionally su richiesta.
- **Known Issues (Questioni note)**  
Questo file contiene importazioni informazioni last-minute non comprese nella corrispondente sezione delle [CardOS API - Release Notes](#).

CardOS è un marchio commerciale registrato di Siemens IT Solutions and Services GmbH.  
© Siemens IT Solutions and Services GmbH, 2004 - 2010 Tutti i diritti riservati.

Figura 1

- A seconda del sistema operativo, si può avviare uno dei due pacchetti di installazione: **Installazione: CardOS API 32-bit** o **Installazione: CardOS API 64-bit**

**Passo 4** Microsoft Internet Explorer mostra un avviso di sicurezza per il download.

- Fidarsi dell'avviso e clickare su *Esegui* per continuare.

**Passo 5** InstallShield Wizard, mostrato in Figura 2, darà il benvenuto all'installazione di CardOS API.

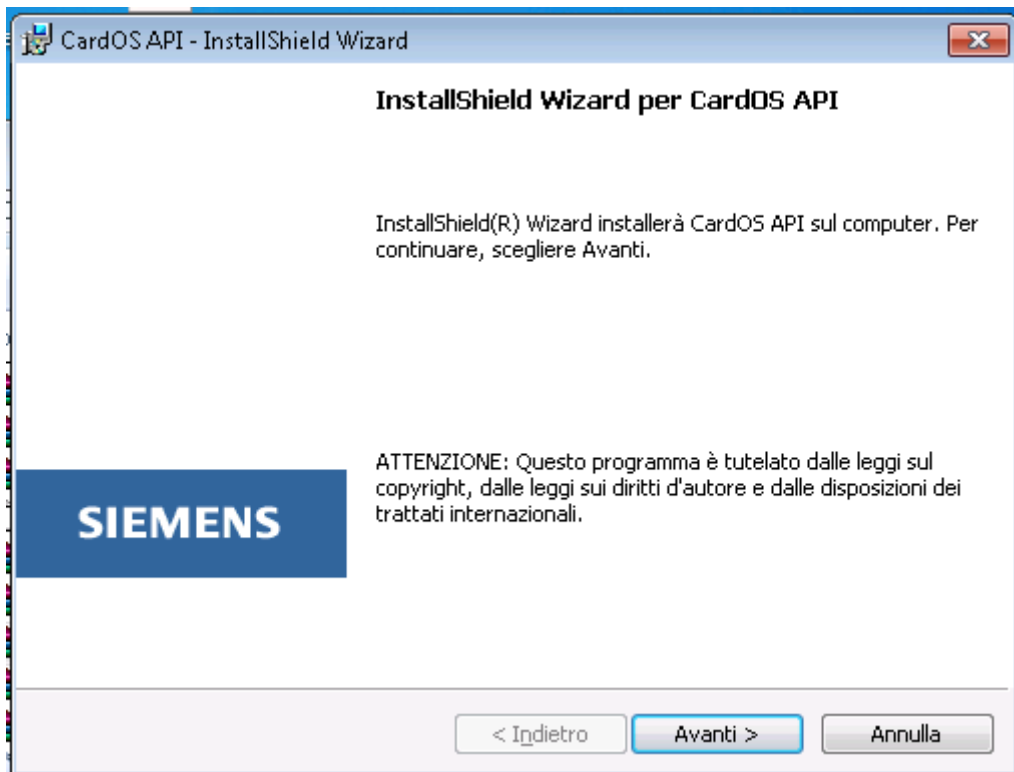


Figura 2

- Premere il tasto *Avanti* per continuare con l'installazione.

**Passo 6** La finestra del Contratto di licenza sarà visualizzato (vedere Figura 3).

- Leggere il contratto di licenza e accettarlo selezionando il tasto di scelta opportuno.



Figura 3

- Premere il tasto *Avanti* per continuare con l'installazione.

- Passo 7** La finestra di scelta del Tipo di installazione verrà mostrata (vedere Figura 4).
- Lasciare inalterata questa finestra per l'installazione completa. Selezionare *Personalizzata* e procedere con il **Passo 9** se si preferisce una installazione personalizzata.

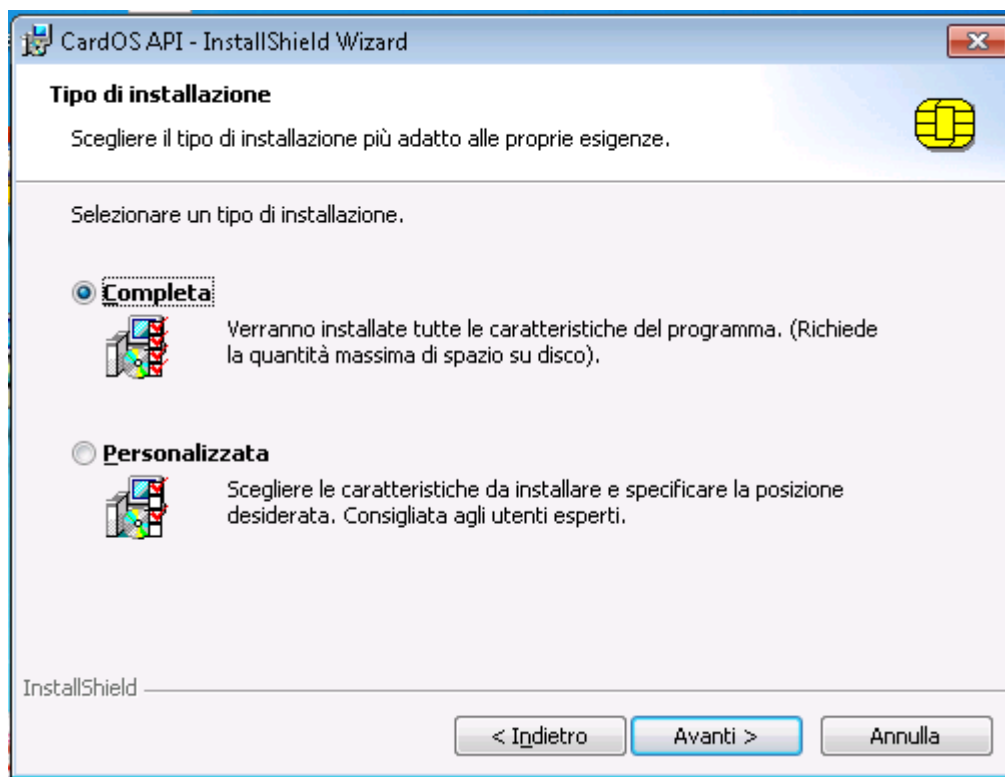


Figura 4

- Premere il tasto *Avanti* per continuare con l'installazione.

- Passo 8** Si è deciso per una installazione completa, e quindi viene chiesta la Cartella di destinazione per l'installazione.
- Cliccare il tasto *Cambia* per selezionare una cartella destinazione differente o accettare la destinazione predefinita.

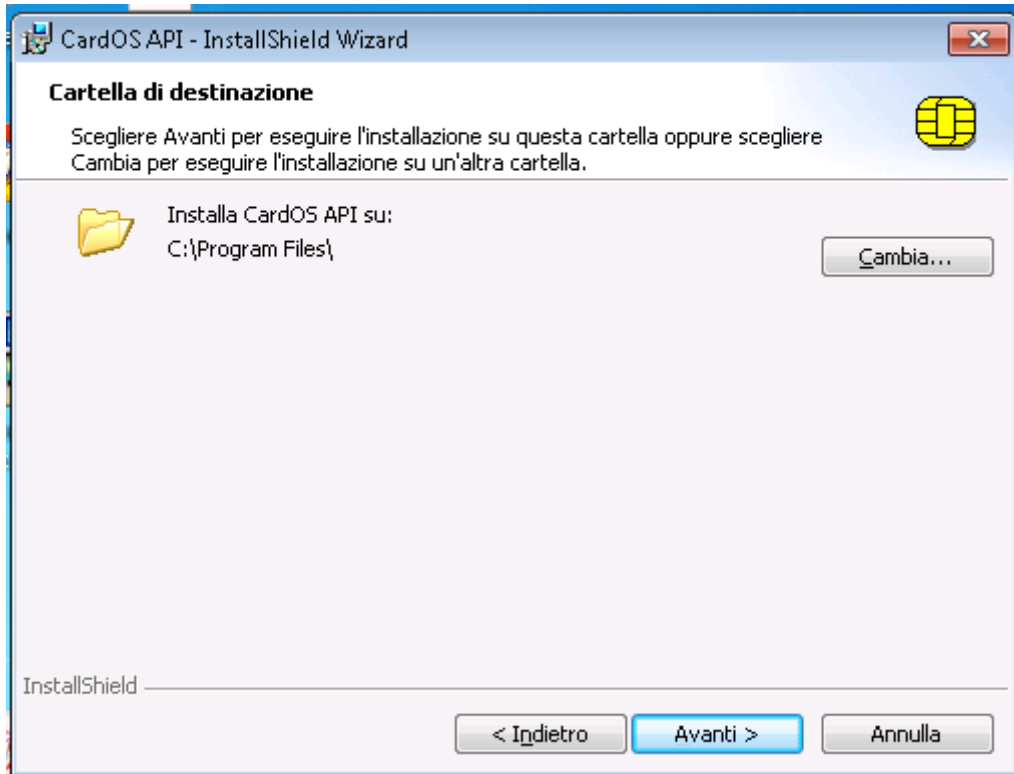


Figura 5

- Premere il tasto *Avanti* per continuare con l'installazione al **Passo 10**.

**Passo 9** Si è deciso per una installazione personalizzata.

- Aprire uno dei menu a comparsa mostrato in Figura 6 e selezionare le caratteristiche richieste.
- Per selezionare una cartella di destinazione differente premere *Cambia...*
- Per consultare lo spazio disponibile su tutti i dischi, clickare il tasto *Spazio*.

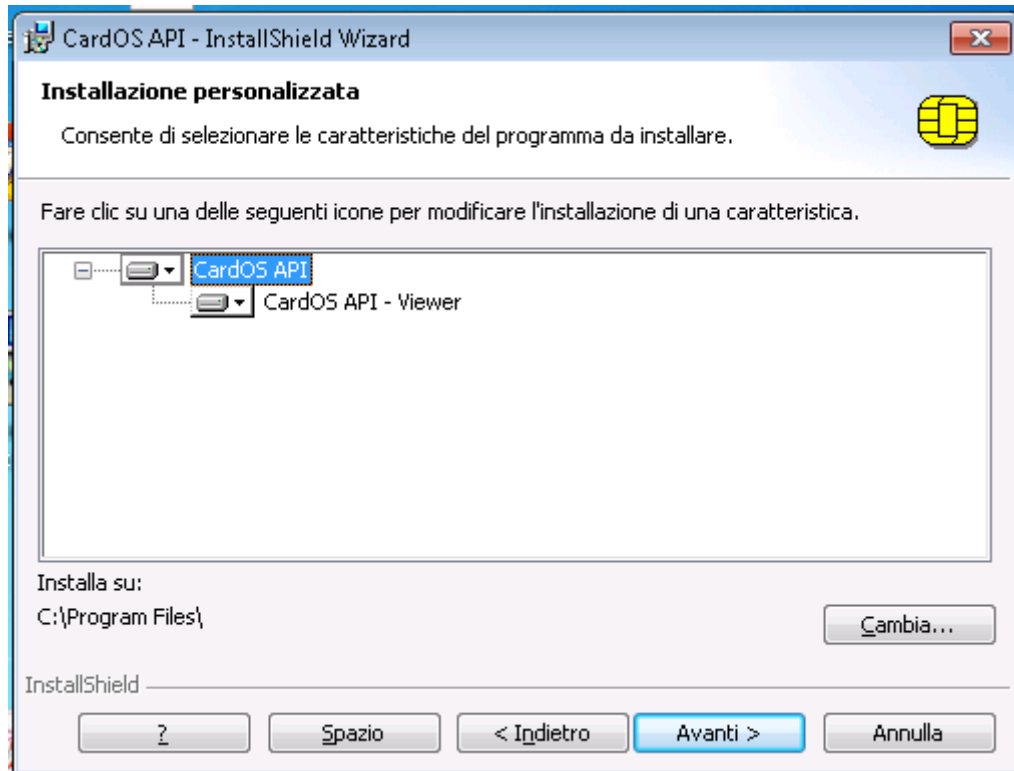


Figura 6

- Premere il tasto *Avanti* per accettare le opzioni scelte o consigliate e continuare.

- Passo 10** La finestra chiamata Pronta per l'installazione del programma verrà mostrata (vedere Figura 7).
- Cliccare il tasto *Indietro* per rivedere o cambiare qualunque settaggio di installazione.

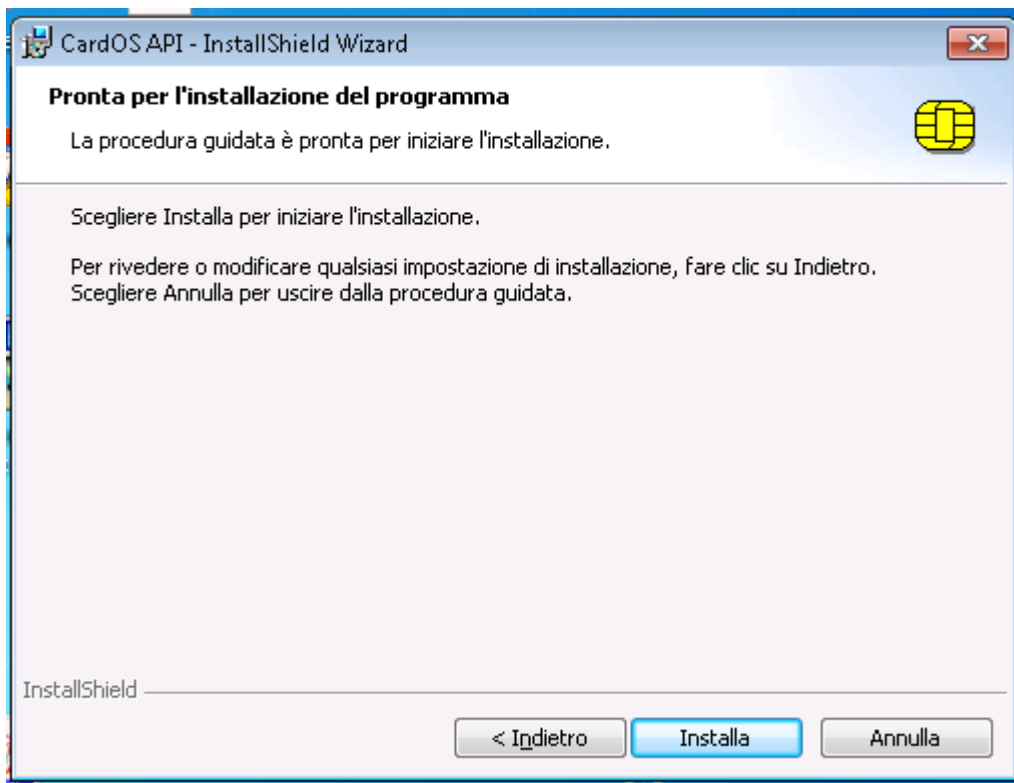


Figura 7

- Premere il tasto *Installa* per cominciare l'installazione.



**Passo 11** L'InstallShield Wizard (vedere Figura 8) conferma che il processo di installazione è stato completato con successo.

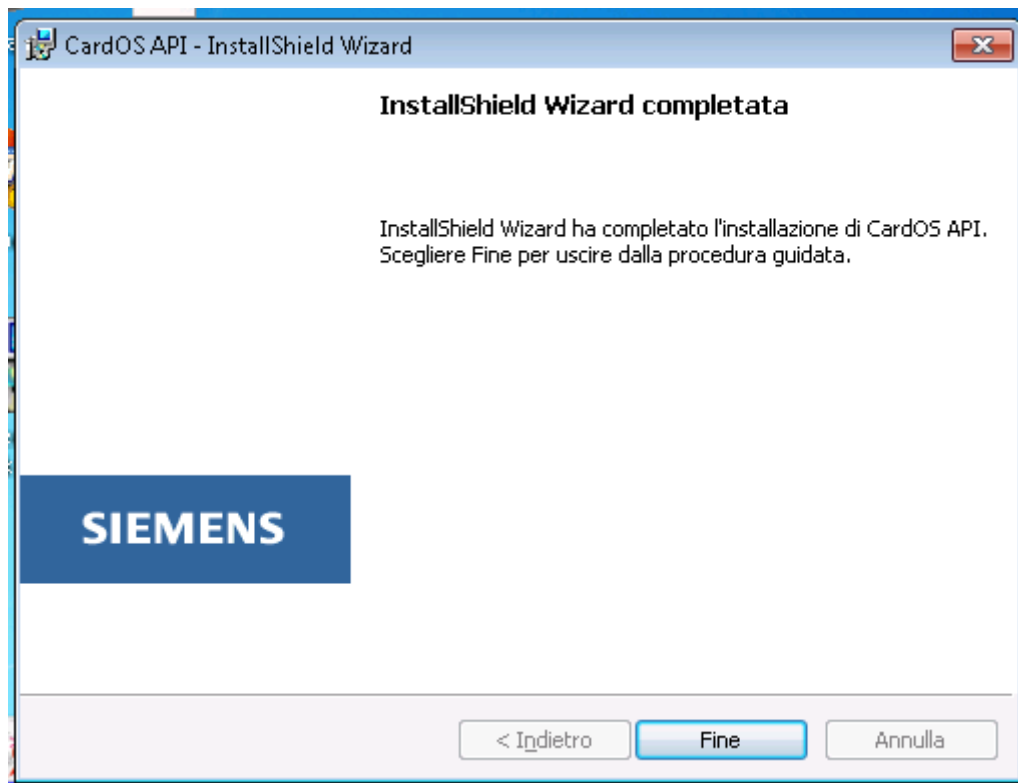


Figura 8

- Selezionare il pulsante *Fine* per terminare l'operazione di installazione.

**Passo 12** Se uno dei componenti software non può essere sostituito durante l'installazione, viene richiesto il riavvio del sistema al termine dell'installazione.

In questo caso, è necessario eseguire i seguenti passi:

- Riavviare il sistema.
- Al termine del riavvio del sistema, viene visualizzata la schermata di accesso: Accedere con lo stesso utente che ha installato inizialmente CardOS API. Questo è necessario per permettere al processo di installazione di eseguire i cambiamenti finali.



**Avviso**

Se non si accede con lo stesso utente che ha inizialmente installato CardOS API, non si sarà in grado di lanciare CardOS API.

## 5 Installazione di CardOS API senza interazione utente

Il CD di installazione contiene il programma di installazione nella directory `Setup`. Usare **CardOS\_API\_Setup.exe** su piattaforme 32-bit x86 e **CardOS\_API\_Setup\_x64.exe** su piattaforme 64-bit x64.



### Nota

La distribuzione di CardOS API fornisce un pacchetto di setup a 32-bit e a 64-bit. Per un sistema operativo a 32-bit è necessario installare CardOS API 32-bit. Per un sistema operativo a 64-bit è necessario installare CardOS API 64-bit. Dopo l'installazione di CardOS API 64-bit sarà possibile utilizzare le applicazioni a 32-bit su ambiente Windows 64-bit.

Per l'installazione nella directory predefinita (C:\Program Files\)) senza interazione con l'utente, usare uno dei seguenti comandi. Per semplicità solo gli esempi della versione a 32-bit vengono elencati di seguito:

- **CardOS\_API\_Setup.exe /S /v"/q"**  
Usare il comando suddetto per una installazione completa di CardOS API V3.3 CNS per Windows 32-bit, CardOS API - Viewer sarà anche installato.
- **CardOS\_API\_Setup.exe /S /v"/q INSTALLLEVEL=1"**  
Usare il comando suddetto per installare CardOS API V3.3 CNS per Windows 32-bit senza CardOS API - Viewer.
- **MsiExec.exe /q /x{8E814717-DE49-4A4A-BD12-39102F9C9FD0}**  
Usare il comando suddetto per disinstallare CardOS API V3.3 CNS per Windows 32/64-bit

Per maggiori informazioni usare il comando "**CardOS\_API\_Setup.exe /?**".

## 6 Modificare o Riparare CardOS API

**Nota**

La distribuzione di CardOS API fornisce un pacchetto di setup a 32-bit e a 64-bit. Per un sistema operativo a 32-bit è necessario installare CardOS API 32-bit. Per un sistema operativo a 64-bit è necessario installare CardOS API 64-bit. Dopo l'installazione di CardOS API 64-bit sarà possibile utilizzare le applicazioni a 32-bit su ambiente Windows 64-bit.

Le funzioni in breve:

- **Modifica**  
Modifica significa che si vuole modificare l'installazione attuale di CardOS API V3.3 CNS per Windows, per esempio per aggiungere CardOS API - Viewer.
- **Ripristina**  
Se uno qualunque dei file dell'installazione corrente di CardOS API si corrompe o è stato cancellato, è necessario riparare utilizzando lo stesso pacchetto di installazione.

Seguire i seguenti passi spiegati di seguito per modificare o riparare l'installazione corrente di CardOS API V3.3 CNS per Windows in un ambiente Windows.

**Passo 1** ➤ E' consigliato chiudere tutte le applicazioni Windows prima di lanciare il programma di installazione.

**Passo 2** ➤ Per riparare CardOS API, inserire il CD CardOS API nel lettore CD-ROM o DVD del computer. Internet Explorer si aprirà automaticamente sulla pagina iniziale di CardOS API come visualizzato in Figura 9 a pagina seguente.


**Nota**

Nel caso non si usi Internet Explorer o la funzione di AutoRun sia disattivata sul PC, posizionarsi sulla directory `Setup` sul CD di installazione e avviare, a seconda del sistema operativo, uno dei due pacchetti di setup: `CardOS_API_Setup.exe` (32-bit) o `CardOS_API_Setup_x64.exe` (64-bit).

Saltare il **Passo 3** e procedere con il **Passo 4**.

**Passo 3** Figura 9 visualizza la pagina di avvio di CardOS API.

- Per cambiare lingua, selezionare una lingua nel menu in alto alla pagina.



**Nota**  
La lingua dell'interfaccia grafica durante il processo di installazione e l'esecuzione di CardOS API è la stessa del sistema operativo.



**SIEMENS**

IT Solutions and Services

English Deutsch Español Français Italiano Português

### CardOS API V3.3 CNS for Windows

#### Installazione Windows

La distribuzione di CardOS API viene fornita con la routine di installazione de 32 bits i una de 64 bits para configurazione Microsoft Windows. Su un sistema Windows 32 bit installa solamente la version CardOS API 32 bit i su un sistema Windows 64 bit installa la version CardOS API 64 bit. Si raccomanda di fare riferimento al documento [CardOS API - Release Notes](#) prima di installare il software.

- **Installazione: CardOS API 32 bit**  
Seguire le istruzioni passo per passo descritte in [CardOS API - Installation Manual](#) per installare CardOS API su un sistema Windows 32 bit. Il programma Card Viewer può essere installato addizionalmente su richiesta.
- **Installazione: CardOS API 64 bit**  
Seguire le istruzioni passo per passo descritte in [CardOS API - Installation Manual](#) per installare CardOS API su un sistema Windows 64 bit. Il programma Card Viewer può essere installato addizionalmente su richiesta.
- **Known Issues (Questioni note)**  
Questo file contiene importazioni informazioni last-minute non comprese nella corrispondente sezione delle [CardOS API - Release Notes](#).

CardOS è un marchio commerciale registrato di Siemens IT Solutions and Services GmbH.  
© Siemens IT Solutions and Services GmbH, 2004 - 2010 Tutti i diritti riservati.

Figura 9

- A seconda del sistema operativo, si può avviare uno dei due pacchetti di installazione: **Installazione: CardOS API 32-bit** o **Installazione: CardOS API 64-bit**.

**Passo 4** Microsoft Internet Explorer mostra un avviso di sicurezza per il download.

- Fidarsi dell'avviso e clickare su *Esegui* per continuare.

**Passo 5** InstallShield Wizard darà il benvenuto all'installazione di CardOS API.

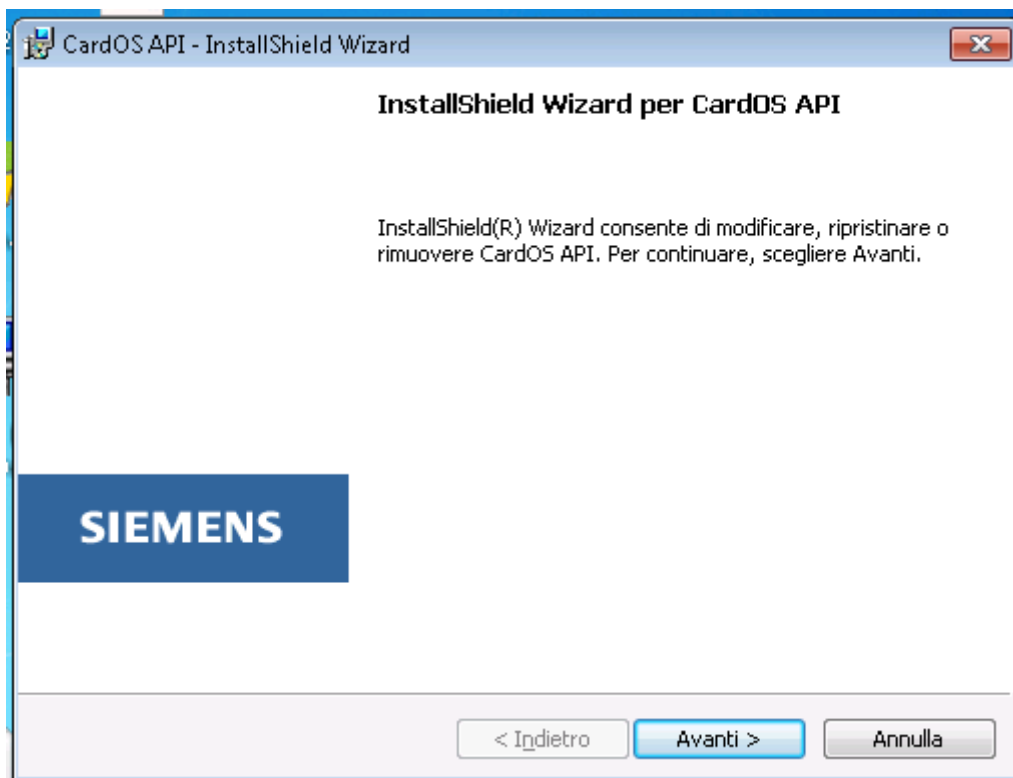


Figura 10

Premere il tasto *Avanti* per continuare con l'installazione.

**Passo 6** La finestra *Manutenzione del programma* viene mostrata.

- Lasciare questa finestra intatta per modificare l'installazione attuale, per esempio per installare l'applicazione CardOS API - Viewer.
- O selezionare l'opzione Ripristina, se si vuole riparare l'installazione attuale.

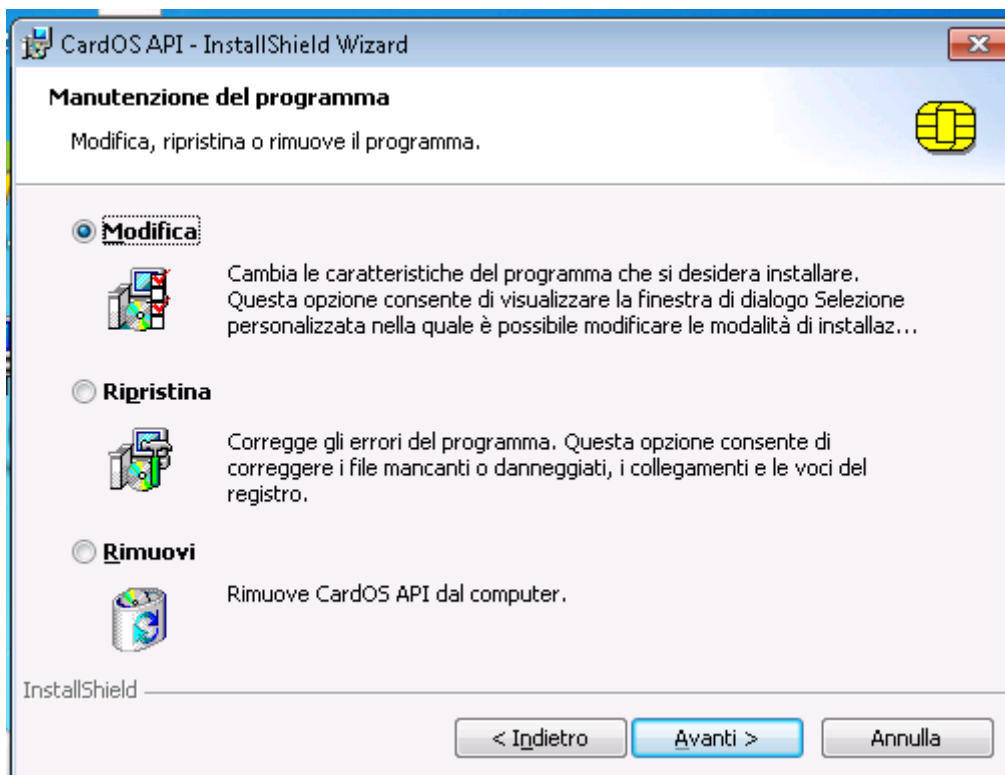


Figura 11

- Premere il tasto *Avanti* per continuare. Nel caso si fosse selezionata l'opzione *Ripristina*, procedere con il **Passo 8**.

- Passo 7** Si è deciso di modificare l'installazione corrente, quindi viene mostrata la finestra di Installazione personalizzata (vedere la Figura 12).
- Selezionare le componenti aggiuntive da installare selezionando “Questa caratteristica verrà installata sul disco rigido locale” dal menu a comparsa.

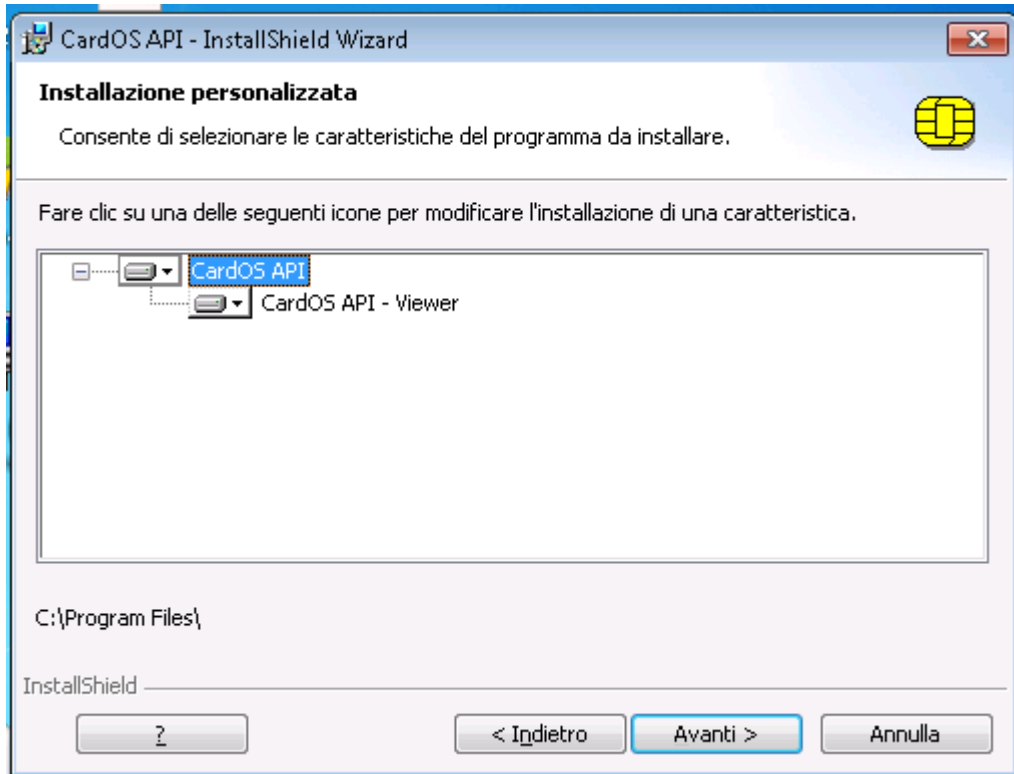


Figura 12

- Premere il tasto *Avanti* per continuare.

**Passo 8** Il wizard è pronto a cominciare l'installazione.

- Cliccare il tasto *Indietro* per rivedere o cambiare qualunque settaggio di installazione.

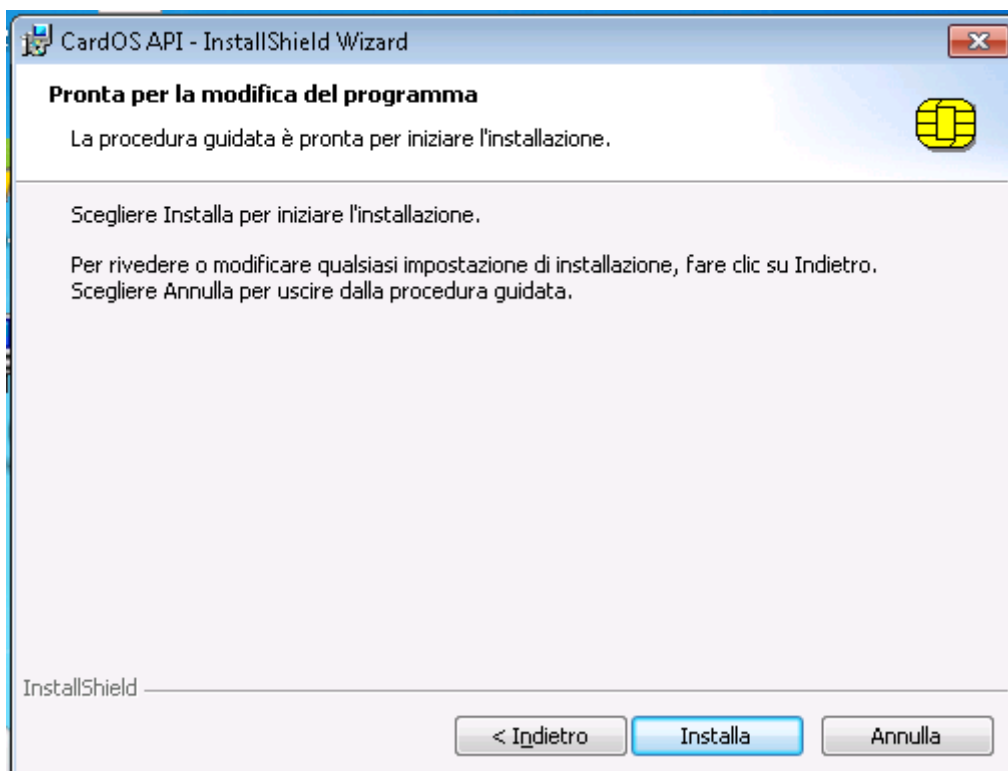


Figura 13

- Premere il tasto *Installa* per cominciare l'installazione.



**Passo 9** L'InstallShield Wizard conferma che il processo di installazione è stato completato con successo.

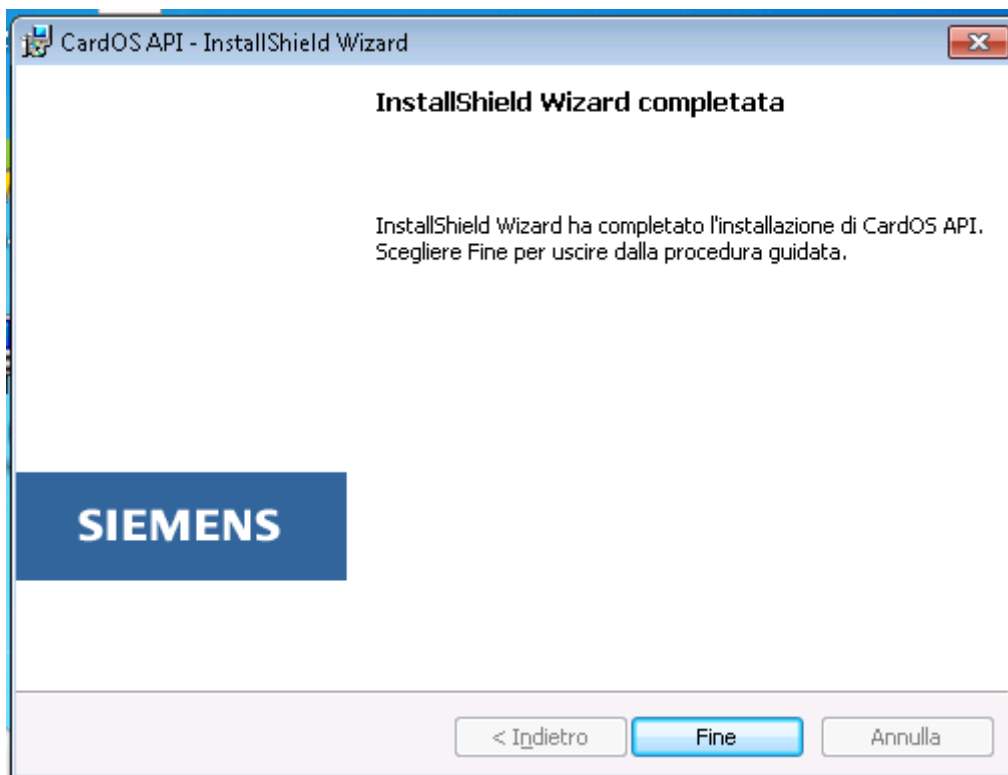


Figura 14

- Selezionare il pulsante *Fine* per completare la modifica o il ripristino dell'installazione attuale.

**Passo 10** Se uno dei componenti software non può essere sostituito durante il ripristino, viene richiesto il riavvio del sistema al termine del ripristino.

In questo caso, è necessario eseguire i seguenti passi:

- Riavviare il sistema.
- Al termine del riavvio del sistema, viene visualizzata la schermata di accesso: Accedere con lo stesso utente che ha installato inizialmente CardOS API. Questo è necessario per permettere al processo di installazione di eseguire i cambiamenti finali.



**Nota**

Controllare i cambiamenti nel registro:

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API\...]

## 7 Propagazione dei certificati Microsoft vs CardOS API

Il compito della propagazione dei certificati è di fornire l'accesso ai certificati X.509 immagazzinati su una smart card alle applicazioni dell'utente. Per ottenere ciò, il certificato X.509 immagazzinato sulla smart card e i riferimenti alle rispettive chiavi private sono copiati nello store dei certificati Microsoft del PC.

A seconda della configurazione del sistema operativo in uso, la propagazione dei certificati di Microsoft e di CardOS API potrebbero essere attive allo stesso tempo.



### Nota

La propagazione dei certificati Microsoft supporta le smart card CardOS solo se CardOS API è installato.

E' consigliabile attivare solo uno dei meccanismi di propagazione dei certificati per avere prestazioni di sistema ottimali e per avere un'esperienza utente consistente nell'utilizzo dei certificati. Per le caratteristiche dettagliate di ogni meccanismo, consultare le sezioni successive.

Dopo l'installazione di CardOS API, l'applicazione di propagazione dei certificati di CardOS API è attiva. Comunque, nel caso la propagazione dei certificati di Microsoft fosse già attiva, è necessario disattivarla manualmente.

### 7.1 Propagazione dei certificati di CardOS API

CardOS API include un'applicazione di propagazione dei certificati eseguita come un processo utente (SIECACST.EXE). Essa viene eseguita come un processo di avvio durante l'accesso dell'utente al sistema e terminata quando l'utente si disconnette. Lo stato corrente della propagazione dei certificati di CardOS API viene indicato da un'icona nella barra delle applicazioni.

La propagazione dei certificati di CardOS API copia tutti i certificati immagazzinati su una carta CardOS nello store dei certificati Microsoft. In modo predefinito, tutti i certificati vengono rimossi dallo store dei certificati Microsoft appena la carta viene rimossa.

In confronto alla propagazione dei certificati integrata di Microsoft Windows, la propagazione dei certificati di CardOS API offre diverse opzioni di configurazione avanzate. Consultare la sezione 8.4 per maggiori dettagli.

### 7.2 Propagazione dei certificati di Windows XP e Windows Server 2003/2008

Su Windows XP e su piattaforme Windows Server 2003/2008, la propagazione dei certificati Microsoft è inclusa come un *Winlogon Notification Package*.

Questa propagazione integrata Microsoft copia il cosiddetto certificato predefinito dell'utente (solitamente il certificato di smart card logon) nello store dei certificati Microsoft. Ulteriori certificati X.509 immagazzinati sulla smart card non vengono copiati nello store dei certificati Microsoft.

Il settaggio di registro **[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\ScCertProp\Enabled]** specifica se la propagazione dei certificati Microsoft è abilitata (1) o disabilitata (0).

## 7.3 Propagazione dei certificati di Windows Vista e Windows 7

A partire da Windows Vista, la propagazione dei certificati Microsoft è realizzata da un servizio chiamato *Propagazione Certificati*.

Questo servizio copia tutti i certificati personali nello store dei certificati Microsoft.

Nel caso si stia utilizzando il classico CardOS API V3 Classic CSP è fortemente consigliato di disabilitare il servizio Microsoft *Propagazione Certificati* altrimenti si potrebbero avere problemi nell'uso di EFS (Encrypted File System).

Microsoft definisce diverse chiavi di registro sotto **[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\SmartCardCredentialProvider]** e **[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsNT\CurrentVersion\CertProp]** che permettono di influenzare il comportamento della propagazione integrata dei certificati Microsoft. Per una descrizione dettagliata riferirsi alla documentazione fornita con Microsoft Windows.

## 8 Configurare CardOS API

CardOS API fornisce un insieme di settaggi, che permettono di configurare CardOS API come richiesto.

### 8.1 Abilitare i log di CardOS API

Per ragioni di sicurezza i log di CardOS API dovrebbero essere disattivi durante il normale utilizzo delle API. Comunque, potrebbero essere utili durante le prove e per rintracciare gli errori.

#### Attenzione



Tenere in considerazione i rischi di sicurezza causati dai log. A seconda del livello di log scelto, nei file di log vengono scritte informazioni sensibili (ad esempio dati risultanti da operazioni di decifra, PIN della smart card).

Assicurarsi che solo gli utenti autorizzati possano modificare i settaggi e leggere i file di log. Di default le chiavi di registro rilevanti potrebbero non essere protette adeguatamente contro modifiche indesiderate.

E' caldamente consigliato cambiare i PIN di una smart card utilizzata su un sistema con i log attivati.

#### Nota



E' consigliato utilizzare nomi assoluti per i percorsi dei file di log. Altrimenti i file di log verranno creati nella directory relativa all'applicazione chiamante e potrebbe essere difficile rintracciarli.

Abilitare i diritti di accesso sufficienti per tutti gli utenti che vogliono scrivere i file di log.

## 8.1.1 Log PKCS#11

Il log della libreria PKCS#11 di CardOS API è controllata dai seguenti settaggi:

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API\P11LogFile]<sup>1</sup> e  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API\P11LogLevel]<sup>2</sup>

Chiave	Tipo	Descrizione	Predefinito
P11LogFile	REG_SZ	Percorso completo del file di log PKCS#11. Se questo parametro è vuoto, non viene scritto alcun log.	C:\pkcs11.log <sup>3</sup>
P11LogLevel	REG_DWORD	Livello di log PKCS#11.	0

Il nome del file del log PKCS#11 può contenere le seguenti wildcard:

Wildcard	Descrizione
&u	Nome dell'utente corrente.
&p	Id del processo corrente.

Ad esempio, configurando il nome del file di log come "C:\temp\pkcs11.&u.&p.log" verrà creato un file di log con nome "C:\temp\pkcs11.utente23.0123.log" assumendo che l'utente corrente è chiamato "utente23" e il processo che ha creato il file di log ha Id "0123".

<sup>1</sup> Usare [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Siemens\CardOS API\P11LogFile] per configurare le applicazioni a 32-bit che girano su sistemi operative a 64-bit

<sup>2</sup> Usare [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Siemens\CardOS API\P11LogLevel] per configurare le applicazioni a 32-bit che girano su sistemi operative a 64-bit.

<sup>3</sup> L'utente potrebbe non avere i diritti di creare o scrivere su un file di log con questo percorso. E' consigliato cambiare questo percorso con uno in una directory in cui l'utente ha pieni diritti.

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API\P11LogLevel]<sup>4</sup> può essere usato per decidere il livello di log così come definito nella tabella seguente.

Livello	Significato	Descrizione
0	Nessun Log	Non viene scritto alcun log.
1	Minimo	Viene scritto solo un minimo di informazioni di log.
2	Errori	Vengono scritti solo errori critici ed eccezioni.
3	Avvisi	Vengono scritti solo errori critici, eccezioni e avvisi.
4	Più Informazioni	Vengono scritti solo errori critici, eccezioni, avvisi e informazioni.
5	Trace	Vengono scritti gli argomenti delle funzioni a livello di API. Questo è il livello minimo di log da utilizzare per l'invio di un report di errore con file di log allegati.
6	Debug	Vengono scritte informazioni interne di debug addizionali. Questo è il livello raccomandato di log da utilizzare per l'invio di un report di errore con file di log allegati.
7	ASN.1	Vengono scritte le strutture ASN.1 lette dalla smart card. Questo settaggio aumenta considerevolmente la dimensione dei file di log. Non è consigliato utilizzare questo livello di log se non richiesto esplicitamente dal contatto del supporto tecnico.
8	Tutto	

---

<sup>4</sup> Usare [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Siemens\CardOS API\P11LogFile] per configurare le applicazioni a 32-bit che girano su sistemi operative a 64-bit.

## 8.1.2 Log CSP

Il log del CSP Siemens Card API CSP è configurato dai seguenti settaggi:

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API\CSPLogFile] e  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API\CSPLogLevel]

Chiave	Tipo	Descrizione	Predefinito
CSPLogFile	REG_SZ	Percorso completo del file di log del CSP. Se questo parametro è vuoto, non viene scritto alcun log.	C:\csp.log <sup>5</sup>
CSPLogLevel	REG_DWORD	Livello di log del CSP.	0

Il nome del file del log del CSP può contenere le seguenti wildcard:

Wildcard	Descrizione
&u	Nome dell'utente corrente.
&p	Id del processo corrente.

Ad esempio, configurando il nome del file di log come "C:\temp\csp.&u.&p.log" verrà creato un file di log con nome "C:\temp\csp.utente23.0123.log" assumendo che l'utente corrente è chiamato "utente23" e il processo che ha creato il file di log ha Id "0123".

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API\CSPLogLevel] può essere usato per decidere il livello di log così come definito nella tabella seguente.

Livello	Significato	Descrizione
0	Nessun Log	Non viene scritto alcun log.
1	Minimo	Viene scritto solo un minimo di informazioni di log.
2	Errori	Vengono scritti solo errori critici ed eccezioni.
3	Avvisi	Vengono scritti solo errori critici, eccezioni e avvisi.
4	Più Informazioni	Vengono scritti solo errori critici, eccezioni, avvisi e informazioni.
5	Trace	Vengono scritti gli argomenti delle funzioni a livello di API. Questo è il livello minimo di log da utilizzare per l'invio di un report di errore con file di log allegati.
6	Debug	Vengono scritte informazioni interne di debug aggiuntive. Questo è il livello raccomandato di log da utilizzare per l'invio di un report di errore con file di log allegati.
7	ASN.1	Non applicabile per il log CSP, quindi si applica quanto detto per il livello 6
8	Tutto	

<sup>5</sup> L'utente potrebbe non avere i diritti di creare o scrivere su un file di log con questo percorso. E' consigliato cambiare questo percorso con uno in una directory in cui l'utente ha pieni diritti.

### 8.1.3 Log della propagazione dei certificati

Il log della propagazione dei certificati di CardOS dalle smart card agli store dei certificati di Microsoft è configurato dai seguenti settaggi:

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API\CertstoreLogFile] e  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API\CertstoreLogLevel]

Chiave	Tipo	Descrizione	Predefinito
CertstoreLogFile	REG_SZ	Percorso completo del file di log della propagazione dei certificati. Se questo parametro è vuoto, non viene scritto alcun log.	C:\certstore.log <sup>6</sup>
CertstoreLogLevel	REG_DWORD	Livello di log della propagazione dei certificati.	0

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API\CertstoreLogLevel] può essere usato per decidere il livello di log così come definito nella tabella seguente.

Livello	Significato	Descrizione
0	Nessun Log	Non viene scritto alcun log.
1	Minimo	Viene scritto solo un minimo di informazioni di log.
2	Errori	Vengono scritti solo errori critici ed eccezioni.
3	Avvisi	Vengono scritti solo errori critici, eccezioni e avvisi.
4	Più Informazioni	Vengono scritti solo errori critici, eccezioni, avvisi e informazioni.
5	Trace	Non applicabile per il log di CertStore, quindi si applica quanto detto per il livello 4
6	Debug	Vengono scritte informazioni interne di debug addizionali. Questo è il livello raccomandato di log da utilizzare per l'invio di un report di errore con file di log allegati.
7	ASN.1	Non applicabile per il log di CertStore, quindi si applica quanto detto per il livello 6
8	Tutto	

### 8.1.4 Log dell'interfaccia con la Smart Card

Il log dei dati inviati alla smart card e ricevuti dalla smart card è abilitato impostando la chiave di registro REG\_SZ: [HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API\SCardLogFile]

Chiave	Tipo	Descrizione	Predefinito
SCardLogFile	REG_SZ	Percorso completo del file di log dell'interfaccia della smart card. Se questo parametro è vuoto, non viene scritto alcun log.	Non presente

<sup>6</sup> L'utente potrebbe non avere i diritti di creare o scrivere su un file di log con questo percorso. E' consigliato cambiare questo percorso con uno in una directory in cui l'utente ha pieni diritti.



## 8.2 Opzioni PKCS#11

L'implementazione dell'interfaccia PKCS#11 di CardOS API può essere configurata attraverso la chiave di registro: [HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API]

Chiave	Tipo	Descrizione	Predefinito
P11Flags	REG_DWORD	Nessun flag definito attualmente.	Non presente
P11GDOv1TokenLabel	REG_SZ	Siccome i token GDOv1 (cioè le smart card inizializzate con CardOS API precedenti alla versione 3.0) non sono dotati di una etichetta individuale di smart card, CardOS API solitamente restituisce "CardOS GDOv1 Token" per questo tipo di token. Questa chiave di registro permette di sostituire questa etichetta statica con una dicitura a propria scelta. La lunghezza dell'etichetta token è limitata a 32 caratteri.	Non presente
P11MinorVersionOverride	REG_DWORD	Sovrascrive la versione minore della versione della libreria cryptoki ottenuta da C_GetFunctionList() e C_GetInfo(). Questo settaggio può essere utilizzato per risolvere problemi di interoperabilità con alcune applicazioni che si aspettano una versione cryptoki inferiore a 2.11. Cambiare questo valore potrebbe causare effetti indesiderati con altre applicazioni che invece si aspettano la versione 2.11 di cryptoki.	Non presente
P11ScriptDir	REG_SZ	Specifica il percorso degli script richiesti per l'inizializzazione della smart card. Questo valore è impostato dal setup di CardOS API.	Punta alla directory \scripts sotto la directory di installazione di CardOS API selezionata durante il Setup.
P11VirtualTokens	REG_DWORD	Riservato per usi futuri.	Non presente

## 8.3 Opzioni CSP

Il CSP Siemens Card API CSP può essere configurato con i settaggi delle sotto chiavi di registro [HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API] definite nella tabella seguente:

Chiave	Tipo	Descrizione	Predefinito
CSPFlags	REG_DWORD	Consultare la tabella sottostante per i flag validi.	Non presente, 0 viene usato come predefinito
CSPPinCacheExpirationTime	REG_DWORD	Periodo di scadenza in secondi della cache dei PIN del CSP (0 = Nessuna scadenza). Se il periodo di tempo specificato è passato e l'applicazione deve chiedere il PIN all'utente, verrà richiesto il PIN indipendentemente dalla cache del PIN. A seconda dello stato interno del CSP, potrebbe essere richiesto il PIN all'utente anche prima della scadenza di questo periodo di tempo. I PIN che sono stati impostati dall'applicazione in un contesto acquisito in modo silente, non scadono mai.	0

Il valore dato in [HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API\CSPFlags] rappresenta varie opzioni Booleane. Ogni opzione disponibile è rappresentata da un valore intero unico (ognuno di essi è una potenza di 2). Per abilitare più di una opzione alla volta, è necessario sommare i valori:

Flag	Significato	Descrizione
1	Ignora CRYPT_ARCHIVABLE	Se questo flag è attivo, il flag CRYPT_ARCHIVABLE di CryptGenKey() viene ignorato.
2	Permetti la generazione software delle chiavi	Se questo flag non è attivo, la generazione delle chiavi asimmetriche viene sempre eseguita sulla smart card.
4	Riservato	Non configurare questo flag per questa versione di CardOS API.
8	Riservato	Non configurare questo flag per questa versione di CardOS API.
16	Utilizza la cache dei PIN per le operazioni di firma.	Il comportamento predefinito di CardOS API è di richiedere il PIN utente per ogni operazione di firma in un contesto CSP non silente. Le operazioni di decifra saranno sempre in grado di utilizzare la cache dei PIN. Se questo flag è attivo, le strategie di cache del PIN sono portate indietro a quelle delle versioni precedenti a CardOS API V3.1 B, ovvero un PIN in cache può essere ereditato ed utilizzato da un nuovo contesto CSP sia per le operazioni di firma sia per quelle di decifra.
32..2 <sup>31</sup>	Riservato	Non configurare queste opzioni.

La seguente tabella fornisce una panoramica sull'interdipendenza dei flag del CSP che influenzano la generazione di una coppia di chiavi RSA:

CSPFlags	Descrizione
0	<b>Forza la generazione della chiave su smart card</b> La chiamata a CryptGenKey() con il flag CRYPT_ARCHIVABLE abilitato, fallirà immediatamente.
1	<b>Forza la generazione della chiave su smart card</b> Il flag CRYPT_ARCHIVABLE viene ignorato quando passato a CryptGenKey(). Le coppie di chiavi asimmetriche sono sempre generate sulla smart card.
2	Se CryptGenKey() è chiamata con il flag <b>CRYPT_ARCHIVABLE attivo</b> , la coppia di chiavi asimmetrica è <b>generata via software</b> e immagazzinata sulla smart card. La chiave privata può essere immediatamente archiviata dopo il processo di generazione della chiave. Se CryptGenKey() è chiamata con il flag <b>CRYPT_ARCHIVABLE disattivo</b> la coppia di chiavi asimmetrica è <b>generata sulla smart card</b> .
3	Lo stesso del valore 1.

## 8.4 Opzioni della propagazione dei certificati

La propagazione automatica dei certificati di CardOS API può essere configurata con i settaggi delle sotto chiavi di registro [HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API] definite nella seguente tabella:

Chiave	Tipo	Descrizione	Predefinito
--------	------	-------------	-------------

## 8 Configurare CardOS API

CertstoreFlags	REG_DWORD	Consultare la tabella sottostante per i flag validi.	Non presente
CertstoreSCardStartedTimeout	REG_DWORD	Timeout utilizzato per aspettare che il sotto-sistema delle smart card si riavvii dopo una riconnessione di una sessione terminal server. Il valore specifica il timeout in secondi e dovrebbe essere compresa tra diversi secondi e alcuni minuti. Se questo valore impostato a 0xFFFFFFFF il timeout è infinito. Nel caso questa sotto chiave non sia presente, si applica un valore di default di 10 secondi.	Non presente

Il valore specificato in CertStoreFlags rappresenta diverse opzioni Booleane. Ogni opzione disponibile è rappresentata da un valore intero unico (ognuno di essi è una potenza di 2). Per abilitare più di una opzione alla volta, è necessario sommare i valori (per esempio settare CertstoreFlags a 0x00000006 per abilitare le opzioni definite con i valori 0x00000002 e 0x00000004). Le seguenti opzioni possono essere configurate:

Flag	Significato	Descrizione
1	Riservato	Non configurare questo flag per questa versione di CardOS API.
2	Rendere i certificati persistenti.	I certificati che sono propagati allo store dei certificati Microsoft da CardOS API, non vengono cancellati dallo store di Microsoft quando la smart card viene rimossa dal lettore.
4	Non propagare certificati di CA.	CardOS API non propaga i certificati di CA dalla smart card allo store dei certificati Microsoft.
8	Rimuovi i certificati, quando CardOS API viene chiuso o l'utente si disconnette.	Se le opzioni 2 e 8 sono attivate, i certificati che sono stati propagati permanentemente nello store dei certificati Microsoft, non sono rimossi finquando CardOS API non viene chiuso o l'utente si disconnette da Windows.  Questo può essere utile per tenere i certificati utente, che sono stati trasferiti dalla smart card allo store dei certificati Microsoft, durante tutta la sessione utente, per poi fare pulizia dello store quando l'utente si disconnette.
16	Riservato	Non configurare questa opzione.
32	Setta il friendly name	Se questa opzione è attiva, l'attributo friendly name del certificato sarà impostata al nome del container.
64..2 <sup>31</sup>	Riservato	Non configurare queste opzioni.

## 8.5 Opzioni dell'inserimento sicuro del PIN

La lunghezza del PIN delle smart card che usano il Secure PIN Entry (SPE), può essere configurata dalle sotto chiavi di registro di [HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API] definite nella seguente tabella:

Chiave	Tipo	Descrizione	Predefinito
SCardSPEFixedPinLength <sup>7</sup>	REG_DWORD	<p>Alcuni vecchi dispositivi Secure PIN Entry (SPE) (lettori a PIN Pad) non offrono il supporto completo all'inserimento di PIN di lunghezza variabile.</p> <p>In questo caso il PIN deve essere o di una lunghezza fissa o riempito a una lunghezza fissa.</p> <p>L'inizializzazione predefinita della smart card permette un PIN a lunghezza variabile, ma non specifica un carattere di riempimento. Come soluzione, CardOS API assume una lunghezza PIN fissa di 8. Questo significa che ogni PIN inserito usando un lettore SPE deve avere una lunghezza reale di 8.</p> <p>La chiave SCardSPEFixedPinLength sovrascrive questa lunghezza fissa di PIN<sup>8</sup>.</p> <p>Un supporto migliore per i vecchi dispositivi Secure PIN Entry può essere ottenuto adattando il file system della carta alle necessità specifiche.</p>	Non presente
SCardSPETimeout01	REG_DWORD	<p>Timeout per la prima digitazione su un lettore a PIN pad.</p> <p>Valori validi sono: 1 – 60 secondi (predefinito 60).</p>	Non presente
SCardSPETimeout02	REG_DWORD	<p>Timeout dopo la prima digitazione su un lettore a PIN pad.</p> <p>Valori validi sono: 1 – 60 secondi (predefinito 60).</p> <p>Se non supportato dal lettore, si applica solo SCardSPETimeout01.</p>	Non presente



<sup>7</sup> Questa chiave di registro non è usata per i lettori a PIN pad PC/SC V2.01 part 10, in quanto questi supportano la gestione dei PIN a lunghezza variabile.

<sup>8</sup> Prima di cambiare questi settaggi, assicurarsi che i PIN sulle proprie carte siano configurati a lunghezza fissa. Altrimenti non sarà possibile verificare questi PIN utilizzando il Secure PIN Entry. Il gamma dei valori della lunghezza dei PIN va da 4 a 16.

## 9 Configurazione di CardOS API - Viewer

Il Viewer fa parte della suite di prodotti CardOS API. Il pacchetto di installazione di CardOS API crea le seguenti voci di registro [HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS APIViewer]

Le seguenti opzioni possono essere configurate usando le seguenti sotto chiavi:

Chiave	Tipo	Descrizione	Predefinito
CryptokiLibrary	REG_SZ	Nome e percorso della libreria cryptoki (PKCS#11) usata dal Viewer.	C:\WINDOWS\system32\siecap11.dll
ReadOnlyToken	REG_DWORD	Se questo valore è impostato a 1, il Viewer considera tutte le smart card come se fossero delle smart card a sola lettura. Tutte le voci di menu che richiedono l'accesso in scrittura alla smart card (ad esempio Import File) sono disabilitate.	0
P12ImportCreatePublicKey	REG_DWORD	<p>0 → Se il valore è impostato a 0, il Viewer crea un certificato e una chiave privata durante l'importazione di un file PKCS#12 (come mostrato nell'esempio in Figura 15).</p>  <p>Figura 15</p> <p>1 → Se il valore è impostato a 1, il Viewer crea un certificato, una chiave pubblica e una chiave privata durante l'importazione di un file PKCS#12 (come mostrato nell'esempio in Figura 16).</p>  <p>Figura 16</p>	0
P12ImportObjectLabelType	REG_DWORD	<p>0 → Usa il Common Name del titolare del certificato (CN) come etichetta PKCS#11 (CKA_LABEL) per gli oggetti (certificati e relative chiavi pubblica e privata) creati durante l'importazione di un file PKCS#12. Questo è il valore predefinito nel caso la chiave non fosse presente.</p> <p>1 → Crea un identificativo univoco a partire dalla chiave pubblica del certificato e la usa come etichetta PKCS#11 per gli oggetti creati durante l'importazione di un file PKCS#12.</p>	Non presente
P12ImportEnhancedKeyUsage	Subkey	<p>Lista degli OID di utilizzo chiave avanzata per i quali sarà definita una particolare corrispondenza con gli attributi cryptoki.</p> <p>Vedere sotto per dettagli.</p>	Non presente
HideChangeUserPIN	REG_DWORD	Se impostato a 1, la voce di menu "Change User PIN..." è nascosta.	Non presente
HideUnblockUserPIN	REG_DWORD	Se impostato a 1, la voce di menu "Unblock User PIN..." è nascosta.	Non presente
HideChangePUK	REG_DWORD	Se impostato a 1, la voce di menu "Change PUK..." è nascosta.	Non presente
ShowChangeSecAuthPIN	REG_DWORD	Se impostato a 1, la voce di menu "Change	Non presente

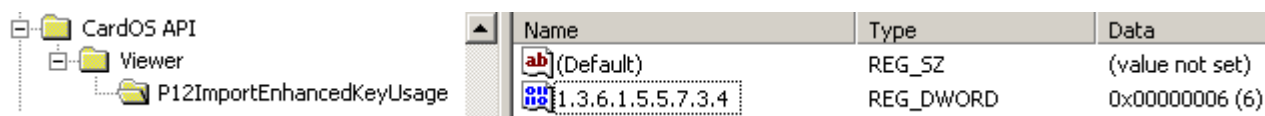
		Secondary Auth PIN..." è visualizzata.	
ShowUnblockSecAuthPIN	REG_DWORD	Se impostato a 1, la voce di menu "Unblock Secondary Auth PIN..." è visualizzata.	Non presente

Durante l'importazione di un file PKCS#12, Card Viewer deriva gli attributi cryptoki per l'utilizzo della chiave privata CKA\_SIGN, CKA\_DECRYPT e CKA\_UNWRAP dal flag utilizzo chiave del certificato X.509 (consultare PKCS#11 v2.11: Cryptographic Token Interface Standard, Tabella 35).

La voce di registro **[HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API\Viewer\P12ImportEnhancedKeyUsage]** permette di specificare ulteriori attributi cryptoki di utilizzo chiave che devono essere impostati in relazione all'estensione utilizzo avanzato della chiave nel certificato. Ogni elemento è indicato secondo l'OID che identifica l'uso avanzato della chiave e un flag REG\_DWORD che specifica l'attributo cryptoki di utilizzo chiave che deve essere impostato. Per impostare più di un attributo, i valori corrispondenti vanno sommati.

Flag	Significato	Descrizione
1	Decifra	Imposta CKA_DECRYPT nel caso il corrispondente utilizzo avanzato della chiave è trovato.
2	Unwrap	Imposta CKA_UNWRAP nel caso il corrispondente utilizzo avanzato della chiave è trovato.
4	Firma	Imposta CKA_SIGN nel caso il corrispondente utilizzo avanzato della chiave è trovato.
8..2 <sup>31</sup>	Riservato	Non configurare questa opzione.

La Figura 17 mostra un esempio che imposta CKA\_UNWRAP e CKA\_SIGN nel caso sia presente l'utilizzo avanzato della chiave Protezione email (1.3.6.1.5.5.7.3.4):



Name	Type	Data
(Default)	REG_SZ	(value not set)
1.3.6.1.5.5.7.3.4	REG_DWORD	0x00000006 (6)

Figura 17

## 10 Registrare la libreria PKCS#11 con Applicazioni di Terze Parti

Per poter utilizzare il modulo PKCS#11 di CardOS API con applicazioni di terze parti (ad esempio Firefox) è necessario registrare il modulo PKCS#11 nell'applicazione. Come questo vada eseguito dipende dalla singola applicazione – quindi riferirsi alla documentazione dell'applicazione..

Durante il processo di registrazione verrà chiesto il nome e il percorso del modulo DLL. Il nome del modulo PKCS#11 di CardOS API è **siicap11.dll**.

Il modulo è posizionato nella seguente cartella di sistema:

Predefinito: C:\WINDOWS\system32



# 11 Configurare CardOS API su Citrix Metaframe

Questa sezione descrive come configurare CardOS API per l'utilizzo con Citrix Metaframe.



## Attenzione

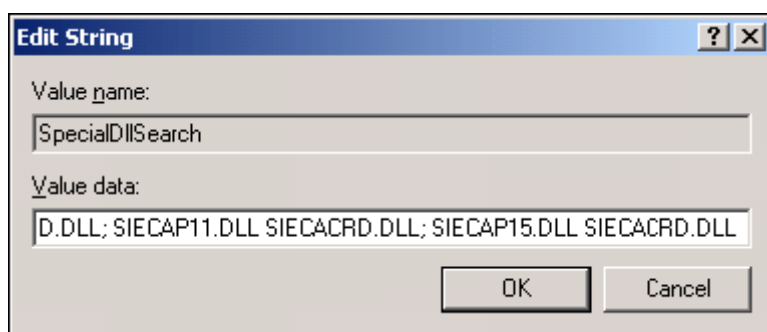
Negli ambienti di tipo terminal server la comunicazione con la smart card è esposta. Tutti i dati trasmessi vengono rediretti dall'applicazione che gira sul terminal server gestore di risorse della smart card che gira sul client remoto. La comunicazione con la smart card può essere soggetta ad attacchi sulla rete (intercettazione, uomo-nel-mezzo (man-in-the-middle)). E' fortemente raccomandato mettere in sicurezza il canale di comunicazione attraverso uno strumento quale SSL/TLS o VPN.

## 11.1 Configurazione lato Server

### 11.1.1 Abilitare Citrix Smart Card Hooking per CardOS API

Per abilitare il meccanismo di aggancio alla smart card di Citrix con CardOS API, è necessario includere le DLL di CardOS API nel *SpecialDllSearch* path di Citrix:

- Autenticarsi come amministratore di dominio sulla macchina dove è in esecuzione Citrix Metaframe Server.
- Aprire il registro di sistema e posizionarsi su:  
**HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CtxHook\Applnit\_DLLs\Smart Card Hook**  
 Se il valore *SpecialDllSearch* non esiste, creare il valore *SpecialDllSearch* con il tipo *String*
- Copiare le seguenti coppie di DLL e inserirle all'inizio del valore di *SpecialDllSearch*:  
 SIECACSP.DLL SIECACRD.DLL; SIECAP11.DLL SIECACRD.DLL; SIECAP15.DLL SIECACRD.DLL  
 Questo abilita l'aggancio alla smart card di Citrix con CardOS API.



## 11.1.2 Abilitare l'accesso remoto tramite Smart Card per le applicazioni singole



### Nota

Citrix Presentation Server V4.0 e successivi non richiede alcuna configurazione speciale per le applicazioni singole. La funzionalità di smart card è già abilitata per tutte le applicazioni in modo predefinito.

Per Citrix Metaframe Presentation Servers V3.0, ogni applicazione deve essere configurata usando lo strumento SCCONFIG.EXE in modo da garantire l'accesso remoto alla smart card.

Per eseguire SCCONFIG.EXE sono necessari i privilegi di amministratore di dominio.

La tabella seguente mostra i comandi necessari per abilitare l'accesso remoto alla smart card per alcune applicazioni. Consultare la documentazione di Citrix Metaframe Presentation Server V3.0 per dettagli su questo argomento.

Applicazione	SCConfig
<b>CardOS API</b>	
CardOS API propagazione automatica dei certificati	SCCONFIG /ENABLE_PROCESS:SIECACST.EXE
CardOS API modifica/sblocco PIN	SCCONFIG /ENABLE_PROCESS:SIECAPIN.EXE
CardOS API – Viewer	SCCONFIG /ENABLE_PROCESS:CARDVIEW.EXE
<b>Microsoft Windows Smart Card Logon</b>	
Smart Card Logon	SCCONFIG /LOGON:ON
	SCCONFIG /ENABLE_PROCESS:WINLOGON.EXE
<b>Further Third Party Applications</b>	
Microsoft Internet Explorer 6.0	SCCONFIG /ENABLE_PROCESS:IEXPLORER.EXE
Microsoft Management Console	SCCONFIG /ENABLE_PROCESS:MMC.EXE
Microsoft Outlook 2000	SCCONFIG /ENABLE_PROCESS:OUTLOOK.EXE
Microsoft Outlook Express 6.0	SCCONFIG /ENABLE_PROCESS:MSIMN.EXE
Netscape 7.1	SCCONFIG /ENABLE_PROCESS:NETSCP.EXE
Netscape Communicator 4.78	SCCONFIG /ENABLE_PROCESS:NETSCAPE.EXE

## 11.2 Configurazione lato Client

Assicurarsi che sul client sia installato solo un lettore USB di smart card. Citrix non funziona correttamente con più di un lettore USB installato sulla macchina che esegue l'ICA Client (L'articolo del Citrix Knowledge Center si trova a <http://support.citrix.com/kb/entry!default.jspx?categoryID=149&entryID=3297> e descrive questo sintomo per i token Rainbow USB, ma anche gli altri lettori sono affetti dallo stesso problema).

Per abilitare lo smart card logon per il Citrix ICA Client, impostare ICA Properties Logon Information su Smart card.

## 12 Rimuovere CardOS API

Seguire i passi successivi spiegati di seguito per rimuovere l'installazione attuale di CardOS API V3.3 CNS per Windows in ambiente Windows.

- Passo 1** ➤ Terminare CardOS API e tutte le applicazioni che usano CardOS API.
- Passo 2** ➤ Selezionare la seguente sequenza del sistema operativo:  
*Start → Pannello di Controllo → Programmi e funzionalità (o Aggiungi o rimuovi programmi)*
- Passo 3** La finestra con la lista dei programmi viene mostrata.
- Selezionare la voce CardOS API nella lista, come mostrato in Figura 18 per Windows XP.

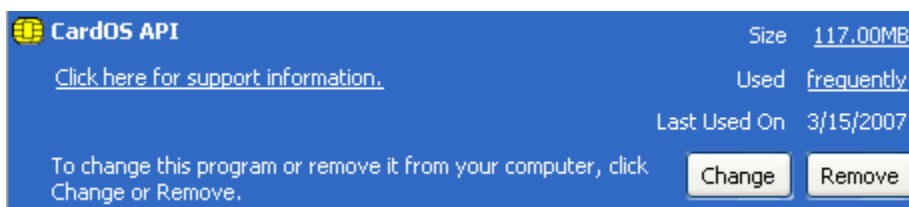
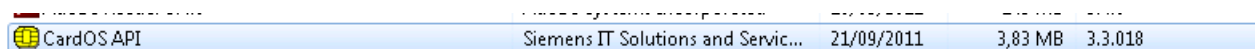


Figura 18

Su Windows Vista/7:



- Clickare il pulsante *Disinstalla*.

- Passo 4** Il CardOS API - InstallShield Wizard (vedere Figura 19) chiede conferma dell'operazione.

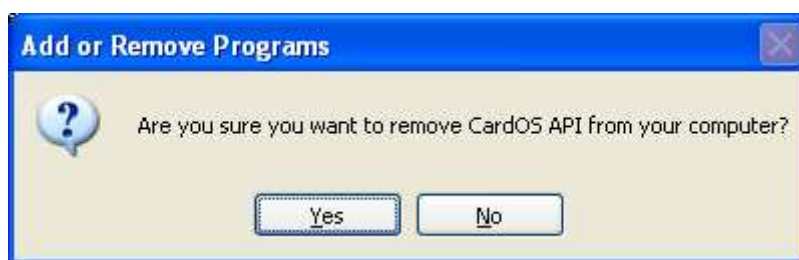


Figura 19

- Cliccare *Sì* per confermare la disinstallazione di CardOS API. Quindi attendere qualche secondo finché il software viene rimosso.



### Nota

I collegamenti a CardOS API nel menu Start di Windows potrebbero essere visibili fino al prossimo accesso al sistema.

## 13 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