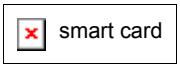
Autenticazione con SMART CARD in WINDOWS
Smart Card



Una *smartcard* è un dispositivo che ha le dimensioni di una carta di credito, è protetto da una *password*, ed integra un processore a 8 *bit*, un coprocessore crittografico e un sistema per l'archiviazione locale. La *card* utilizza un sistema operativo dedicato che risiede all'interno di un *chip* ROM con capacità compresa tra 6 e 24 *Kbyte*. Un *chip* EPROM (*Erasable Programmable Read Only Memory*) con capacità compresa tra 1 e 16 *Kbyte* consente invece di memorizzare una quantità limitata di dati dell'utente, per esempio i certificati e le chiavi private. Tali *chip* EPROM dispongono di una limitata quantità di RAM per i dati di *runtime*, compresa tra 128 e 512 *byte*.

È possibile archiviare in una *smartcard* un certificato rilasciato da *Certificate Server*. Successivamente, se al *computer* viene collegato un lettore di *smartcard* si potrà accedere al certificato. La portabilità delle *smartcard* rende possibile usare il certificato su qualsiasi *computer* che sia dotato di un apposito lettore.

La diffusione di un modello *standard* che determina il modo in cui i lettori e le *smart card* si interfacciano con un *computer* promuove l'interoperabilità tra *smart card* e lettori di diversi produttori. Nel passato, la mancanza di interoperabilità è stata una delle ragioni principali della lenta diffusione delle *smart card* al di fuori dell'Europa.

Lo *standard* principale nel settore dell'interoperabilità tra lettori e *smart card* è lo *standard* ISO 7816 per le *smart card* a circuito integrato con contatto. Queste specifiche hanno come obiettivo l'interoperabilità a livello fisico, elettrico e di protocollo per il collegamento dati. Questi *standard* sono stati incorporati nelle seguenti iniziative:

- *Europay*, MasterCard e VISA (EMV). Nel 1996, l'iniziativa EMV ha definito una specifica per *smart card* basata sullo *standard* ISO 7816, destinata soprattutto al settore dei servizi finanziari.
- Sistema GSM (*Global System for Mobile Communications*). Il settore europeo delle telecomunicazioni ha adottato gli *standard* ISO 7816 per le specifiche delle *smart card* per abilitare l'identificazione e l'autenticazione degli utenti di telefonia mobile.

Sebbene queste specifiche abbiano rappresentato un passo nella giusta direzione, ognuna di esse rappresentava un livello eccessivamente basso o era troppo specifica rispetto alle applicazioni per poter ottenere un supporto più ampio e diffuso e pertanto non è stato possibile risolvere le problematiche legate all'interoperabilità delle applicazioni. Nel 1996 è stato costituito il gruppo di lavoro PC/SC, formato da aziende del settore informatico e delle *smart card*, tra cui *Microsoft*, *Hewlett-Packard*, *Schlumberger* e *Gemplus*, proprio al fine di sviluppare specifiche volte alla soluzione di tali problematiche.

La versione 1.0 della specifica è stata pubblicata nel dicembre del 1997 e ha ottenuto un ampio supporto nel settore. *Microsoft* ha partecipato rendendo disponibili i componenti di base per *smart card*, scaricabili gratuitamente dal *Web* e validi per i sistemi operativi *Microsoft Windows* 95, *Microsoft Windows* 98, *Microsoft Windows Millennium Edition* (Me) e *Microsoft Windows* NT 4.0. Tali componenti sono inclusi in *Windows* 2000.

Componenti base 1

Componenti *software*

Le interfacce **API** indipendenti dalle periferiche consentono agli sviluppatori di applicazioni di non occuparsi delle differenze tra le realizzazioni attuali e quelle future. Dal punto di vista di uno sviluppatore di applicazioni, esistono tre metodi di programmazione per le *smart card*:

- **API** *Microsoft Win32*.
- Crypto**API**.
- SCard COM.

Il metodo scelto dipende dal tipo di applicazione e dalle capacità di una *smart card* specifica.

Win32

Le interfacce **API** *Win32* sono quelle di livello base per l'accesso alle *smart card*. Per un efficace utilizzo di tali interfacce **API**, è necessaria un'approfondita conoscenza del sistema operativo *Windows* e delle *smart card*. Tali interfacce offrono all'applicazione una grande flessibilità per il controllo di lettori, *smart card* e altri componenti correlati. Per gli sviluppatori che intendono avere il massimo controllo sul modo in cui un'applicazione utilizza le *smart card*, l'estensione all'**API** *Win32* di base rende disponibili le interfacce necessarie per la gestione dell'interazione con le periferiche per *smart card*.

CryptoAPI

Crypto**API** è l'interfaccia **API** crittografica di *Microsoft*. È concepita in modo da potersi astrarre dai dettagli della funzione di crittografia, ad esempio dagli algoritmi di crittografia, in modo che le applicazioni possano utilizzare una crittografia collegabile. Per ottenere ciò, le **API** vengono sovrapposte a moduli crittografici sostituibili detti *provider* CSP (*Cryptographic Service Provider*). I *provider* CSP possono essere prodotti basati solo sul *software*, oppure far parte di una soluzione *hardware* nella quale il motore crittografico risiede in una *smart card* o in un altro elemento *hardware* collegato al *computer*.

Nel modello *Microsoft* per l'accesso alle *smart card*, il *provider* CSP per *smart card* è associato a un tipo specifico di *smart card*, rendendo così disponibile l'associazione tra le funzioni crittografiche esposte tramite l'interfaccia Crypto**API** e i comandi di basso livello accessibili tramite le interfacce **API** *Win32* per *smart card*. Pertanto, il *provider* CSP è in grado di indicare alla *smart card* come portare a termine specifiche operazioni di crittografia. In *Windows* 2000, *Microsoft* ha integrato due *provider* CSP che supportano diverse *smart card* prodotte da *Gemplus* e da *Schlumberger*. Altri fornitori hanno sviluppato *provider* CSP specifici per le proprie *smart card*.

SCard COM

SCard COM è un'interfaccia non crittografica resa disponibile da *Microsoft* per accedere a servizi generici basati su *smart card* utilizzando applicazioni scritte in linguaggi diversi, ad esempio C, *Microsoft Visual* C++, *Java* e *Microsoft Visual Basic*.

L'interfaccia SCard COM rende disponibili a un'applicazione i servizi non crittografici di una *smart card*, mediante *provider* di servizi che supportano interfacce specifiche. Un'interfaccia per *smart card* include un insieme predefinito di servizi, i protocolli necessari per richiamare tali servizi e quanto presupposto dal contesto di questi servizi. È qualcosa di simile all'identificatore di applicazioni ISO 7816-5, ma con un ambito diverso.

Una *smart card* è in grado di registrare il supporto per un'interfaccia tramite l'associazione con il **GUI**D (Identificatore univoco globale, *Globally Unique IDentifier*) dell'interfaccia. Questo collegamento tra *smart card* e interfaccia avviene quando la *smart card* viene inserita per la prima volta nel sistema, in genere al momento dell'installazione del *provider* di servizi. Dopo aver inserito

la *smart card* nel sistema, le applicazioni possono eseguire la ricerca di *smart card* in base a un'interfaccia o a un **GUI**D specifici. Ad esempio, è possibile rendere disponibile alle applicazioni *Windows* una *smart card* per prelievo di denaro, registrando le interfacce affinché accedano al relativo schema di spesa.

Integrandoli nella versione 1.0 di *Smart Card Base Components*, *Microsoft* ha reso disponibili vari *provider* di servizi di livello base in grado di eseguire operazioni generiche, ad esempio l'individuazione delle *smart card*, la gestione APDU (*Application Protocol Data Unit*) di comandi e risposte nonché l'accesso al *file system* delle *smart card*. I *provider* di servizi resi disponibili da *Microsoft* vengono installati come oggetti interfaccia COM per consentire agli sviluppatori di *software* e ai *provider* di *smart card* di sviluppare *provider* di servizi e applicazioni di livello superiore.

Gli sviluppatori di *software* possono utilizzare strumenti di sviluppo *standard* quali *Visual* C++ e *Visual Basic* per sviluppare applicazioni e *provider* di servizi in grado di utilizzare le *smart card*.

Componenti base 2

Il sottosistema per *smart card* include i componenti seguenti:

- *Provider* di servizi: *provider* CSP per *smart card* e *provider* di servizi SCard COM.
- Gestore di risorse.
- *Driver* di periferica.
- Libreria di *driver* per lettori.

Provider **di servizi**

Affinché le applicazioni *Windows* siano in grado di accedere ai servizi basati su *smart card*, tutte le *smart card* devono disporre di almeno un *provider* di servizi. A seconda del tipo di *smart card* e del relativo distributore, possono esistere più *provider* di servizi. In generale, esistono due categorie di *provider* di servizi: crittografici e non crittografici.

Gestore di risorse

Il gestore di risorse delle *smart card* viene eseguito come servizio attendibile (*trusted*) in un unico processo. Tutte le richieste di accesso con *smart card* vengono indirizzate mediante il gestore di risorse al lettore che contiene la *smart card*. Pertanto, il gestore di risorse è responsabile della gestione e del controllo dell'accesso di tutte le applicazioni a qualsiasi *smart card* inserita in qualsiasi lettore collegato a un *computer* che esegue un sistema operativo *Windows*. Il gestore di risorse rende disponibile a una determinata applicazione una connessione virtuale diretta alla *smart card* richiesta.

Durante la gestione dell'accesso a più lettori e *smart card*, il gestore di risorse esegue tre attività fondamentali. Innanzitutto identifica e registra le risorse. In secondo luogo, controlla l'allocazione dei lettori e delle risorse tra più applicazioni. Infine, supporta le transazioni essenziali per l'accesso ai servizi disponibili in una *smart card* specifica. Si tratta di un aspetto importante, poiché le *smart card* attuali sono periferiche a *thread* singolo che spesso richiedono l'esecuzione di più comandi per portare a termine una singola funzione. Il controllo delle transazioni consente l'esecuzione senza interruzione di più comandi, garantendo così che le informazioni sullo stato intermedio non vengano danneggiate.

Driver **di periferica**

Un *driver* di periferica per un lettore specifico associa la funzionalità del lettore ai servizi originali resi disponibili dal sistema operativo *Windows* e dall'infrastruttura della *smart card*. Il *driver* del lettore comunica l'inserimento e la rimozione della *smart card* al gestore di risorse e rende disponibili le funzioni di comunicazione delle informazioni da e verso la *smart card*.

Libreria di *driver* per lettori

Smart Card Base Components 1.0 include una libreria di *driver* per lettori utilizzabile dagli sviluppatori per semplificare lo sviluppo di *driver* di periferiche. Questa libreria condivisa supporta lo *standard* ISO 7816 e le comuni funzioni di sistema necessarie alla comunicazione di dati tra una *smart card* e un lettore. Rappresenta un miglioramento significativo rispetto alle modalità con cui i *driver* per lettori di *smart card* venivano sviluppati in passato, poiché esistono oggi interfacce *standard* su cui gli sviluppatori possono basarsi. Queste interfacce comuni consentono uno sviluppo omogeneo di *driver* per lettori di *smart card* e la conseguente accessibilità da parte di tutte le applicazioni *Windows*, e non solo di un selezionato numero in grado di comunicare solo con un lettore specifico.

Soluzioni avanzate

Migliorando le soluzioni basate solo su *software*, quali l'autenticazione dei *client* e la messaggistica protetta, le *smart card* disponibili in *Windows* 2000 consentono alle applicazioni di sfruttare le opportunità offerte dall'emergente economia digitale globale. Le *smart card* offrono agli sviluppatori di applicazioni un metodo sicuro per migliorare le soluzioni per l'azienda e il consumatore.

Autenticazione *client*

L'autenticazione *client* implica l'identificazione e la convalida di un *client* a un *server* per stabilire un canale di comunicazione protetto. In genere vengono utilizzati protocolli protetti quali SSL (*Secure Sockets Layer*) o TLS (*Transport Layer Security*), di solito insieme con un certificato con chiave pubblica attendibile che viene fornito dal *client*. Questo certificato consente al *server* di identificare il *client*. Ad esempio, il *client* potrebbe essere *Microsoft Internet Explorer* in esecuzione in un sistema operativo *Windows* e il *server* potrebbe essere *Internet Information Server* o un altro *server Web* che supporta i protocolli SSL/TLS.

La sessione protetta viene stabilita utilizzando l'autenticazione con chiave pubblica con scambio di chiavi, per ricavare una chiave di sessione univoca che può essere quindi utilizzata per garantire l'integrità e la riservatezza dei dati durante la sessione. È inoltre possibile ottenere un'autenticazione aggiuntiva associando il certificato a un *account* utente o di gruppo che disponga di privilegi per il controllo dell'accesso precedentemente stabiliti. La *smart card* migliora il processo di autenticazione con chiave pubblica, poiché viene utilizzata come archivio protetto della chiave privata e come motore crittografico per l'esecuzione di una firma digitale o di uno scambio di chiavi.

Posta elettronica protetta

La posta elettronica protetta è una delle più interessanti applicazioni abilitate all'utilizzo della chiave pubblica, perché consente agli utenti di condividere informazioni in completa riservatezza e garantisce che l'integrità delle informazioni venga mantenuta durante il transito in *Internet*. Utilizzando *Microsoft Outlook Express* o *Microsoft Outlook*, è possibile selezionare un certificato con chiave pubblica emesso da un'autorità di certificazione attendibile, da utilizzare per firmare digitalmente e decifrare messaggi protetti. Pubblicando il certificato dell'utente in una *directory* pubblica dell'azienda o in *Internet*, altri utenti dell'azienda o di *Internet* possono inviare messaggi di posta elettronica crittografati all'utente e viceversa.

Le *smart card* aggiungono un ulteriore livello di integrità alle applicazioni di posta elettronica protetta poiché consentono di archiviare internamente la chiave privata e di proteggerla con un codice *PIN*. Per manomettere la chiave privata e inviare messaggi firmati assumendo l'identità di un'altra persona, è necessario appropriarsi della *smart card* e del relativo *PIN*.

Programmabilità delle *smart card*

Le *smart card* consentono di ospitare sistemi operativi come *Microsoft Windows for Smart Cards*, e in molti casi un tipo di *file system* nel quale è possibile archiviare dati. Per funzionalità quali l'accesso con *smart card* di *Windows* 2000, è necessario che la *smart card* sia programmabile, così da consentire le operazioni seguenti:

- Archiviazione di una coppia di chiavi utente.
- Archiviazione di un certificato con chiave pubblica associato.
- Recupero di un certificato con chiave pubblica.
- Operazioni con chiave privata complete per conto dell'utente.

Accesso interattivo con chiave pubblica

Un tipo di utilizzo delle *smartcard* particolarmente importante in *Windows* 2000 è quello relativo al *logon* a chiave pubblica. È possibile utilizzare il certificato contenuto nella *smartcard* per compiere il *logon* su un dominio *Windows* 2000, invece di utilizzare il normale procedimento di *logon* di NT.

Nel passato, l'accesso interattivo indicava la capacità di autenticare un utente in una rete utilizzando una forma di credenziale condivisa, ad esempio una *password* con *hash*. *Windows* 2000 supporta l'accesso interattivo con chiave pubblica utilizzando la versione 3 del certificato X.509 archiviato in una *smart card* con la chiave privata. Invece della *password*, l'utente digita un codice *PIN* per l'autenticazione GINA (*Graphical IdentificatioN and Authentication*). Tale codice autentica l'utente per la *smart card*.

Il certificato con chiave pubblica dell'utente viene recuperato dalla *smart card* mediante un processo protetto, ne viene verificata la validità e la provenienza da una fonte attendibile. Durante il processo di autenticazione, viene inviato alla *smart card* un messaggio di verifica (*challenge*) basato sulla chiave pubblica contenuta nel certificato. Questo messaggio verifica chi è il proprietario della *smart card* e la sua autorizzazione a utilizzare la chiave privata corrispondente.

Dopo la verifica della coppia di chiavi pubblica e privata, l'identità dell'utente contenuta nel certificato viene utilizzata per far riferimento all'oggetto utente archiviato in *Active Directory*, per elaborare un *token* e restituire al *client* il *ticket* TGT (*Ticket-Granting Ticket*). *Microsoft* ha integrato l'accesso con chiave pubblica nella versione 5 di *Kerberos*, che è compatibile con l'estensione per chiave pubblica specificata nella bozza RFC-1510 dell'organizzazione IETF.

schema di autenticazione tramite Smart Card

Quando la si inserisce nel lettore (1) collegato al *computer, Windows* 2000 chiede di inserire il codice *PIN* (*Personal Identification Number*) (2) nell'apposita finestra. Se il sistema operativo identifica l'utente quale proprietario della *card*, l'autorità LSA (*Local Security Authority*) del *computer* recupera il certificato dalla *smartcard* (3) e lo invia al centro KDC (4) (*Key Distribution Center*) *Kerberos*, il quale è un *controller* di dominio *Windows* 2000.

Dopo che quest'ultimo ha verificato la validità del certificato (5) e di chi lo ha rilasciato (per esempio, dell'autorità CA), il nome del soggetto presente del certificato viene utilizzato quale riferimento per compiere la ricerca di un *user object* (6) in AD. Quando il centro KCD trova

l'oggetto, viene creato un *ticket* TGT (7) (*Ticket-Granting Ticket*) *Kerberos* che contiene l'*account* dell'utente e le informazioni per il controllo dell'accesso. Il centro KDC crittografa il *ticket* TGT utilizzando una chiave di sessione (che viene successivamente crittografata con la chiave pubblica dell'utente) e lo restituisce al *computer* (8).

(9) La *smartcard* decodifica quindi la chiave di sessione utilizzando quella privata che è contenuta dalla *smartcard* stessa, e utilizza la prima per decodificare il *ticket* TGT. Il centro KDC consente infine all'autorità LSA di autorizzare il *logon* dell'utente sul dominio *Windows* 2000.

Oltre al *logon* tramite *smartcard*, è possibile utilizzare questo servizio di *Windows* 2000 anche per altre operazioni PKI, come l'autenticazione *client* e *server* nel protocollo SSL (*Secure Sockets Layer*). Per sfruttare completamente le possibilità offerte dalla *smartcard*, si possono integrare anche altre funzioni di sicurezza oltre al certificato digitale, per esempio le informazioni identificative dell'azienda e l'autorizzazione Bancomat.

Configurare le Smart Card

Prima di poter utilizzare le *Smart Card*, occorre l'infrastruttura PKI fornita da *Windows* 2000 con *Certificate Server* e *Active Directory*. È disponibile un gran numero di opzioni relative all'impostazione dell'infrastruttura PKI, a seconda che si ospiti una propria *authority* CA (*Certification Authority*), la si assegni in *outsourcing* a un *provider* come *VeriSign*, oppure si faccia uso di uno schema intermedio.

Questo scenario prevede l'uso di un *computer* che funge da *controller* di dominio *Active Directory*, di *Certificate Server* installato su un'*authority* CA radice dell'azienda e di un lettore di *Smart Card*. L'*authority* CA radice (CA *Root*) è la più alta in assoluto nella gerarchia della fiducia. La presenza di un'*authority* CA dell'azienda implica che il *server* di certificati userà *Active Directory* quale proprio *data store* e in conseguenza metterà a disposizione una serie di funzioni per la gestione dei certificati. Le *authority* CA indipendenti, che utilizzano un *database* locale invece di *Active Directory*, vengono usate di solito dai *server Web* pubblici per fornire i certificati agli utenti di *Internet*.

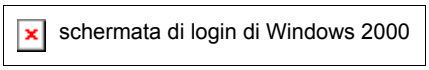
Dopo avere installato *Windows* 2000 quale *controller* di dominio che usa lo schema DNS (*Domain Name System*) e il *server Microsoft* IIS (*Internet Information Server*), occorre installare anche *Certificate Server*.

Porsi in corrispondenza della *applet Add/Remove Windows Components* nel Pannello di Controllo, quindi selezionare *Certificate Services*. Installare *Certificate Server* quale *authority* CA aziendale radice. Dopo avere specificato il nome, si possono usare i valori di *default* in tutte le successive finestre di dialogo. Si dovrà quindi definire quali tipi di certificati possono essere emessi dalla nuova *authority* CA. Si possono usare i certificati per vari scopi, tra cui quello di convalidare i *server Web*, crittografare i *file* con il sistema EFS (*Encrypting File System*) e rendere sicura la posta elettronica. I modelli dei certificati, che sono una funzionalità di gestione delle *authority* CA aziendali, permettono di definire i possibili usi di un particolare certificato.

Tra i modelli è necessario senz'altro il modello *Smartcard Logon* (si accede a questi modelli tramite lo *snap-in Certificate Authority* della *consolle* MMCche risulta disponibile dopo la configurazione di *Certificate Server*). Come suggerisce il nome, i certificati *Smartcard Logon* sono limitati al *logon*; i certificati *Smartcard User* permettono invece di usare una *Smart Card* per compiere il *logon* e per firmare la posta elettronica. Occorre inoltre aggiungere il modello *Enrollment Agent*, che si rende necessario per creare nuovi certificati. A questo punto, si ha a disposizione un'infrastruttura PKI in grado di autenticare gli utenti attraverso le *Smart Card*.

Configurare l'hardware

La fase successiva è quella di installare, ad esempio, il lettore di *Smart Card* GCR410; questa installazione è semplice grazie al *Plug and Play*. Spegnere il sistema, quindi collegare al *computer* i due cavi del lettore. Il cavo PS/2 utilizza un connettore a cuneo, che si inserisce tra la porta PS/2 e il cavo della tastiera o del *mouse*. Il lettore viene alimentato dalla porta PS/2. Il cavo seriale, che deve essere collegato a una porta seriale di riserva, permette di instaurare le comunicazioni tra il sistema e il lettore. Quando si avvia il *computer, Windows* 2000 rileva automaticamente la presenza del nuovo lettore.


schermata di login di Windows 2000

Dal momento che l'implementazione delle *Smart Card* è una funzione amministrativa particolarmente delicata, proprio come l'assegnazione dei valori di *ID* utente e *password*, questa capacità dovrebbe essere limitata a utenti e *workstation* specifiche. In conseguenza, la fase successiva è quella di trasformare un *computer* in una *workstation* per il rilascio dei certificati *Smart Card*. Per prima cosa, richiedere un certificato *Enrollment Agent* per l'amministratore che dovrà rilasciare le *Smart Card* agli utenti. Quando l'amministratore richiede i certificati *Smart Card* per i nuovi utenti, *Windows* 2000 firma la richiesta con questo certificato *Enrollment Agent*. Successivamente aprire lo *snap-in* MMC *Certificates*, che permette di gestire i certificati associati al proprio *account* utente e di richiederne di nuovi. Richiedere infine un nuovo certificato *Enrollment Agent*, fornire un nome amichevole e fare clic con il *mouse* sul pulsante *Install*.

Le fasi precedenti sono necessarie soltanto per la configurazione iniziale. Quelle successive dovranno invece essere ripetute per ciascun utente che deve utilizzare una *Smart Card* (in questo esempio che prevede soltanto un *computer*, l'utente avrà bisogno del diritto di compiere il *logon* localmente su questo *server*, essendo per esempio un membro del gruppo *Server Operators*).

È ora possibile richiedere i certificati *Smart Card* per conto di altri utenti. Selezionare un *account* utente già esistente, oppure crearne uno nuovo. Aprire *Microsoft Internet Explorer* e digitare il nome del proprio *server* di *authority* CA (per esempio, b1) seguito da /CertSrv, ad esempio http://b1/CertSrv.

Accesso interattivo con chiave pubblica

Richiedere un certificato, quindi specificare una richiesta avanzata nella schermata successiva. In corrispondenza di quest'ultima, selezionare *Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station* (Richiedere un certificato per una *Smart Card* per conto di un altro utente, usando la *Smart Card Enrollment Station*).

Selezionare il *Certificate Template* (per esempio, *Smartcard User o Smartcard Logon*); è inoltre possibile specificare quale *authority* CA utilizzare, anche se il valore di *default* per questo campo è relativo all'*authority* CA che è stata installata. Si può specificare il *provider* CSP (*Cryptographic Service Provider*) che deve essere utilizzato con questo certificato. Il *provider* CSP fornisce al sistema operativo e alle applicazioni alcuni servizi crittografici di base; quelli specifici alle *Smart Card* utilizzano la scheda per soddisfare le richieste relative ai servizi che prevedono l'uso della chiave privata.

È inoltre possibile specificare il certificato *Enrollment Agent* che dovrà firmare questa richiesta. Utilizzare il certificato *Enrollment Agent* creato in precedenza. È infine necessario specificare l'utente per conto del quale si sta richiedendo il certificato, quindi fare clic con il *mouse* in corrispondenza del pulsante *Enroll*. Il sistema chiederà di inserire la *Smart Card* nel lettore e di digitare il relativo codice *PIN*. A questo punto, *Certificate Server* visualizza una pagina nel *browser*, informando che l'operazione è stata compiuta con successo. È ora possibile visualizzare il

certificato sulla *Smart Card*, oppure passare a un altro utente.

A questo punto, si è pronti per compiere il *logon* usando la *Smart Card*. Per prima cosa, scollegarsi dal sistema e re-inserire la scheda. Il lettore notifica al sistema che è stata inserita la scheda, quindi viene chiesto di digitare il codice *PIN*. Dopo averlo digitato, questa parte del *logon* è completa. *Windows* 2000 invia il codice *PIN* alla *Smart Card* per l'autenticazione.

Successivamente, il codice viene usato per compiere alcune funzioni crittografiche richieste da *Windows* 2000 (per esempio, il sistema operativo potrebbe chiedere alla *Smart Card* di firmare una richiesta di *logon*).

Microsoft utilizza una proposta della IETF (*Internet Engineering Task Force*) chiamata PKINIT, per estendere il protocollo di autenticazione *Kerberos* versione 5 in modo da supportare anche l'autenticazione a chiave privata e pubblica, oltre al metodo a chiave simmetrica e segreto condiviso già usato da questo protocollo.

In conseguenza, la *workstation* invia la richiesta di *logon* a un *controller* di dominio, tramite una richiesta AS (*Authentication Services*) *Kerberos*. Il centro KDC (*Key Distribution Center*) *Kerberos* sul *controller* di dominio verifica la richiesta usando la chiave pubblica del certificato, che viene pubblicata dall'*authority* CA. Se i dati sono corretti, *Kerberos* assegna un *ticket* e permette di compiere il *logon*. Se l'utente perde la *Smart Card*, è sufficiente aprire lo *snap-in* MMC *Certificate Services*, selezionare il certificato sotto *Issued Certificates*, revocarlo, pubblicare la lista CRL (*Certificate Revocation List*) aggiornata e fornire all'utente una nuova *Smart Card*. Se qualcuno dovesse cercare di usare la vecchia *Smart Card* ormai non più valida, *Windows* 2000 rifiuterebbe il *logon*.