

Ileano Bonfà

Servizio Sistemi Informativi



Provincia Autonoma di Trento
Azienda Provinciale per i Servizi Sanitari



Software Open Source in sanità

SPERIMENTAZIONI SULL'UTILIZZO E L'INTEROPERABILITA'
DELLA CARTA NAZIONALE DEI SERVIZI

2009-06-12

- Introduzione Generale
- La normativa sulle smart card
- Diffusione firma digitale operatori sanitari
- La firma digitale
- Linee guida CNIPA per l'interoperabilità
- Specifiche tecniche
- Applicazioni Open Source
- Procedure di test
- Conclusioni

Introduzione Generale

- La possibilità di fornire servizi di firma digitale, di accesso sicuro alle reti informatiche, pagamenti on-line, servizi sanitari, servizi anagrafici è strettamente collegata alla necessità di identificare il cittadino che ne usufruisce.
- Per consentire l'identificazione il progetto CNS ha prodotto la “Carta Nazionale dei Servizi”, una smart card che è in corso di distribuzione a professionisti sanitari e cittadini.



La normativa sulle smart card

- Regolamento concernente la diffusione della carta nazionale dei servizi (DPR n. 177, 2 Marzo 2004)
 - La carta nazionale dei servizi contiene un certificato di autenticazione, consistente nell'attestato elettronico che assicura l'autenticità delle informazioni necessarie per l'identificazione in rete del titolare della carta nazionale dei servizi, rilasciato da un certificatore accreditato.
 - La carta può contenere eventuali informazioni di carattere individuale generate, gestite e distribuite dalle pubbliche amministrazioni per attività amministrative e per l'erogazione dei servizi al cittadino, cui si può accedere tramite la carta, salvo si tratti di dati sensibili
 - La carta nazionale dei servizi ha la validità temporale determinata dall'amministrazione emittente, comunque non superiore a sei anni.
 - Tutte le pubbliche amministrazioni che erogano servizi in rete devono consentire l'accesso ai servizi medesimi da parte dei titolari della carta nazionale dei servizi indipendentemente dall'ente di emissione, che è responsabile del suo rilascio.

La normativa sulle smart card

- Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta nazionale dei servizi (Decreto 9 dicembre 2004 del Ministro dell'interno, del Ministro per l'innovazione e le tecnologie e del Ministro dell'economia e finanze)
 - Caratteristiche delle carte
 - fornisce la struttura dei dati contenuti sulla carte e le rispettive responsabilità
 - Circuito di emissione
 - Misure di sicurezza delle fasi di lavorazione della carta
 - Servizi erogabili
 - Firma digitale
 - Autenticazione
 - Pagamenti informatici
 - La carta sanitaria
 - Inizializzazione CNS a cura dei produttori
 - Caricamento Dati sanitari (Netlink)

Diffusione firma digitale operatori sanitari

- Con la deliberazione della Provincia Autonoma di Trento n. 1518 del 28/07/2006 viene approvato il progetto denominato “Diffusione firma digitale operatori sanitari” selezionato dal Dipartimento per l'Innovazione e le Tecnologie a seguito della manifestazione di interesse del 20 aprile 2005 emessa da parte della Provincia Autonoma di Trento nell'ambito del Tavolo di lavoro per la Sanità Elettronica.
- Sono oggetto dell'atto esecutivo i quantitativi di massima di seguito specificati:
 - circa **2.000** Carta Nazionale dei Servizi senza firma digitale con specifiche operative netlink
 - circa **1000** Carta Nazionale dei Servizi con firma digitale con specifiche operative netlink
- Le regioni che hanno distribuito le CNS ai propri cittadini sono:
 - - Lombardia (9,7 milioni)
 - - Sicilia (5 milioni)
 - - Friuli (1,2 milioni)
 - - Molise (110.000 pari a 1/3 dei cittadini)

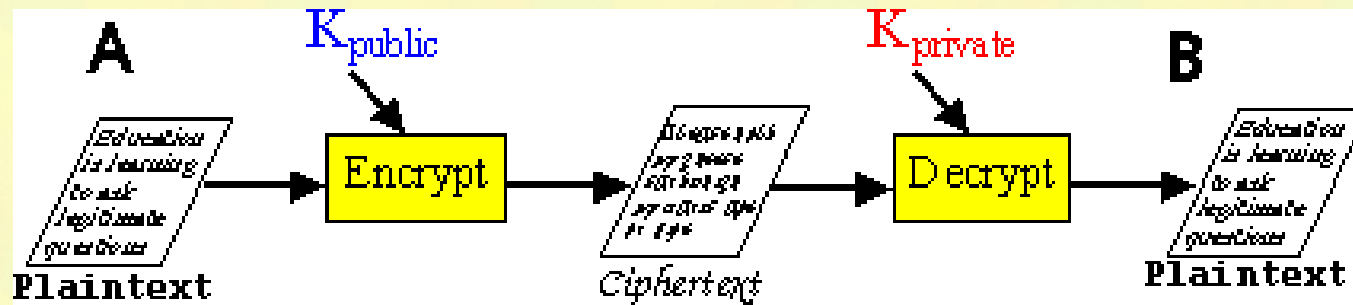
Diffusione firma digitale operatori sanitari

Sistemi Informativi aziendali interessati dal progetto Carta Operatore

- Sistema Informativo Ospedaliero SIO
- Sistema dipartimentale di laboratorio
- Sistema dipartimentale di radiologia
- Sistema Anatomia
- Gestione Documentale amministrativo gestionale
- Gestione referti Medicina Legale

La firma digitale: crittografia a chiave pubblica

- Ogni utente ha due chiavi, una pubblica ed una privata
- Quello che viene crittato da una chiave può solo essere decrittato dall'altra

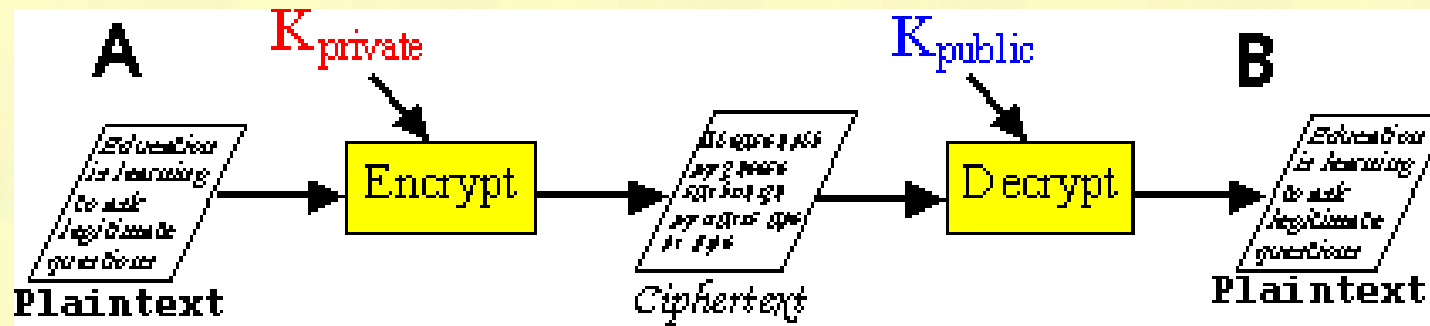


- Per rendere il messaggio leggibile solo da B, esso viene crittato con la chiave pubblica di B.

La firma digitale: certificati digitali

- Hanno lo scopo di collegare una chiave pubblica ad una organizzazione o persona specifica
- Un certificato è una struttura dati che contiene informazioni come:
 - Nome utente
 - Chiave pubblica utente
 - Nome della autorità di certificazione (AC) che emette il certificato
- il certificato è firmato digitalmente con la chiave privata dell'AC

- I ruoli delle chiavi vengono invertiti



- La chiave privata di A è usata per crittare ("firmare")
- La chiave pubblica di A è usata per decrittare ("verificare")

● Firma digitale

E' un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici

● Firma digitale “forte”

E' quella che il legislatore definisce firma digitale. Essa è basata su un sistema a chiavi crittografiche asimmetriche, utilizza un certificato digitale con particolari caratteristiche, rilasciato da un soggetto con specifiche capacità professionali garantite dallo Stato e viene creata mediante un dispositivo con elevate caratteristiche di sicurezza che in genere è una smart card.

● Firma digitale “debole” o “leggera”

L'altra tipologia di firma è la parte complementare. Tutto ciò che non risponde anche in minima parte a quanto appena descritto, ma è compatibile con la definizione giuridica di firma elettronica presentata nella tabella delle definizioni, è una firma “leggera”.

(*) dal doc. CNIPA “Linee guida per l'utilizzo della Firma Digitale”

La firma digitale: il formato p7m

- Il documento, una volta firmato, assumerà l'ulteriore estensione "P7M", in conformità alle regole CNIPA in materia di firma digitale
- Un file p7m (specifica PKCS#7 MIME) contiene:
 - Il documento originario
 - La firma digitale
 - Il certificato del soggetto che ha firmato
- Un file p7m può essere letto con programmi specifici, anche Open Source (p.es Javасign)

Verifying: Makefile.p7m

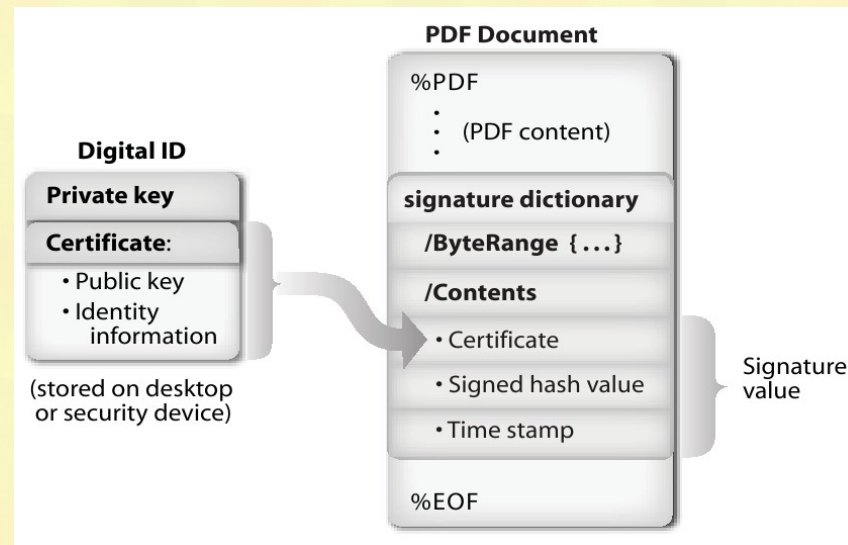
- Document verified
 - Certificate
 - Makefile

Field	Description
Issuer DN	C=IT,O=InfoCamere SCpA,SN=0231
Subject DN	C=IT,O=NON PRESENTE,SURNAME
Version	3
Start date	Mon Apr 24 11:45:10 CEST 2006
End date	Fri Apr 24 02:00:00 CEST 2009
Serial Number	824335
Signature algorithm	SHA1WithRSAEncryption
Signature OID	1.2.840.113549.1.1.5

Ok

La firma digitale: il formato pdf

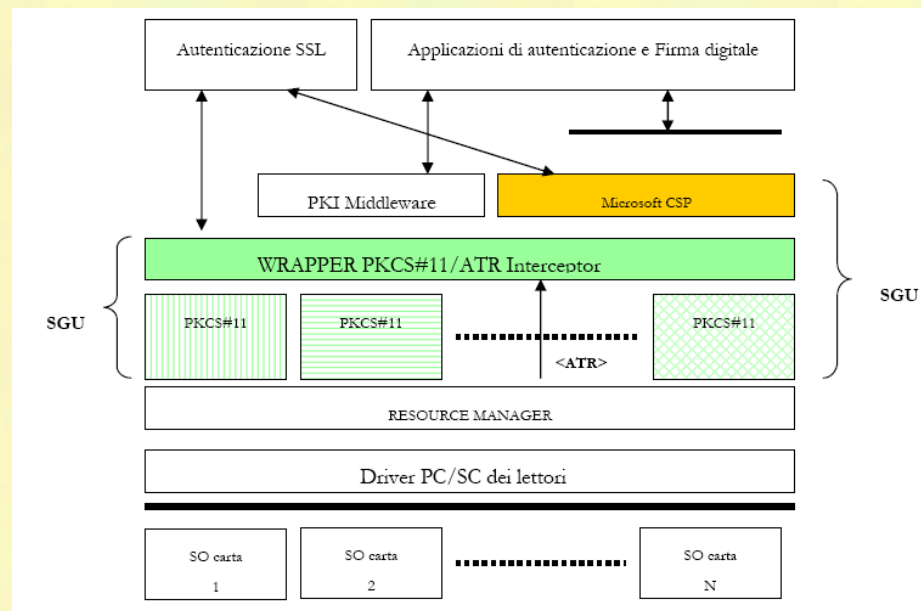
- In riferimento alla Deliberazione CNIPA n. 4/2005, il formato PDF è stato riconosciuto pienamente valido per la firma digitale ai sensi dell'Art. 12, comma 9, mediante la stipula di un Protocollo d'Intesa sottoscritto il 16 Febbraio 2006 dal CNIPA e da Adobe Systems Inc
- Il file PDF firmato può essere letto e la firma verificata p.es. con Adobe Reader 8.x, 9.x



Linee guida CNIPA per l'interoperabilità

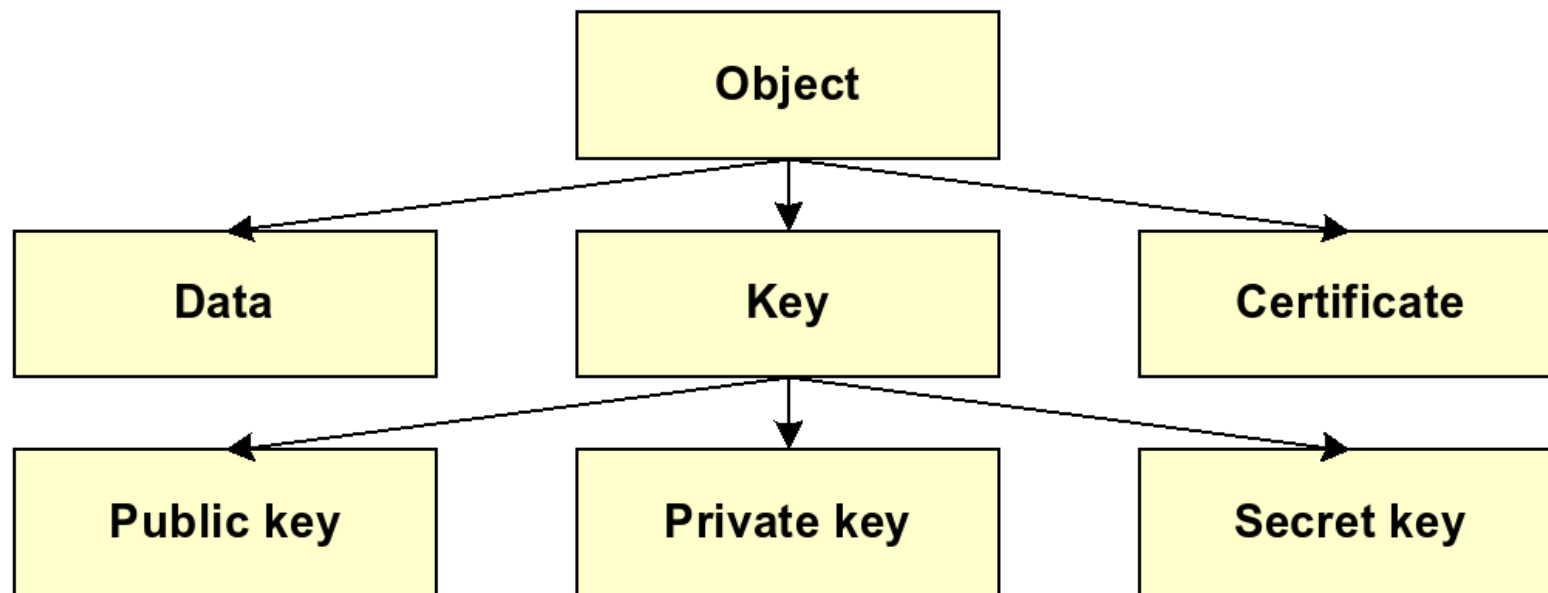
- Una richiesta di interoperabilità basata su dispositivi conformi alla norma ISO 7816
- Ogni carta viene fornita di una libreria PKCS#11 (a volte dette anche cryptoki) in grado di utilizzarne le caratteristiche di token crittografico (strato verde)

L'interoperabilità è garantita dagli strati Software di interfaccia, mostrati nella figura. Questi, che chiameremo Software di Gestione Unificata (SGU), consentono di utilizzare smart card di differenti fornitori senza vincoli restrittivi sul sistema operativo.



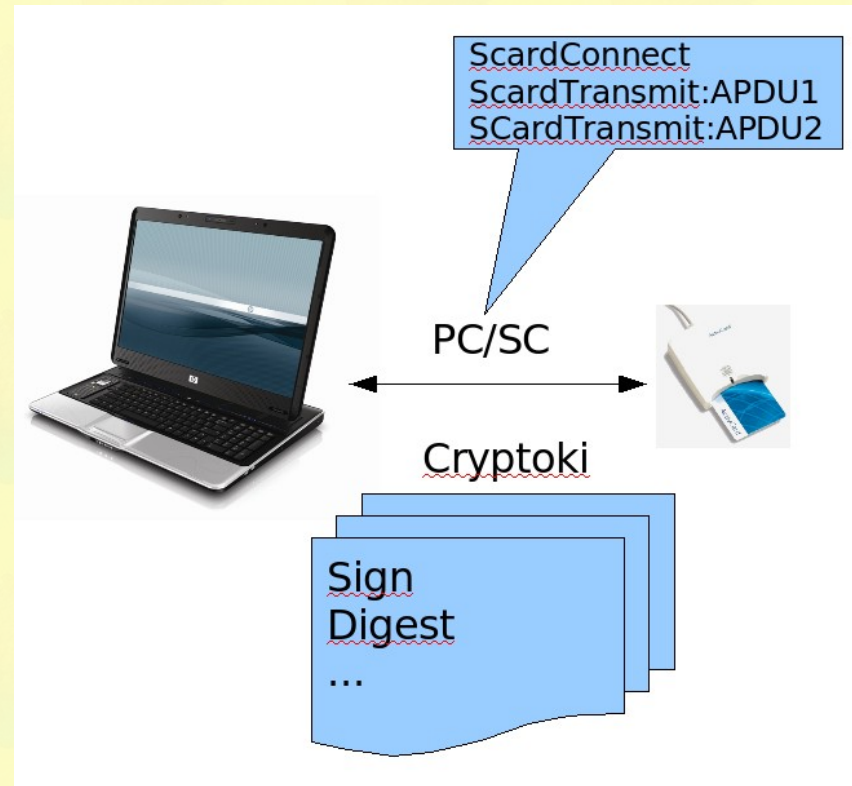
Linee guida CNIPA per l'interoperabilità

- La libreria cryptoki fornisce la rappresentazione a oggetti dei dati e delle quantità di sicurezza contenute nel dispositivo crittografico – Gli oggetti sono definiti dagli attributi (template)



Specifiche tecniche

- Le funzioni di firma e verifica è quindi opportuno che vengano accedute con cryptoki, mentre nel caso in cui la carta è usata come semplice contenitore di dati, sarà necessario ricorrere ai comandi conformi alla norma ISO 7816 effettuando chiamate APDU (application protocol data unit), p.es. per leggere file e dati.
- Il protocollo in ambiente Windows per accedere ad una smart card si chiama PC/SC.



■ Openssl (www.openssl.org)

OpenSSL è un'implementazione open source dei protocolli SSL e TLS. Le librerie di base (scritte in linguaggio C) eseguono le funzioni crittografiche principali. Nei diversi linguaggi di programmazione sono disponibili procedure che permettono di accedere alle funzioni della libreria OpenSSL.

E' disponibile per la maggior parte dei sistemi operativi unix-like, inclusi GNU/Linux e Mac OS X, ed anche per Microsoft Windows. OpenSSL è originariamente basato sulle librerie SSLeay di Eric Young e Tim Hudson.

■ Bouncycastle (www.bouncycastle.org)

Si tratta di un insieme di librerie crittografiche in java, che forniscono le seguenti funzionalità:

- a) Principali algoritmi di crittografia
- b) Gestioni certificati
- c) Gestione timestamp

- **Jaik (jce.iaik.tugraz.at)**

Fornisce le librerie java per l'interfacciamento con gli adattatori delle smart card ed implementa le funzioni cryptoki precedentemente elencate. Utilizzando il PKCS #11 Wrapper è possibile utilizzare le caratteristiche di token crittografico della CNS.

- **Opensc (www.opensc.org)**

Opensc fornisce un insieme di librerie ed utilities per accedere a smart card. Implementa PKCS#11, rendendole disponibili ad applicazioni come Firefox e Thunderbird. Implementa lo standard PKCS#15.

- **Pcsclite (pcsclite.alioth.debian.org)**

Middleware per accedere ad una smart card utilizzando le api PC/SC, che rappresentano lo standard per l'interfacciamento di lettori in ambiente Microsoft.

- **Jaccal (jaccal.sourceforge.net)**

E' un insieme di API java per comunicare con le smart card, utilizzando PC/SC

■ Javasign (javasign.sourceforge.net)

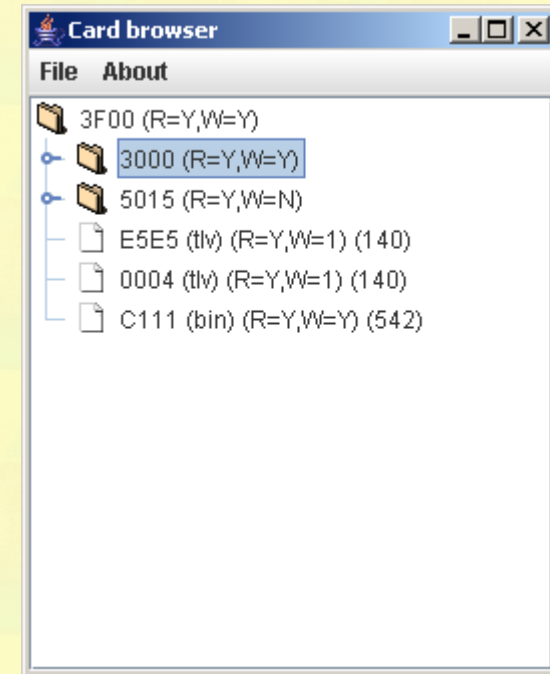
Si tratta di un programma Java, e quindi indipendente dallo specifico sistema operativo, che fornisce la gestione dell'identificazione e della firma digitale.

E' stato testato con le smart card CNS e di infocamere. E' stato integrato con il wrapper IAIK, per poter utilizzare virtualmente qualsiasi carta fornita di driver PKCS#11.

Riportiamo di seguito la struttura dei file di una smart card visualizzata per mezzo di javasign (confrontare con la figura precedente).

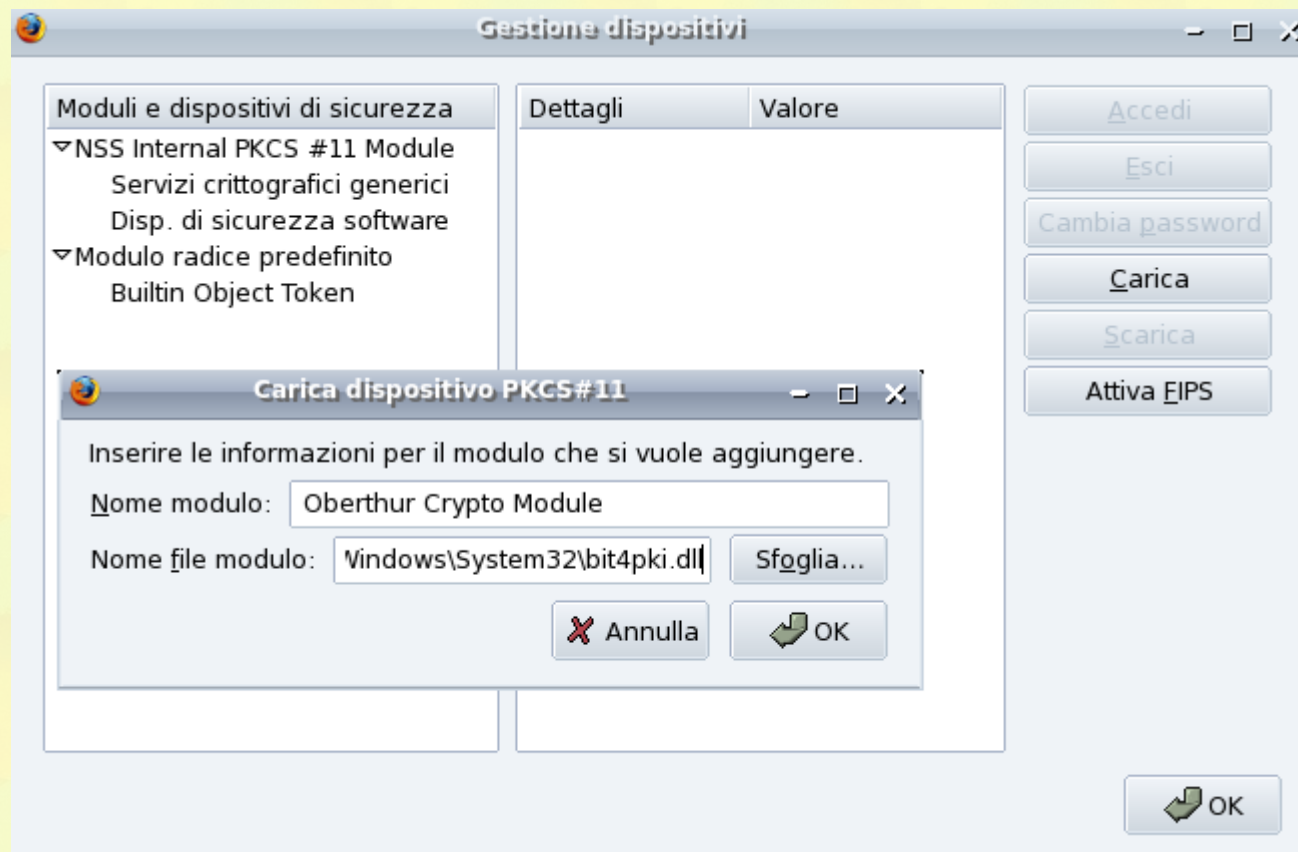
Per estrarre le informazioni in figura, Javasign implementa delle funzionalità di accesso alla carta di basso livello, per mezzo delle librerie Jaccal sopra citate.

Vengono in questo modo implementati comandi conformi alla norma ISO 7816 per la lettura della struttura del filesystem della carta.

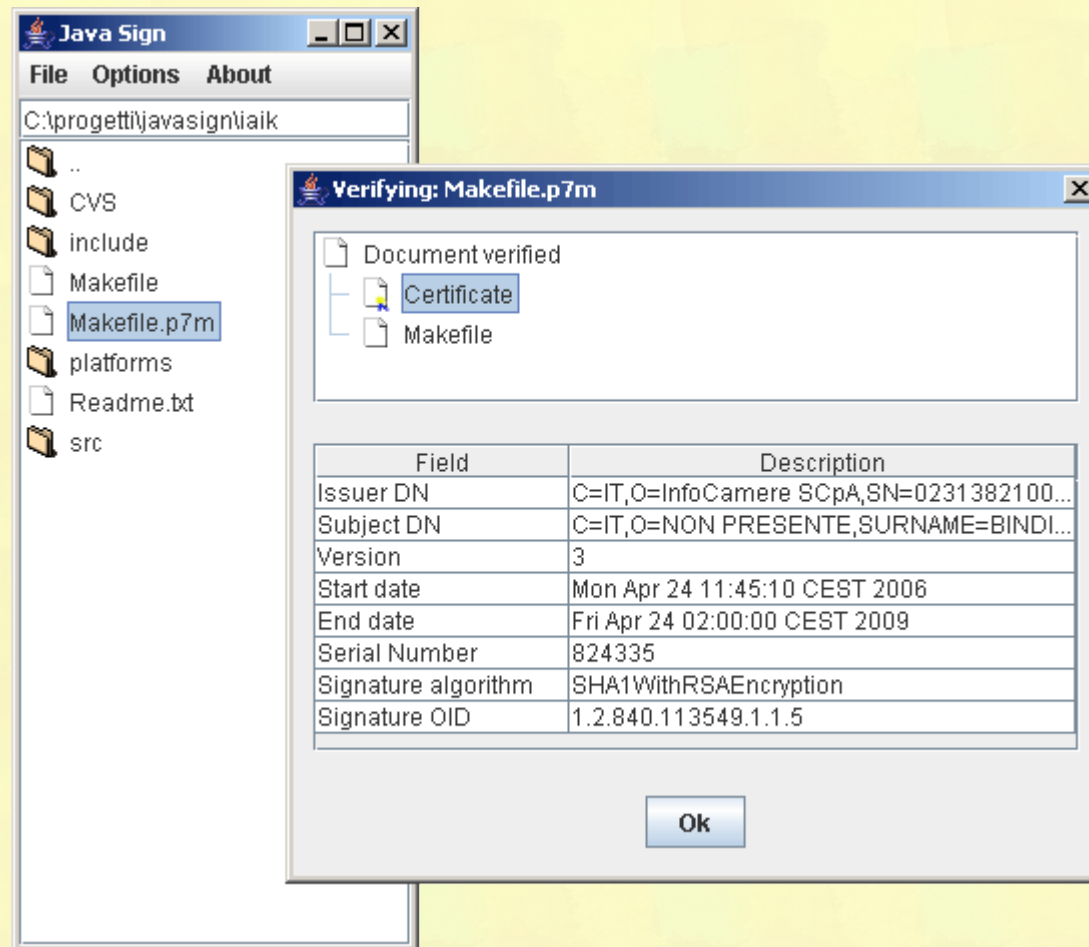


Procedure di test

- Configurazione di Internet Explorer, Firefox e Google Chrome per la consultazione della carta.



- Produzione della una firma digitale di un documento con Javaspign



- Un risultato particolarmente importante di questi test evidenzia la possibilità di utilizzare librerie ed applicazioni open source in ambiente java per i sistemi Informativi aziendali interessati dal progetto Carta Operatore senza essere vincolati a soluzioni proprietarie, che spesso richiedono anche una licenza per ogni posto di lavoro.