Smart Card HOWTO

Tolga KILIÇLI

tolga@deepnight.org

Questo documento fornisce informazioni riguardanti la tecnologia delle smart card e le sue applicazioni in ambiente Linux. Le smart card sono principalmente utilizzate in quelle situazioni in cui la sicurezza è in discussione, ma questa non è l'unica situazione in cui possono essere utilizzate: esse hanno molte proprietà che un fornitore di servizi può desiderare d'utilizzare, quale ad esempio "una scheda per molte applicazioni". Traduzione a cura di Manuele Rampazzo, <manu@linux.it>.

Sommario

1. Introduzione

Per varie ragioni, questa nuova versione ha il nome in codice *OberoN*.

Nuovi nomi in codice appariranno come da linee guida degli standard industriali per enfatizzare lo stato dell'arte di questo documento.

Questo documento è stato scritto quando un amico (JaSoN) mi chiese se potevo scrivere un documento riguardante le smart card e le relative applicazioni. E tutte queste pagine erano una volta un'accozzaglia di fogli. Grazie JaSoN...

1.1. Copyright Information

1.2. Informazioni sul copyright

1.3. Avvertenze per l'uso

Nessuna responsabilità sul contenuto di questo documento può essere accettata. Si usino concetti, esempi e altro contenuto a proprio rischio. Poiché questa è una nuova edizione del documento, possono esserci errori ed inesattezze che possono causare il danneggiamento del proprio sistema. Si proceda quindi con cautela e, sebbene ciò sia alquanto improbabile, l'autore non si assume alcuna responsabilità per ciò che può accadere.

Tutti i copyright sono detenuti dai rispettivi proprietari, tranne dove diversamente specificato. L'utilizzo di un termine in questo documento non deve essere considerato come un attentato alla validità di qualsiasi trademark o service mark.

Il nominare particolari prodotti o marchi non dev'essere considerato un favore che si fa ad essi.

È caldamente consigliato di effettuare un salvataggio del proprio sistema prima di un'installazione di rilievo e di farne altri ad intervalli regolari.

1.4. Nuove versioni

Questa è la prima versione.

L'ultima versione disponibile di questo documento può essere trovata nel mio sito (http://deepnight.org/smartcard/howto/).

1.5. Consigli e critiche

Si inviino aggiunte, commenti e critiche al seguente indirizzo di posta elettronica: <`tolga@deepnight.org`>.

1.6. Traduzioni

Non tutti parlano inglese, sono quindi apprezzati collegamenti a traduzioni. Inoltre, i traduttori tendono a dare suggerimenti molto importanti. Se si vuole tradurre questo documento nella propria lingua, me lo si comunichi affinché io possa indicarlo in questa sezione.

2. Cos'è una smart card?

La smart card, letteralmente "scheda (o carta) intelligente", è una piccola scheda di plastica, delle dimensioni di una carta di credito, con un microprocessore ed una memoria inclusi al suo interno. Nonostante la sua semplice, insignificante apparenza, ha molteplici usi ed un diffuso utilizzo in applicazioni che spaziano dalle schede telefoniche all'identificazione digitale degli individui.

Queste applicazioni possono essere: certificazione dell'identità del cliente, schede per biblioteche, e-wallet, chiavi per porte, ecc... e per tutte queste applicazioni può essere destinata una sola scheda. Le smart card detengono questi dati all'interno di file diversi e, come si leggerà, questi dati sono visibili ai programmi dipendentemente dal sistema operativo presente nella scheda. Questi file di dati sono collocati in un file system piuttosto simile alla struttura delle directory in Linux.

```
FP (File Principale)
         |
```

```
                    -------------+--------------
                    |            |             |
          FE (File Elementare)    FE   FD (File Dedicato)
                                               |
                                       ---------+--------
                                       |        |       |
                                       FE       FD      FE
                                                |
                                                FE
```

Il FP (File Principale) può essere considerato come la directory root in cui sono contenute le intestazioni dei file elementari e dedicati. I file dedicati sono simili alle normali directory e quelli elementari ai semplici file di dati. Il PIN è pure contenuto in un FE, ma solo la scheda ha il permesso d'accedere a quel file. Gli attributi dei file propri degli ambienti UNIX sono qui trasformati in condizioni d'accesso. Molte schede possono avere liste di condizioni d'accesso che devono essere soddisfatte prima di accedere ai dati.

Con un file system, condizioni d'accesso, un microcomputer, RAM, ROM, EEPROM, una smart card non è altro che un computer, con il proprio sistema operativo, in grado di stare dentro a un portafoglio.

3. Classificazione delle smart card

Per via delle diverse modalità di comunicazione col lettore e le differenti funzionalità incluse, le smart card sono classificate in modi differenti.

3.1. A contatto o senza contatto

Poiché le smart card hanno in esse inclusi dei processori, ne consegue che hanno bisogno di energia per funzionare e di alcuni meccanismi per comunicare, ricevere ed inviare i dati. Alcune smart card hanno placche dorate, ovvero degli insiemi di contatti, in un angolo della scheda. Questo tipo di smart card viene chiamato smart card *a contatto* (o *contact* smart card). Le placche sono utilizzate per fornire la necessaria energia e per comunicare attraverso contatti elettrici diretti con il lettore. Quando si inserisce la scheda nel lettore, i contatti di questo si appoggiano alle placche. In base agli standard ISO7816 le connessioni per il PIN sono le seguenti:

```
 ,----,             ,----,
 | C1 |             | C5 |          C1 : Vcc = 5V      C5 : Gnd
 '----'             '----'          C2 : Reset         C6 : Vpp
 ,----,             ,----,          C3 : Clock         C7 : I/O
 | C2 |             | C6 |          C4 : RFU           C8 : RFU
 '----'             '----'
 ,----,             ,----,
 | C3 |             | C7 |
 '----'             '----'
 ,----,             ,----,
 | C4 |             | C8 |
 '----'             '----'
```

- I/O : input o output per dati seriali verso i circuiti integrati presenti nella scheda.
- Vpp : input di tensione programmabile (d'utilizzo opzionale per la scheda).
- Gnd : messa a terra (in riferimento alla tensione).
- CLK : segnali di temporizzazione o frequenza (d'utilizzo opzionale per la scheda).
- RST : utilizzato a seconda dei casi da se stesso (per segnali di reset forniti al dispositivo d'interfacciamento) oppure in combinazione con un circuito interno di controllo del reset (di utilizzo opzionale per la scheda). Se il reset interno è implementato, la fornitura di tensione su Vcc è obbligatoria.
- Vcc : input per la fornitura di tensione (d'utilizzo opzionale per la scheda).

I lettori per le smart card a contatto sono di solito dispositivi separati da collegare alla porta seriale od USB. Esistono tastiere, PC e PDA con inclusi lettori simili a quelli dei telefoni cellulari GSM, anche per mini smart card in stile GSM.

Alcune smart card non hanno connettori sulla propria superficie. La connessione tra il lettore e la scheda viene quindi effettuata via radiofrequenza (RF). Le schede contengono una piccola spira di filo conduttore che viene utilizzata come induttore per fornire energia alla scheda e per comunicare col lettore. Quando la scheda entra nel campo in RF del lettore, una corrente indotta si crea nella spira e viene quindi utilizzata come una sorgente d'energia. Grazie alla modulazione del campo in RF del lettore ed alla corrente indotta nella scheda, la comunicazione ha luogo.

I lettori di smart card di solito si collegano al computer per mezzo della porta seriale od USB. Quando le schede senza contatto (o contactless) non devono essere inserite nel lettore, di solito questo è composto solo da un'interfaccia seriale per il computer e da un'antenna per collegarsi alla scheda. I lettori per smart card senza contatto possono avere o meno un'alloggiamento: la ragione è che alcune smart card possono essere lette fino a 1,5 metri di distanza dal lettore, mentre altre devono essere posizionate a pochi millimetri da esso per poter essere lette con accuratezza.

Esiste un ulteriore tipo di smart card, le schede combinate. Una scheda combinata ha un blocco di contatti per la transazione di dati voluminosi, ad esempio le credenziali PKI, ed una spira in filo per la reciproca autenticazione. Le smart card a contatto vengono utilizzate soprattutto per la sicurezza elettronica, mentre quelle senza contatto vengono utilizzate nei trasporti e/o per l'apertura delle porte.

3.2. Memoria o microprocessore

Le smart card più diffuse e meno costose sono schede a memoria. Questo tipo di smart card contiene una memoria permanente EEPROM (Electrically Erasable Programmable Read-Only Memory). Poiché questa è permanente, quando si rimuove la scheda dal lettore e l'energia viene interrotta la scheda salva i dati. Si può immaginare la struttura di una EEPROM come un normale dispositivo d'immagazzinamento dei dati dotato di file system e gestito con un microcontrollore (di solito ad 8 bit). Questo microcontrollore è responsabile dell'accesso ai file e per -????- l'instaurazione della comunicazione. I dati possono essere bloccati con un PIN (Personal Identification Number), la propria parola chiave. I PIN sono normalmente composti da 3 ad 8 numeri che vengono scritti in un file speciale presente nella scheda. Poiché questo tipo di scheda non consente la crittografia, le schede a memoria vengono utilizzate per contenere credito telefonico, biglietti per il trasporto o denaro elettronico.

Le schede a microprocessore assomigliano molto ai computer che utilizziamo sulla nostre scrivanie. Hanno RAM, ROM e EEPROM con un microprocessore a 8 o 16 bit. Contenuto nella ROM c'è un sistema operativo per gestire il file system presente nella EEPROM e per eseguire le desiderate funzioni nella RAM.

____

```
              | microprocessore |
 Lettore <===|  a 8 o 16 bit   |-----+
              -----------------      |
                                     |
                                     |---> RAM
                   SCHEDA            |
             NON CRITTOGRAFICA       |---> ROM
                                     |
                                     +---> EEPROM
```

Come si vede dallo schema qui sopra, tutte le comunicazioni sono effettuate attraverso il microprocessore. Non c'è connessione diretta tra la memoria ed i contatti. Il sistema operativo è responsabile della sicurezza dei dati presenti in memoria perché è lui a controllare le condizioni d'accesso.

```
              -----------------             --------
              | microprocessore |           | Critto |
 Lettore <===|  a 8 o 16 bit   |-----------| Modulo |
              -----------------     |        --------
                                    |
                                    |---> RAM
                   SCHEDA           |
               CRITTOGRAFICA        |---> ROM
                                    |
                                    +---> EEPROM
```

Con l'aggiunta di un crittomodulo, la nostra smart card può ora gestire i complessi calcoli matematici relativi al PKI. Poiché la frequenza interna dei microcontrolli è compresa tra 3 e 5 MHz, si ha la necessità di aggiungere un componente che acceleri le funzioni crittografiche. Le schede crittografiche sono più costose di quelle non crittografiche, così come le schede a microprocessore lo sono più di quelle a memoria.

La scelta della scheda corretta dipende dalle proprie applicazioni.

4. Sistemi operativi

La nuova moda nei sistemi operativi per smart card è il JavaCard Operating System. Il JavaCard OS è stato sviluppato da Sun Microsystem e quindi promosso al JavaCard Forum. Il JavaCard OS è popolare poiché rendere indipendenti i programmatori rispetto all'architettura e applicazioni pensate per il JavaCard OS possono essere utilizzate da qualsiasi produttore di smart card che supportino JavaCard OS.

La maggior parte delle smart card usano oggi i loro specifici OS per le sottostanti comunicazioni e funzioni. Per poter dare un reale supporto alle applicazioni i sistemi operativi per smart card vanno ben oltre le semplici funzioni indicate dagli standard ISO7816. Conseguenza di ciò è che il porting delle applicazioni sviluppate per un produttore verso un altro produttore di smart card diventa un lavoro particolarmente complesso. Un altro vantaggio del JavaCard OS è che permette il concetto del caricamento posticipato delle applicazioni. Ciò permette di aggiornare le applicazioni delle smart card dopo la consegna della scheda all'utente finale. L'importanza sta nel fatto che l'utilizzo di una smart card è legato all'esecuzione di un'applicazione specifica, necessità che però successivamente può cambiare e rendere necessaria l'esecuzione di un maggior numero di applicazioni.

Un altro sistema operativo per smart card è MULTOS (Multi-application Operating System). Come il nome stesso suggerisce, MULTOS può anch'egli supportare più applicazioni. MULTOS è tuttavia stato disegnato specificatamente per necessità d'elevata sicurezza ed in molte nazioni ha conseguito la certificazion "ITSec E6 High".

Anche Microsoft sta interessandosi alle smart card con Smart Card for Windows.

I citati sistemi operativi possono essere quindi considerati come API dal lato scheda per sviluppare cardlets o piccoli programmi in grado d'essere eseguiti sulla scheda. Esistono inoltre API dal lato lettore come OpenCard Framework e GlobalPlatform.

5. Programmazione

5.1. CT-API

Questa API dipende dal terminale per schede utilizzato, ma fornisce funzioni generiche che consentono la comunicazione con schede a memoria e a processore. Questa API è un'interfaccia di basso livello verso il lettore, ma viene ancora utilizzata perché rispetta gli standard ISO7816 ed ha una semplice logica di programmazione simile a una catena di montaggio. Si devono semplicemente inviare dei messaggi in codice insieme ai pacchetti di dati ed attendere la risposta.

5.2. PC/SC

Il gruppo di lavoro PC/SC è responsabile dello sviluppo delle specifiche PC/SC. Esistono API corrispondenti per gli ambienti Windows, MacOS e Linux. Il pacchetto pcsc-lite per Linux può essere scaricato da http://www.linuxnet.com.

5.3. OpenCard

L'OpenCard Framework, OCF, è un ambiente di lavoro orientato agli oggetti per comunicazioni via smart card. OCF utilizza l'interoperabilità Java tra ambienti diversi per sviluppare architetture ed API per sviluppatori d'applicazioni e fornitori di servizi.

5.4. GlobalPlatform

GlobalPlatform è nata nel 1999 su iniziativa d'organizzazioni interessate alle problematiche delle smart card per applicazioni multiple. Il principale obiettivo di GlobalPlatform è di definire le specifiche e l'infrastruttura per smart card multiapplicazioni.

5.5. Per riassumere

Come si può capire dalle sezioni precedenti, il periodo di standardizzazione delle smart card non è ancora concluso. La richiesta di smart card è in crescita da parte di utenti finali e sviluppatori. La mia opinione è che, se si è uno sviluppatore oppure ci si trova in un ruolo decisionale, si dovrebbero analizzare con attenzione tutti gli standard così come le aziende produttrici di smart card. Dal punto di vista di uno sviluppatore, ritengo che nell'immediato futuro

Java diverrà lo standard grazie alla sua portabilità e l'utilizzo multipiattaforma, nonostante la sua lentezza d'esecuzione e la rapida evoluzione.

6. Applicationi per Linux

In questa sezione si trovano applicazioni che utilizzano per qualche motivo smart card in ambiente Linux. Se si ha sviluppato un software in ambiente Linux, per favore me lo si comunichi, affinché lo possa aggiungere alla lista.

6.1. scas (http://crackinghacking.de/~henning/scas/)

SCAS è un semplice programma che confronta il codice presente nella nella scheda con quello presente nel computer. Si tratta di un ottimo esempio di una procedura d'autenticazione con schede a memoria.

6.2. smartcard (http://www.lionking.org/~kianga/software/smartcard/)

smartcard è un programma d'utilità per smart card in Linux che utilizza CT-API. Con smartcard si possono leggere o scrivere i dati in una smart card. Se l'accesso al lettore può essere effettuato via CT-API, smartcard può essere usato per controllare il lettore. Attualmente smartcard può funzionare solo con schede a memoria che utilizzano i protocolli I2C o 3W. Esiste inoltre un'interfaccia grafica sviluppata per GTK+/Gnome che supporta tutte le funzioni di smartcard.

6.3. ssh-smart (http://www.conostix.com/ssh-smart)

ssh-smart è una dimostrazione dei concetti fondamentali dell'identificazione ssh per smart card, come dichiarato dall'autore. ssh-smart utilizza il programma d'utilità smartcard per comunicare con la smart card. In sostanza, lo strumento ssh-smart-add (uno script perl) chiama ssh-keygen per generare la coppia di chiavi RSA, pubblica e privata; quindi colloca la chiave privata sulla scheda a memoria. Successivamente, lo strumento ssh-smart-addagent può essere utilizzato per estrarre dalla scheda la chiave privata da fornire ad ssh-agent.

6.4. smarttools-rsa (http://www.linuxnet.com)

Questo è un altro modulo PAM per i sistemi UNIX, ma supporta l'autenticazione RSA attraverso la propria chiave privata presente nella smart card. Per utilizzare questo strumento bisogna disporre d'una una scheda Schlumberger Cyberflex Access oppure una scheda Schlumberger Cryptoflex for Windows ed un lettore funzionante.

6.5. smartsign (http://smartsign.sourceforge.net)

Questo programma di utilità offre una quasi completa integrazione PKI con le smart card. Per utilizzarlo bisogna disporre di una OpenCA funzionante e possedere le smart card Schlumberger "Cyberflex Access 16K". Durante il processo di certificazione di OpenCA, la chiave privata ed il certificato pubblico possono essere collocati nella smart card e, successivamente, la chiave privata può essere utilizzata con Netscape per firmare le mail e le news in uscita. Inoltre, smartsign supporta l'autenticazione degli utenti locali grazie a un modulo PAM che utilizza un'autenticazione a chiave pubblica. Insieme a smartsign è fornito gpkcs11, un'implementazione PKCS#11, smastsh, una shell a linea di comando che permette la navigazione nel contenuto della smart card, sign_sc/verify_sc per firmare e verificare qualsiasi file con la smart card.

6.6. I Progetti CITI (http://www.citi.umich.edu/projects/smartcard/)

Presso il CITI, Center for Information Technology Integration dell'Università del Michigan, ci sono alcuni nuovi progetti. Ad esempio, Webcard è un webserver attivo su una scheda Java Schlumberger Cyberflex Access. Si distingue per uno stack TCP/IP ridotto che supporta solo HTTP. Il sistema è disegnato per avere un router che elabora i pacchetti IP secondo ISO7816 ed una Java Virtual Machine sulla scheda. Dettagliati riferimenti tecnici si possono vedere presso http://www.citi.umich.edu/projects/smartcard/webcard/citi-tr-99-3.html.

7. Il rapporto delle smart card con PKI

Come già sappiamo, le smart card sono luoghi sicuri su cui collocare dati sensibili, quali soldi ed identità personale. E se l'argomento è l'identità personale dobbiamo parlare di PKI, Public Key Infrastructure, e smart card.

Si immagini di lavorare in un'azienda con molte filiali e succursali. In queste grandi aziende gli impiegati hanno frequentemente permesso d'accedere in diversi luoghi fisici. Inoltre, si può accedere ai server aziendali per varie mansioni quali inviare posta elettronica, aggiornare le pagine web ed accedere ai database aziendali. Si pensi, una password per ogni server ed una chiave per ogni porta e dei soldi in portafoglio per acquistare cibo o bevande nel ristorante più vicino.

In realtà, si potrebbe utilizzare una smart card. Se s'utilizza una scheda a microprocessore ed il sistema operativo della scheda oppure le cardlet Java lo consentono, si potrebbe in effetti utilizzare un'unica scheda per tutto questo. Affinché questo scenario sia fattibile, l'azienda deve disporre di una propria CA, Certificate Authority. Lo schema seguente mostra una semplice struttura PKI, come descritto nell'RFC 2459.

```
+---+
|   |                      +---------------+
| D | <-------------------->| Entità finale |
| e |      Transazioni     +---------------+
| p |       operative           ^
| o |     e transazioni         |  Transazioni
| s |      gestionali           |  gestionali
| i |                           |              utenti PKI
| t |                           v
| o |      -------------------+--+-----------+----------------
|   |                         ^              ^
|   |                         |              | entità di
| C |                         v              |  gestione  PKI
| e |                        +------+        |
| r | <----------------------| RA   | <--+   |
| t | Pubblica il certificato +------+    |   |
|   |                                     |   |
| / |                                     |   |
|   |                                     v   v
| C |                              +------------+
| R | <----------------------------|     CA     |
| L |   Pubblica il certificato    +------------+
```

```
        |   |   Pubblica la CRL                 ^
        |   |                                   |
        +---+                    Transazioni    |
                                 gestionali     |
                                                v
                                             +------+
                                             |  CA  |
                                             +------+
```

- entità finale: utente dei certificati PKI e/o il sistema utente finale che è il soggetto del certificato;
- RA: registration authority, ovvero un sistema opzionale cui una CA delega certe funzioni gestionali; (in alcune implementazioni, dove tu registri te stesso nel sistema)
- CA: certification authority; (la propria chiave pubblica può essere resa pubblica quando ci si registra oppure può essere resa automaticamente pubblica, firmata e quindi il certificato pubblico viene consegnato dalla CA)
- deposito: un sistema o collezione di sistemi distribuiti che conserva i certificati e le CRL, Certificate Revocation Lists, e che è mezzo per la distribuzione di questi certificati e CRL alle entità finali.

In realtà, questa è solo una visione semplificata delle entità PKI. L'impiegato o l'entità finale si riferisce semplicemente alla CA od alla RA per ottenerne un certificato. Un certificato è solo una chiave pubblica digitalmente firmata con la chiave privata dell'ente rilasciante, la CA. Se firmato con la chiave privata della CA, tutti coloro che ripongono fiducia in essa danno automaticamente fiducia all'entità finale. La propria ID digitale è servita, bisogna solo scrivere la propria ID digitale e la chiave privata nella smart card, meglio ancora se s'utilizzano le nuove smart card, rilasciate con funzioni incluse che generano chiavi pubbliche e private all'interno della scheda, il che significa che la tua chiava privata non è esportata verso alcun luogo.

Le schede di nuova generazione sono in grado di utilizzare funzioni PKI che non richiedono d'esportare la chiave privata verso l'applicazione utilizzata. Ad esempio, quando si vuole mandare una mail firmata il programma di posta elettronica prima genera una hash del documento che si ha appena scritto e poi instaura la comunicazione con la scheda. L'applicazione quindi invia il valore dell'hash alla scheda, che provvede a firmare dentro se stessa tale valore con la chiave privata contenuta nella scheda medesima. In questo modo, la chiave privata non viene mai esportata verso l'ambiente pubblico, ovvero il computer.

Inoltre, quando si accede ad un proprio account remoto si può utilizzare un client ssh, la shell sicura. Un metodo di autenticazione per il protocollo ssh2 è descritto nella man page di OpenSSH. Il principale proposito di tal metodo è l'effettiva identificazione della persona che tenta d'accedere all'account e quindi l'instaurazione di una connessione tra gli host, qualora l'utente venisse accettato. In teoria, solo l'utente può conoscere la propria chiave privata. Sebbene la chiave privata sia leggibile solo dal proprietario, questo può essere un rischio di sicurezza, ma se la chiave privata viene memorizzata all'interno di una smart card si può ottenere una maggiore sicurezza. Naturalmente può capitare di perdere una smart card, ma a questo punto interviene un ulteriore argomento di sicurezza, il PIN. In generale, si può dire che la sicurezza delle smart card ha due origini, una che si sa ed una che si possiede.

SSH non è l'unica applicazione per cui si possono utilizzare le smart card. Transazioni monetarie in rete, autenticazione presso siti cui ci si connette ed altre applicazioni possono essere svolte grazie alle smart card. Il sistema è sempre più o meno lo stesso: l'identificazione viene verificata attraverso la chiave privata ed una sessione sicura viene avviata con le chiavi; a questo punto emergono specifiche e diverse componenti delle applicazioni, così come son state pensate e realizzate dal fornitore dell'applicazione. In alcuni casi le transazioni monetarie vengono effettuate all'interno della smart card, ma con altre applicazioni ad essa viene solo richiesto il numero di conto corrente bancario. Ci possono essere poi ulteriori metodologie.

È possibile trovare sul mercato serrature elettroniche che dialogano con una smart card. PKI può supportare, in aggiunta alla reciproca autenticazione di scheda e lettore, il conteggio degli accessi nello stabile. Si può utilizzare la semplice e reciproca autenticazione, oppure la serratura può effettuare una richiesta ad un server locale che contiene i dati degli utenti e verificare se all'utente è concesso di oltrepassare la porta e, sia che l'accesso sia concesso oppure rifiutato, il server tiene traccia dei tentativi d'accesso.

Man mano che l'integrazione delle smart card con il mondo PKI procederà, molte nuove applicazioni verranno create, soprattutto riguardanti vari aspetti della sicurezza oppure per semplificare la vita dell'utenza.

8. Ulteriori informazioni

In questa sezione sono elencati posti da visitare per informazioni più dettagliate.

8.1. Gruppi di discussione

Alcuni newsgroup sono:

- alt.technology.smartcards (news://alt.technology.smartcards)
- sci.crypt.research (news://sci.crypt.research)
- sci.crypt.random-numbers (news://sci.crypt.random-numbers)

8.2. Liste di discussione

Per il Progetto Muscle, `<sclinux@linuxnet.com>`, lista di discussione degli sviluppatori di smart card. L'argomento della lista è lo sviluppo di smart card negli ambienti Unix e MacOS. Per iscriversi, si invii una mail a `<majordomo@linuxnet.com>` con scritto subscribe linux nel corpo del messaggio. Si possono inoltre consultare gli archivi della lista presso The Mail Archive (http://www.mail-archive.com/sclinux@linuxnet.com/). Vai alla pagina della lista di discussione di linuxnet.com (http://www.linuxnet.com/list.html) per ulteriori informazioni.

8.3. Siti web

È disponibile una gran quantità di siti web con informazioni sulla smart card. Possono cambiare o non essere aggiornati.

Un buon inizio è il sito del Movement for the Use of Smart Cards in a Linux Environment (http://www.linuxnet.com), pieno di documentazioni, progetti e molto altro.

Inoltre, può interessare l'USENIX Workshop on Smartcard Technology (http://www.usenix.org/publications/library/proceedings/smartcard99/).

Se si conoscono altre guide interessanti, per favore me lo si comunichi.

9. TODO

Come tutti gli HOWTO dovrebbero fare, questo documento rimarrà in una costante fase di "lavori in corso" almeno finché la tecnologia delle smart card non diverrà obsoleta.

- La sezione riguardante le caratteristiche fisiche delle smart card dovrebbe essere riorganizzata.
- Nella sezione "Programmazione" dovrebbero esserci più informazioni relative agli standard di programmazione delle smart card.
- Dovrebbe essere aggiunta una nuova sezione con degli esempi.
- Dovrebbe essere aggiunta una sezione "Scenari" (ad esempio, come realizzare una PKI associativa) con informazioni approfondite. (Entro alcune settimane avrò un po' più tempo :))
- Ci potrebbe essere una sezione a proposito della resistenza delle smart card alle alterazioni, su com'è fornita questa resistenza e quanto son sicuro le smart card contro i nuovi giocatori high-tech. (Ho recuperato alcune informazioni e riferimenti, ma il tutto dev'essere riorganizzato prima d'essere aggiunto.)

Oibò, sembra che ci siano davvero tante cose da fare :))