SIEMENS

CardOS API V3.3 CNS per Windows

Note di rilascio **Edizione 12/2010**

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

Contenuti

1 Introduzione

Questo documento fornisce i requisiti di sistema, così come i problemi noti, per l'installazione e l'utilizzo di CardOS API per Microsoft Windows. E' consigliata la consultazione di queste informazioni prima di procedere con l'installazione.

1.1 Destinatari

Il documento CardOS API – Note di rilascio è destinato ai system integrator e agli amministratori di sistema.

1.2 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).

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 Argomento di questo rilascio

2.1 Versione rilasciata

Queste note di rilascio sono per:
CardOS API V3.3 CNS per Windows (Build 18)
Rilasciato in dicembre 2010
Nome CD: CardOSAPIV3.3W18

2.2 Software licenziato

CardOS API è un prodotto licenziato. Il numero di client installati è limitato al numero di licenze in proprio possesso. I termini e le condizioni del contratto di licenza per l'utente finale sono mostrate durante l'installazione del software.

2.3 Interfaccie Crittografiche supportate

2.3.1 Microsoft Cryptographic Service Provider Interface Versione 2

CardOS API V3.3 CNS per Windows supporta il Microsoft Cryptographic Service Provider Interface Versione 2 (CSP classico). Per informazioni dettagliate, riferirsi al Microsoft Developer Network (MSDN):

- Cryptographic Functions (http://msdn2.microsoft.com/en-us/library/Aa380252.aspx)
- The Smart Card Cryptographic Service Provider Cookbook (http://msdn.microsoft.com/en-us/library/ms953432.aspx)

2.3.2 PKCS#11 Cryptographic Token Interface Standard v2.11

CardOS API V3.3 CNS per Windows supporta il PKCS#11 Cryptographic Token Interface Standard v2.11. Le specifiche PKCS#11 sono disponibili sul sito web di RSA all'indirizzo: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v211/pkcs-11v2-11r1.pdf.

L'implementazione di CardOS API copre tutti i meccanismi, algoritmi, e funzioni così come definiti nelle sezioni 5, 6, e 8 del documento "PKCS #11: Conformance Profile Specification" (ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/pkcs11Conformance.pdf).

CardOS API V3.3 CNS per Windows supporta i tipi di oggetti:

Tipo di Oggetto	Descrizione	Immagazzinamento su Carta
CKO_CERTIFICATE	Certificato X.509[1]	sì
CKO_DATA	Dati semplici	sì
CKO_PRIVATE_KEY	Chiave privata RSA[2]	sì
CKO_PUBLIC_KEY	Chiave pubblica RSA[2]. I calcoli che usano questo tipo di oggetto sono sempre eseguiti via software.	sì
CKO_SECRET_KEY	Chiavi di sessione segrete	no

CardOS API supporta i seguenti meccanismi crittografici:

Meccanismo	Forza del meccanismo	Calcolo su Carta / Software

[1] CKA_SUBJECT e CKA_ISSUER sono in sola lettura
[2] CKA_SUBJECT è in sola lettura

Meccanismo	Forza del meccanismo	Calcolo su Carta / Software
CKM_RSA_PKCS	256 ... 2048bit	Su carta
CKM_RSA_X_509	256 ... 2048bit	Su carta
CKM_MD5_RSA_PKCS	256 ... 2048bit	Firma su carta, digest software
CKM_SHA1_RSA_PKCS	256 ... 2048bit	Firma su carta, digest software
CKM_SHA224_RSA_PKCS	256 ... 2048bit	Firma su carta, digest software
CKM_SHA256_RSA_PKCS	256 …2048bit	Firma su carta, digest software
CKM_SHA384_RSA_PKCS	256 …2048bit	Firma su carta, digest software
CKM_SHA512_RSA_PKCS	256 …2048bit	Firma su carta, digest software
CKM_MD5	128bit	Software
CKM_SHA1	160bit	software
CKM_SHA224	224bit	software
CKM_SHA256	256bit	software
CKM_SHA384	384bit	software
CKM_SHA512	512bit	software
CKM_DES_KEY_GEN	56bit	software
CKM_DES_CBC	56bit	software
CKM_DES3_KEY_GEN	168bit	software
CKM_DES3_CBC	168bit	software
CKM_RC2_KEY_GEN	40 … 128bit	software
CKM_RC2_CBC	40 … 128bit	Software
CKM_RC4_KEY_GEN	8 … 2048bit	Software
CKM_RC4	8 … 2048bit	Software
CKM_AES_CBC		Software

CardOS API non supporta funczioni per ottenere e impostare lo stato delle operazioni crittografiche (`C_GetOperationState`, `C_SetOperationState`). Le funzioni crittografiche duali (`C_DigestEncryptUpdate`, `C_DecryptDigestUpdate`, `C_SignEncryptUpdate`, `C_DecryptVerifyUpdate`) sono sono supportate e necessitano di essere divise in chiamate separate. `C_GetFunctionStatus` e `C_CancelFunction` sono deprecate e restituiscono `CKR_FUNCTION_NOT_PARALLEL`.

2.4 File System delle Carte

CardOS API V3.3 CNS per Windows supporta i seguenti tipi di carte CNS:

Tipo Carta	File system di base	File system applicazione di firma
CNS	Carta Nazionale dei Servizi, specificata in “Carta Nazionale dei Servizi CNS; File System; Terza emissione 11 marzo 2005” emesso da Centro Nazionale per l’Informatica nella Pubblica Amministratzione (CNIPA).	• CardOS DI V4.2B CNS Administrator Guidance • CardOS DI V4.2C CNS Administrator Guidance
PDC	Carta Nazionale dei Servizi, specificata in “Carta Nazionale dei Servizi CNS; File System; Terza emissione 11 marzo 2005” emesso da Centro Nazionale per l’Informatica nella Pubblica Amministratzione (CNIPA).	Non applicabile
HPC	HPC Lombardia, specificata in “Carta Regionale dei Servizi SISS, Secondo Stadio, Specifiche del Servizio” Draft version, emesso da Lombardia Integrata S.p.a; distribuito a Ottobre 2010	• CardOS V4.2 CNS Administrator Guidance • CardOS V4.2B CNS Administrator Guidance • CardOS V4.4 CNS Administrator Guidance

Le seguenti funzionalità sono supportate:

- Accesso in lettura ai certificati X.509 immagazzinati sulla carta CNS
- Esecuzione di operazioni crittografiche RSA

- Cambio del PIN utente (BSO_PIN_USR)
- Sblocco del PIN utente tramite il PUK utente (BSO_PUK_USR)
- Cambio del PIN di firma digitale (PIN_DS)
- Sblocco del PIN di firma digitale tramite il PUK di firma digitale (PUK_DS)

Le funzioni di firma digitale sono solo disponibili su carte contenenti l'applicazione di firma digitale.

Per utilizzare l'applicazione di firma digitale è necessario configurare le chiavi di secure messaging MASTER_KEY_SM_DS_KA e MASTER_KEY_SM_DS_KC.

Queste chiavi 3DES sono specificate al percorso del registro `[HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\CardOS API\CNS]`[3] utilizzando le chiavi di registro (`REG_SZ`):

```
CNSMasterKeySM_DS_KA_<iiii>_<gg>_<xx>
CNSMasterKeySM_DS_KC_<iiii>_<gg>_<xx>
```

dove:

`<iiii>` è il gruppo a 4 cifre che identifica i primi 4 byte dell'identificativo carta salvato nel file EF_ID_Carta
`<gg>` è l'identificato a 2 cifre attualmente impostato a 00
`<xx>` è l'identificativo a 2 cifre che identifica il DS_X ed è attualmente impostato a 01

Esempio:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Siemens\CardOS API\CNS]
"CNSMasterKeySM_DS_KC_6030_00_01"="4664c2291c7c029bf8763b1c345b4c344664c2291c7c029b"
"CNSMasterKeySM_DS_KA_6030_00_01"="e0f7e3c7d0a11f3209511a2ad56292dae0f7e3c7d0a11f32"
```

2.5 Oggetti Rilasciati

La tabella sottostante fornisce una panoramica dei documenti, script di inizializzazione carta, e binari per Windows contenuti nella distribuzione di CardOS API (N/A = non applicabile).

Documenti	Edizione	Descrizione
CardOS API - Note di rilascio.pdf	12/2010	Questo documento; descrive i requisiti di sistema per Windows. Così come fornisce informazioni sulle applicazioni supportate, nuove funzionalità e problemi noti.
CardOS API - Manuale di Installazione.pdf	12/2010	Contiene guide passo-passo per installare, modificare, riparare, e rimuovere CardOS API V3.3 CNS per Windows così come le informazioni di configurazione dettagliate in ambiente Windows. Questo documento è destinato agli amministratori di sistema.
CardOS API - Manuale Utente.pdf	12/2010	Descrive l'utilizzo di CardOS API durante il lavoro di tutti i giorni. Questo documento è destinato agli utenti di CardOS API.
CardOS API - Viewer - Manuale Utente.pdf	12/2010	Descrive l'utilizzo di Viewer. Questo documento è destinato agli amministratori di sistema e ai system integrator così come agli utenti che vogliono gestire gli oggetti immagazzinati sulla propria carta.

[3] Per supportare le applicazioni a 32bit sui sistemi Windows x64, queste chiavi di registro vanno anche configurate nel ramo WOW64 del registro [HKEY_LOCAL_MACHINE\Software\WOW6432Node\Siemens\CardOS API\CNS].

File Binari per Windows x86	Versione	Descrizione
CardView.exe	1.9.0.0	CardOS API - Viewer
chkSCreg.exe	1.2.2.0	Utility per il controllo dei conflitti del registro
gmp4_2_1.dll	4.2.1	Libreria GNU Multiple Precision Arithmetic Library
iplasn1.dll[4]	ipl3	Libreria ASN.1 del toolkit IPLt
iplcsp.dll[5]	ipl3	Libreria ASN.1 del toolkit IPLt
ipldev.dll[6]	ipl3	Implementazione software della libreria del dispositivo crittografico del toolkit IPL
iplutils.dll[7]	ipl3	Libreria ASN.1 del toolkit IPLt
siecaces.dll	2.4.1	Implementazione software degli algoritmi crittografici
siecacpc.dll	1.20.2.4	Modulo base del Cryptographic Service Provider (CSP)
siecacns.dll	1.1.2.2	Libreria per le carte CNS
siecacrd.dll	3.0.2.3	Libreria di accesso alla carta
siecacsp.dll	n/a	Libreria MS Cryptographic Service Provider per carte CardOS
siecacst.exe	1.13.2.3	Tool di propagazione automatica dei certificati
siecadu8.dll	3.0.2.10	Libreria di interfacce grafiche comuni
siecap11.dll	2.18.2.0	Libreria PKCS#11 per smart card CardOS
siecap15.dll	5.0.2.3	Libreria PKCS#15
siecapin.exe	1.8.2.5	Strumento di gestione PIN per CardOS API
zlib.dll[8]	1.1.4.1	Funzioni di compressione dal progetto zlib (http://www.gzip.org/zlib). La libreria di compressione zlib compression è copyright di Jean-loup Gailly e Mark Adler.

File binari per Windows x64	Versione	Descrizione
CardView.exe	1.9.0.0	CardOS API - Viewer
chkSCreg.exe	1.2.2.0	Utility per il controllo dei conflitti del registro
gmp4_2_1.dll	4.2.1	Libreria GNU Multiple Precision Arithmetic Library
iplasn1.dll[4]	ipl3	Libreria ASN.1 del toolkit IPLt
iplcsp.dll[5]	ipl3	Libreria ASN.1 del toolkit IPLt
ipldev.dll[6]	ipl3	Implementazione software della libreria del dispositivo crittografico del toolkit IPL
iplutils.dll[7]	ipl3	Libreria ASN.1 del toolkit IPLt
siecaces.dll	2.4.1	Implementazione software degli algoritmi crittografici
siecacpc.dll	1.20.2.4	Modulo base del Cryptographic Service Provider (CSP)
siecacns.dll	1.1.2.2	Libreria per le carte CNS
siecacrd.dll	3.0.2.3	Libreria di accesso alla carta
siecacsp.dll	n/a	Libreria MS Cryptographic Service Provider per carte CardOS
siecacst.exe	1.13.2.3	Tool di propagazione automatica dei certificati
siecadu8.dll	3.0.2.10	Libreria di interfacce grafiche comuni
siecap11.dll	2.18.2.0	Libreria PKCS#11 per smart card CardOS
siecap15.dll	5.0.2.3	Libreria PKCS#15
siecapin.exe	1.8.2.5	Strumento di gestione PIN per CardOS API
zlib.dll[8]	1.1.4.1	Funzioni di compressione dal progetto zlib (http://www.gzip.org/zlib). La libreria di compressione zlib compression è copyright di Jean-loup Gailly e Mark Adler.

[4] A seconda della distribuzione, il file iplasn1.dll può essere linkato staticamente a CardOS API. In questo caso nessun file separato iplasn1.dll è incluso nella distribuzione.
[5] A seconda della distribuzione, il file Iplcsp.dll può essere linkato staticamente a CardOS API. In questo caso nessun file separato Iplcsp.dll è incluso nella distribuzione.
[6] A seconda della distribuzione, il file ipldev.dll può essere linkato staticamente a CardOS API. In questo caso nessun file separato ipldev.dll è incluso nella distribuzione.
[7] A seconda della distribuzione, il file iplutils.dll può essere linkato staticamente a CardOS API. In questo caso nessun file separato iplutils.dll è incluso nella distribuzione.
[8] A seconda della distribuzione, il file zlib.dll può essere linkato staticamente a CardOS API. In questo caso nessun file separato zlib.dll è incluso nella distribuzione.

3 Requisiti di Sistema

Questa sezione elenca i requisiti hardware e software per il funzionamento di CardOS API V3.3 CNS per Windows. Assicurarsi che i seguenti prerequisiti siano soddisfatti prima di installare CardOS API.

3.1 Smart Card supportate

CardOS API V3.3 CNS per Windows supporta le carte CNS in conformità con “CNS – Carta Nazionale dei Servizi Functional Specification”, versioni da 1.1.2 a 1.1.5 emesse dal Centro Nazionale per l’informatica nella Pubblica Amministratzione (CNIPA). Le smart card devono essere inizializzate e personalizzate secondo i requisiti del file system descritti nella sezione 2.4. La tabella seguente mostra una lista degli ATR supportati ATR:

Smart Card	ATR
CardOS V4.2 HPC	3B FF 18 00 FF C1 0A 31 FE 55 00 6B 05 08 C8 05 01 12 01 48 50 43 00 31 80 <TCK>
	3B FF 18 00 FF C1 0A 31 FE 55 00 6B 05 08 C8 05 01 12 02 48 50 43 00 31 80 <TCK>
	3B FF 18 00 FF C1 0A 31 FE 55 00 6B 05 08 C8 05 01 02 01 48 50 43 00 31 80 <TCK>
	3B FF 18 00 FF C1 0A 31 FE 55 00 6B 05 08 C8 05 01 02 0A 48 50 43 00 31 80 <TCK>
CardOS V4.2 B HPC	3B FF 18 00 FF C1 0A 31 FE 55 00 6B 05 08 C8 05 01 12 02 48 50 43 00 31 80 <TCK>
	3B FF 18 00 FF C1 0A 31 FE 55 00 6B 05 08 C8 05 01 02 0A 48 50 43 00 31 80 <TCK>
	3B FF 18 00 FF C1 0A 31 FE 55 00 6B 05 08 C8 09 01 12 02 48 50 43 00 31 80 <TCK>
	3B FF 18 00 FF C1 0A 31 FE 55 00 6B 05 08 C8 09 01 02 0A 48 50 43 00 31 80 <TCK>
CardOS V4.2 PDC	3B FF 18 00 FF C1 0A 31 FE 55 00 6B 05 08 C8 05 01 11 01 43 4E 53 10 31 80 <TCK>
CardOS V4.2 B PDC	3B FF 18 00 FF C1 0A 31 FE 55 00 6B 05 08 C8 09 01 11 01 43 4E 53 10 31 80 <TCK>
CardOS DI V4.2 B PDC	3B FF 18 00 FF C1 0A 31 FE 55 00 6B 05 08 C8 0A 01 11 01 43 4E 53 10 31 80 <TCK>
CardOS DI V4.2 B CNS	3B FF 18 00 FF C1 0A 31 FE 55 00 6B 05 08 C8 0A 01 21 01 43 4E 53 10 31 80 <TCK>
CardOS DI V4.2 C CNS	3B FF 18 00 FF C1 0A 31 FE 55 00 6B 05 08 C8 0C 01 21 01 43 4E 53 10 31 80 <TCK>
CardOS V4.4 HPC	3B DF 18 02 C1 0A 31 FE 58 00 6B 05 08 C8 0D 01 12 02 48 50 43 00 31 80 <TCK>
	3B DF 18 02 C1 0A 31 FE 58 00 6B 05 08 C8 0D 01 02 0A 48 50 43 00 31 80 <TCK>
ST/Incard PDC	3B FF 18 00 FF 81 31 FE 55 00 6B 02 09 02 00 01 01 01 43 4E 53 10 31 80 <TCK>
	3B FF 18 00 FF 81 31 FE 55 00 6B 02 09 02 00 01 11 01 43 4E 53 10 31 80 <TCK>
	3B FF 18 00 FF 81 31 FE 55 00 6B 02 09 02 00 01 01 01 43 4E 53 11 31 80 <TCK>
	3B FF 18 00 FF 81 31 FE 55 00 6B 02 09 02 00 01 11 01 43 4E 53 11 31 80 <TCK>
Athena PDC	3B DF 18 00 81 31 FE 7D 00 6B 15 0C 01 80 01 01 01 43 4E 53 10 31 80 <TCK>
	3B DF 18 00 81 31 FE 7D 00 6B 15 0C 01 80 01 11 01 43 4E 53 10 31 80 <TCK>

3.1.1 Microsoft Windows

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.

3.1.2 Prerequisiti di Piattaforma

CardOS API V3.3 CNS per Windows gira su versioni di Window a 32-bit x86 e a 64-bit x64. CardOS API è stato progettato e testato per la compatibilità con le interfacce dei seguenti sistemi operativi Microsoft Windows:

Sistema Operativo	
Windows XP Professional (SP3)[9]	
Windows XP x64 Professional Edition (SP2)[9]	
Windows Vista Enterprise Edition (SP2)	
Windows Vista Enterprise x64 Edition (SP2)	
Windows 7	
Windows 7 x64 Edition	
Windows Server 2003 Enterprise Edition (SP2)[9]	
Windows Server 2003 Enterprise x64 Edition (SP2)[9]	
Windows Server 2008 Enterprise Edition (SP2)	
Windows Server 2008 Enterprise x64 Edition (SP2)	

[9] E' consigliata l'installazione dell'hot fix Microsoft RDP hot fix 925876

3.1.3 Lettori di Smart Card supportati

CardOS API V3.3 CNS per Windows è stato testato su una varietà di lettori di smart card conformi PC/SC (www.pcscworkgroup.com) su piattaforme Microsoft Windows. I driver appropriati per i lettori sono forniti dai rispettivi produttori e venditori del lettore.

Si noti che, dipendentemente all'interfaccia usata per accedere alla carta (Microsoft CAPI, PKCS#11 Cryptoki), il collegamento a caldo dei lettori non è supportato. Alcuni produttori di token USB forniscono un driver dedicato che fornisce il collegamento a caldo. Nel caso un nuovo lettore non sia riconosciuto automaticamente o da CardOS API o da un'applicazione che utilizzi CardOS API, l'applicazione corrispondente richiede un riavvio.

3.1.4 Applicazioni Supportate

CardOS API V3.3 CNS per Windows lavora su tutte le applicazioni Windows che usano le interfacce Microsoft CAPI o PKCS#11 Cryptoki per l'accesso alla smart card. Una limitazione delle funzionalità potrebbe verificarsi, se l'applicazione non è completamente conforme alle specifiche dell'interfaccia o se utilizza delle funzioni proprietarie o non documentate di altri produttori.

4 Cambiamenti rispetto ai rilasci precedenti

4.1 Nuove funzionalità

CardOS API V3.3 per Windows (CNS)

- Supporto per Carta Nazionale dei Servizi CNS
- Supporto per HPC Lombardia
- Supporto per PDC Lombardia

4.2 Problemi risolti e cambiamenti richiesti

Non applicabile.

4.3 Migrazione dalle versioni precedenti

Se una qualunque versione precedente di CardOS API V3 è già installata sul proprio sistema, è necessario rimuovere questa versione prima di installare CardOS API V3.3 CNS per Windows.

5 Informazioni sul Setup per Microsoft Windows

Questa sezione fornisce informazioni per l'installazione di CardOS API. Queste informazioni possono essere utilizzate per creare i propri script di installazione e per la distribuzione automatica del software.

Le seguenti variabili sono utilizzate:

%WINDIR%
Si riferisce alla directory di sistema di Microsoft Windows contenente tutti gli oggetti a 32-bit sui sistemi operativi a 32-bit o tutti gli oggetti a 64-bit sulle edizioni x64 dei sistemi operativi:
Default: `C:\WINDOWS\system32`

%WOW64%
Si riferisce alla directory di sistema di Microsoft Windows contenente tutti gli oggetti a 32-bit sui sistemi operativi a 64-bit:
Default: `C:\WINDOWS\SysWOW64`
Gli oggetti di questa directory sono installati solo dal setup a 64-bit (`CardOS_API_Setup_x64.exe`). Questi oggetti sono richiesti per l'utilizzo di CardOS API con applicazioni di terzi a 32-bit che girano su un PC a 64-bit.

%SIECADIR%
Si riferisce alla directory di installazione di CardOS API:
Default: `C:\Programmi\Siemens\CardOS API`

5.1 Collegamenti Creati da CardOS API Setup

I seguenti collegamenti sono creati nel menu *Start* di Windows durante il setup di CardOS API a prescindere dal setup a 32-bit o a 64-bit.

Shortcut	Target	Note
Start → Programmi → Avvio Automatico → CardOS API	"%SIECADIR%\bin\siecacst.exe"	Richiesto per avviare automaticamente CardOS API.
Start → Programmi → Siemens → CardOS API → Modifica PIN	"%SIECADIR%\bin\siecapin.exe"	Opzionale
Start → Programmi → Siemens → CardOS API → Modifica PUK	"%SIECADIR%\bin\siecapin.exe" /s	Opzionale
Start → Programmi → Siemens → CardOS API → Modifica PIN aut. sec.	"%SIECADIR%\bin\siecapin.exe" /x	Opzionale
Start → Programmi → Siemens → CardOS API → Sblocco PIN	"%SIECADIR%\bin\siecapin.exe" /u	Opzionale
Start → Programmi → Siemens → CardOS API → Sblocco PIN aut. sec.	"%SIECADIR%\bin\siecapin.exe" /y	Opzionale
Start → Programmi → Siemens → CardOS API → Viewer	"%SIECADIR%\bin\ CardView.exe"	Opzionale
Start → Programmi → Siemens → CardOS API → Documentazione → API – Manuale di Installazione	"%SIECADIR%\doc\Italiano\ CardOS API – Manuale di Installazione.pdf"	Opzionale
Start → Programmi → Siemens → CardOS API → Documentazione → API – Note di rilascio	"%SIECADIR%\doc\Italiano\ CardOS API – Note di rilascio.pdf"	Opzionale
Start → Programmi → Siemens → CardOS API → Documentazione → API – Manuale Utente	"%SIECADIR%\doc\Italiano\ CardOS API – Manuale Utente.pdf"	Opzionale
Start → Programmi → Siemens → CardOS API → Documentazione → License Agreement	"%SIECADIR%\doc\ License_Agreement_Card_API.rtf"	Opzionale
Start → Programmi → Siemens → CardOS API → Documentazione → Viewer – Manuale Utente	"%SIECADIR%\doc\English\ CardOS API – Viewer – Manuale Utente.pdf"	Opzionale

5.2 Oggetti Copiati da CardOS API Setup

Gli oggetti che possono essere rimossi dal setup senza causare alcuna limitazione di funzionalitàsono marcati come 'Opzionale'. Gli oggetti che possono essere rimossi ma che causeranno limitazioni di funzionalità sono descritti nel dettaglio.

A seconda della propria piattaforma, i file binari a 32-bit o 64-bit sono installati nelle directory %SIECADIR%\bin e %WINDIR%. Gli oggetti che appartengono alla directory di destinazione %WOW64% sono installati solo dal setup a 64-bit (`CardOS_API_Setup_x64.exe`).

Oggetto	Cartella Destinazione	Note
License_Agreement_Card_API.rtf	%SIECADIR%\doc	Opzionale
CardOS API – Release Notes.pdf	%SIECADIR% \doc\Italiano	Opzionale
CardOS API – Installation Manual.pdf	%SIECADIR% \doc\Italiano	Opzionale
CardOS API – User Manual.pdf	%SIECADIR% \doc\Italiano	Opzionale
CardOS API – Viewer – User Manual.pdf	%SIECADIR% \doc\Italiano	Opzionale
CardView.exe	%SIECADIR%\bin	Può essere rimosso: il Viewer non sarà disponibile per l'utilizzo.
chkSCreg.exe	%SIECADIR%\bin	Opzionale
siecacst.exe	%SIECADIR%\bin	Richiesto
siecapin.exe	%SIECADIR%\bin	Può essere rimosso: non sarà possibile cambiare o sbloccare il PIN, PUK e il PIN di firma. Gli elementi "Modifica PIN…" e "Sblocco PIN…" saranno rimossi dal menu contestuale dell'icona CardOS API nella task bar.
gmp4_2_1.dll	%WINDIR%	Richiesto
iplasn1.dll[10]	%WINDIR%	Richiesto
iplcsp.dll[11]	%WINDIR%	Richiesto
ipldev.dll[12]	%WINDIR%	Richiesto
iplutils.dll[13]	%WINDIR%	Richiesto
siecaces.dll	%WINDIR%	Richiesto
siecacpc.dll	%WINDIR%	Richiesto
siecacsp.dll	%WINDIR%	Richiesto
siecacns.dll	%WINDIR%	Richiesto
siecacrd.dll	%WINDIR%	Richiesto
siecadu8.dll	%WINDIR%	Richiesto
siecap11.dll	%WINDIR%	Richiesto
siecap15.dll	%WINDIR%	Richiesto
zlib.dll[14]	%WINDIR%	Richiesto
gmp4_2_1.dll	%WOW64%	Richiesto
iplasn1.dll[10]	%WOW64%	Richiesto
iplcsp.dll[11]	%WOW64%	Richiesto
ipldev.dll[12]	%WOW64%	Richiesto
iplutils.dll[13]	%WOW64%	Richiesto
siecaces.dll	%WOW64%	Richiesto
siecacpc.dll	%WINDIR%	Richiesto

[10] A seconda della distribuzione, il file iplasn1.dll può essere linkato staticamente a CardOS API. In questo caso nessun file separato iplasn1.dll è incluso nella distribuzione.
[11] A seconda della distribuzione, il file Iplcsp.dll può essere linkato staticamente a CardOS API. In questo caso nessun file separato Iplcsp.dll è incluso nella distribuzione.
[12] A seconda della distribuzione, il file ipldev.dll può essere linkato staticamente a CardOS API. In questo caso nessun file separato ipldev.dll è incluso nella distribuzione.
[13] A seconda della distribuzione, il file iplutils.dll può essere linkato staticamente a CardOS API. In questo caso nessun file separato iplutils.dll è incluso nella distribuzione.
[14] A seconda della distribuzione, il file zlib.dll può essere linkato staticamente a CardOS API. In questo caso nessun file separato zlib.dll è incluso nella distribuzione.

Oggetto	Cartella Destinazione	Note
siecacsp.dll	%WINDIR%	Richiesto
siecacns.dll	%WINDIR%	Richiesto
siecacrd.dll	%WOW64%	Richiesto
siecadu8.dll	%WOW64%	Richiesto
siecap11.dll	%WOW64%	Richiesto
siecap15.dll	%WOW64%	Richiesto
zlib.dll[14]	%WOW64%	Richiesto

5.3 Settaggi di registro richiesti da CardOS API

Questa sezione descrive i settaggi di default del registro scritti durante il setup. Riferirsi al documento CardOS API – Manuale di Installazione per ulteriori settaggi del registro.

5.3.1 Registro di Microsoft CSP

In caso di installazione personalizzata, dopo aver copiato i file elencati sopra, il modulo Siemens Card API CSP deve essere registrato su Microsoft Windows. Includere il seguente comando nel proprio pacchetto di setup per registrare il modulo CSP (alcuni programmi di Setup – ad esempio InstallShield – lo fanno automaticamente se riconoscono una DLL ad auto-registrazione):

```
regsvr32 %WINDIR%\SIECACSP.DLL
```

Per de-registratore il modulo Siemens Card API CSP usare il seguente comando:

```
regsvr32 /u %WINDIR%\SIECACSP.DLL
```

6 Considerazioni di Sicurezza

Dato che CardOS API sarà verosimilmente utilizzato in ambienti che trattano informazioni sensibili, prima di utilizzare CardOS API, considerare i seguenti punti:

- CardOS API usa lo standard PC/SC per comunicare con la smart card. Questa comunicazione può essere intercettata per spiare informazioni sensibili (ad esempio i PIN, i risultati di operazioni di decifra) o per causare risultati sbagliati (ad esempio verifica positiva di una firma non valida).
  E' fortemente consigliato prendere misure efficaci per proteggere la sicurezza globale del sistema e tenere lontani dal sistema Trojan Horses e altro software malevolo.

- Nel caso si voglia utilizzare CardOS API in scenari di rete (Remote Desktop, Terminal Server), sono necessarie misure appropriate per mettere in sicurezza le proprie comunicazioni di rete.

7 Problemi noti

I seguenti punti descrivono limitazioni note e problemi di interoperabilità della versione attuale di CardOS API. La lista include tutti i problemi noti indipendentemente dal sistema operativo. La lista è stata numerata per una più semplice consultazione. I numeri assegnati non riflettono alcuna severità o priorità assegnataal problema.

1. Lo standard PKCS#11 Cryptographic Token Interface non supporta il collegamento a caldo dei lettori di carte o dei token USB. Tutte le applicazioni che usano CardOS API devono essere chiuse e riavviatese un nuovo lettore è stato installato o rimosso dal sistema.

2. Alcuni lettori di smart card non sono in grado di accedere a carte CardOS alla velocità più alta in baud suggerita dall'ATR CardOS. I lettori affetti da questo problema, non negoziano una connessione a velocità minori e la comunicazione con la smart card non funziona. L'ATR CardOS può essere configurato per suggerire una velocità fissa in baud (ad esempio 9600 bit/s e superiori) per evitare questi problemi al costo di prestazioni di sistema. Referirsi al documento CardOS Manuale Utente per maggiori informazioni.

3. Gli handler IFD di alcuni lettori di smart card non implementato correttamente il supporto per il comando ISO time wait (WTX). Questi lettori falliscono l'esecuzione di comandi che richiedono tempi lunghi come il comando `GENERATE KEY PAIR`.

4. Utenti di terminal service con profilo Roaming che utilizzano sistemi con periferiche differenti (lettori di smart card) potrebbero dover riavviare le applicazioni che utilizzano CardOS API.

5. A seconda della versione del protocollo di Citrix ICA usato, il protocollo Citrix ICA non supporta più di un lettore USB su un client Citrix ICA.

6. Potrebbe essere richiesto il riavvio dell'applicazione di propagazione automatica dei certificati di CardOS API dopo la riconnessione di una sessione remota Citrix.

7. Le chiavi private protette da un PIN di Secondary Authentication non dovrebbero mai essere usate nè per lo Smart Card Logon Windows, nè per la funzione *Run as… (Esegui come...*), nè per EFS (Encrypted File System), altrimenti CardOS API potrebbe non funzionare correttamente.

8. Le funzioni di Microsoft Vista *Run as…* (*Esegui come...*) e EFS (Encrypted File System) non funzionano correttamente se più di una smart card è inserita.

9. Il pannello di preview di Outlook Express dovrebbe essere disattivato.

10. Il pannello di preview di Windows Mail per Windows Vista dovrebbe essere disattivato.

11. Alcune applicazioni eseguite su Windows Vista/7 potrebbero non avere sufficienti privilegi per scrivere i file di log.

12. Il gestore di default CCID IFD fornito con Microsoft Windows non supporta correttamente le APDU estese. Questo significa che le chiavi a 2048 bit non possono essere usate. In tal caso è necessario installare il gestore IFD fornito dal produttore del proprio lettore di smart card.

13. L'installer di CardOS API imposta il proprio linguaggio dipendentemente dal Linguaggio impostato nelle opzioni *Paese e lingua*. Questo può risultare in un linguaggio differente dal proprio systema Windows nativo.

14. Alcune applicazioni PKCS#11 (ad esempio Firefox) non sono in grado di gestire più di una smart card con la stessa label del token. Tenere a mente questo prima di inizializzare le carte.

15. La dimensione dei certificati non deve eccedere i 4096 byte.

16. A seconda del tipo della card, Card Viewer potrebbe non visualizzare le informazioni in tutti i campi informativi.

17. L'installer include un pacchetto con le librerie di runtime Microsoft Visual C++ 2005. Nel caso queste librerie manchino dopo l'installazione, è consigliato reinstallare il Visual C++ 2005 Redistributable Package. Le librerie per piattaforme x86 sono fornite da Microsoft come `vcredist_x86.exe` (http://www.microsoft.com/downloads/details.aspx?familyid=32bc1bee-a3f9-4c13-9c99-220b62a191ee&displaylang=en). Le librarie per piattaforme x64 sono fornite da Microsoft come `vcredist_x64.exe` (http://www.microsoft.com/downloads/details.aspx?familyid=90548130-4468-4BBC-9673-D6ACABD5D13B&displaylang=en).

18. CardOS API V3.3 (CNS) non fornisce script di inizializzazione, ovvero le funzioni per inizializzare nuovi token non saranno eseguite con successo.

Riferirsi anche alla lista dei Problemi Noti contenuta sul supporto di installazione che potrebbe fornire informazioni dell'ultima ora e note sui cambiamenti.

8 Come riportare i problemi

Utilizzare la scheda Registrazione Ticket (situata sul CD-ROM in formato PDF e Word) per segnalare un problema o richiedere un cambiamento. Inviare la scheda compilata al contatto indicato nel contratto di assistenza (o il contratto del partner). Nel caso non si disponga di un contratto di assistenza, contattare il proprio agente commerciale.

Prima di compilare la scheda Registrazione Ticket, sono necessarie le seguenti informazioni:

- *Informazioni Contatto*
  Azienda, Stato, Nome, E-mail, No. Contratto Assistenza, e ticket di riferimento cliente.
- *Numero Contratto di Manutenzione*
  Numero identificativo del proprio contratto di manutenzione con il proprio Rappresentante Commerciale della Smartcard Solutions.
- *Descrizione*
  Nome Prodotto, Numero Versione, Numero Build, e descrizione del problema.
- *Informazioni sul Sistema*
  Piattaforma OS, Versione OS, Tipo Processore, Tipo Smart Card, e Lettore Smart Card.
- *Informazioni sull'Ambiente*
  Descrizione dell'architettura (ad esempio Client/Server, Workflow, ecc...).
- *File Allegati*
  Log della smart card Log o file di Log locali così come spiegato nel Manuale di Installazione.

9 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 emettitrice.
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 eseguiono funzioni crittografiche.
CSP	Cryptographic Service Provider (CSP). Un CSP è responsabile della crezione 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, independentemente 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 systema 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 cosidetto 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