

# Interoperabilità SISTRI

## Specifiche tecniche per l'utilizzo della firma elettronica con il Soft Token PKCS#11

Prot. N.: SISTRI-TN\_SIS-001

Versione: 1.0

Data: 28/09/2010





Specifiche tecniche per l'utilizzo della firma elettronica con il Soft Token PKCS#11  
Interoperabilità SISTRI

Prot. N.:	SISTRI-TN_SIS-001
Versione:	1.0
Data:	28/09/2010

#### STORIA DEL DOCUMENTO

VER.	DATA	DESCRIZIONE
1.0	28/09/2010	Prima Edizione

Specifiche tecniche per l'utilizzo della firma elettronica con il Soft Token PKCS#11  
Interoperabilità SISTRI

Prot. N.:	SISTRI-TN_SIS-001
Versione:	1.0
Data:	28/09/2010

## INDICE

<b>1</b>	<b>ARCHITETTURA .....</b>	<b>4</b>
1.1	DESCRIZIONE GENERALE .....	4
1.2	DIAGRAMMA DELL'ARCHITETTURA .....	4
1.3	CARATTERISTICHE FUNZIONALI .....	5
1.4	ARCHITETTURE HARDWARE/SOFTWARE SUPPORTATE .....	5
<b>2</b>	<b>CARATTERISTICHE SPECIFICHE DEL SOFTWARE .....</b>	<b>7</b>
2.1	PROFILO DI CONFORMITÀ STANDARD PKCS#11 .....	7
2.1.1	<i>Compatibilità .....</i>	7
2.1.2	<i>General-purpose functions .....</i>	8
2.1.3	<i>Slot and Token Management Functions .....</i>	8
2.1.4	<i>Session Management Functions .....</i>	8
2.1.5	<i>Object Management Functions .....</i>	9
2.1.6	<i>Encryption Functions .....</i>	9
2.1.7	<i>Decryption Funcions .....</i>	9
2.1.8	<i>Message Digest Functions .....</i>	10
2.1.9	<i>Signing Functions .....</i>	10
2.1.10	<i>Functions for Verifying Signatures .....</i>	10
2.1.11	<i>Key Management Functions .....</i>	10
2.1.12	<i>Random Number Generation Functions. ....</i>	10
2.2	COMPORTAMENTI SPECIFICI EXTRA STANDARD .....	10

Prot. N.:	SISTRI-TN_SIS-001
Versione:	1.0
Data:	28/09/2010

## 1 ARCHITETTURA

### 1.1 DESCRIZIONE GENERALE

Soft Token PKCS#11 è un modulo software parte del token SISTRI.

Nel contesto del token SISTRI, il modulo Soft Token PKCS#11 si occupa di veicolare le credenziali di firma digitale e autenticazione forte basate su PKI, offrendo uno “store” e una libreria per tali meccanismi, indipendente da specifici applicativi e sistemi operativi.

Soft Token PKCS#11 opera simulando le funzionalità di un token crittografico PKCS#11, nella fattispecie è totalmente equivalente ad una SmartCard di firma digitale.

### 1.2 DIAGRAMMA DELL'ARCHITETTURA

La figura seguente mostra nell'insieme i moduli del software crittografico, gli interfacciamenti fra i moduli sono realizzati tramite interfacce standard (PKCS#11) garantendo, di conseguenza, una possibile sostituzione dei moduli fronte di possibili evoluzioni tecnologiche.

### 1.3 CARATTERISTICHE FUNZIONALI

Soft Token PKCS#11 è in grado di operare come un dispositivo di firma digitale standard PKCS#11 riproducendo tutte le funzionalità di un token di firma digitale standard.

Le funzionalità sono implementate utilizzando le interfacce e le strutture dati descritte nella documentazione ufficiale di riferimento (<http://www.rsa.com/rsalabs/node.asp?id=2133>) nei profili funzionali “*RSA Asymmetric Client Signing Profile*” e “*RSA Asymmetric Acceleration Profile*”: oltre ai meccanismi di crittografia asimmetrica e firma digitale, sono anche implementate le funzioni necessarie a supportare le seguenti funzionalità di alto livello:

- Generazione di coppie di chiavi RSA (ad esempio finalizzata alla realizzazione da parte del client di procedure di enrollment secondo gli standard);
- Funzione di firma e di decifratura con chiave privata protetta da PIN (utile a proteggere file e documenti riservati);

**Specifiche tecniche per l'utilizzo della firma elettronica con il Soft Token PKCS#11**  
**Interoperabilità SISTRI**

<b>Prot. N.:</b>	SISTRI-TN_SIS-001
<b>Versione:</b>	1.0
<b>Data:</b>	28/09/2010

- Funzione di firma e di decifratura con chiave privata protetta da PIN (finalizzata all'autenticazione, ad esempio di tipo SSL, VPN, etc.);
- Funzioni di cifratura e decifratura con algoritmi DES, 3DES e AES.

Il software non richiede alcuna installazione nei sistemi sui quali opera né richiede all'utente di disporre dei privilegi di amministratore del sistema.

#### **1.4 ARCHITETTURE HARDWARE/SOFTWARE SUPPORTATE**

Nel token SISTRI, Soft Token PKCS#11 è disponibile in 3 distinte versioni, per altrettante piattaforme hardware/software:

- Microsoft Windows, versioni "XP", "Vista", "Seven (7)";
- Linux, compatibile con tutte le distribuzioni basate su kernel 2.6.x e processori compatibili IA32;
- Apple Mac OS X, nelle versioni 10.4.x, 10.5.x, 10.6.x su processori Intel.

Soft Token PKCS#11 è compilato a 32 bit: questo lo rende compatibile con applicazioni a 32 bit eseguite su sistemi operativi a 32 e 64 bit.

Il token può essere impiegato indifferentemente su tutti i sistemi operativi supportati, è anche possibile alternarne l'uso su computer differenti e sistemi operativi differenti senza che questo alteri in alcun modo le sue caratteristiche.

Le librerie da interfacciare possono essere ricercate all'interno dei seguenti percorsi:

Windows:

[unità-logica]:\sistri\DigitalID\SoftTokenEngine.dll

Linux :

[mount-point-chiavetta]/sistri/DigitalID/libSoftTokenEngine.so

MacOS X:



Specifiche tecniche per l'utilizzo della firma elettronica con il Soft Token PKCS#11  
Interoperabilità SISTRI

Prot. N.:	SISTRI-TN_SIS-001
Versione:	1.0
Data:	28/09/2010

[mount-point-chiavetta]/sistri/DigitalID/libSoftTokenEngine.dylib

DRAFT

<b>Prot. N.:</b>	SISTRI-TN_SIS-001
<b>Versione:</b>	1.0
<b>Data:</b>	28/09/2010

## 2 CARATTERISTICHE SPECIFICHE DEL SOFTWARE

Il P11\_Datastore implementa la crittografia ed esporta una interfaccia secondo lo standard PKCS#11.

Il modello presentato in questo paragrafo rappresenta il contesto applicativo di riferimento per la soluzione software per la parte client del TOKEN USB. Il modello è applicabile nel caso di utilizzo di una soluzione completamente software:

**FIGURA 1 :MODELLO ARCHITETTURA SOFTWARE SOFT TOKEN**

La figura esemplifica le due peculiarità maggiori del TOKEN Software:

1. Il token emula quindi una smart card per l'autenticazione al SISTRI e firma in rete. La gestione delle funzioni crittografiche è realizzata tramite l'interfaccia standard PKCS#11.
2. Il Token non richiede alcun driver kernel-mode o driver di lettore di smart card, questa caratteristica lo rende utilizzabile senza richiedere una installazione permanente nel sistema e accessibile anche dalle applicazioni impiegate da utenti privi di privilegi di amministrazione del sistema.

### 2.1 PROFILO DI CONFORMITÀ STANDARD PKCS#11

#### 2.1.1 COMPATIBILITÀ

Il prodotto espone le funzionalità più utilizzate dagli applicativi di firma digitale e cifratura, segue un elenco più dettagliato diviso per tipologia di funzione.

Per una descrizione più completa della funzione supportata viene descritta nel documento ufficiale RSA PKCS#11 v2.20: Cryptographic Token Interface Standard, <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf> il numero di pagina riferita a questo documento viene segnalato per ogni singola funzione.

#### 2.1.2 GENERAL-PURPOSE FUNCTIONS

**C\_Initialize** (pag. 102), la funzione è 100% compatibile. L'eventuale fallimento funzione è unicamente legato al tentativo di copiatura dei file di sistema del token.

Specifiche tecniche per l'utilizzo della firma elettronica con il Soft Token PKCS#11  
Interoperabilità SISTRI

Prot. N.:	SISTRI-TN_SIS-001
Versione:	1.0
Data:	28/09/2010

**C\_Finalize** (pag. 104).

**C\_GetFunctionList** (pag. 106).

**C\_GetInfo** (pag. 105).

### 2.1.3 SLOT AND TOKEN MANAGEMENT FUNCTIONS

**C\_GetSlotList** (pag. 106).

**C\_GetSlotInfo** (pag. 108).

**C\_GetTokenInfo** (pag. 109).

**C\_GetMechanismList** (pag. 111).

**C\_GetMechanismInfo** (pag. 109).

**C\_InitToken** (pag. 113)

**C\_InitPIN** (pag. 115).

**C\_SetPIN** (pag. 116).

### 2.1.4 SESSION MANAGEMENT FUNCTIONS

**C\_OpenSession** (pag. 117).

**C\_CloseSession** (pag. 118).

**C\_CloseAllSessions** (pag. 120).

**C\_GetSessionInfo** (pag. 120)

**C\_Login** (pag. 125)

**C\_Logout** (pag. 127)

### 2.1.5 OBJECT MANAGEMENT FUNCTIONS

**C\_CreateObject** (pag. 128), è possibile creare oggetti Certificato, Chiavi pubbliche e private e Secret keys.

**C\_DestroyObject** (pag. 131).

**C\_GetObjectSize** (pag. 132).

**C\_GetAttributeValue** (pag. 133), è possibile ottenere i seguenti attributi:



Specifiche tecniche per l'utilizzo della firma elettronica con il Soft Token PKCS#11  
Interoperabilità SISTRI

Prot. N.:	SISTRI-TN_SIS-001
Versione:	1.0
Data:	28/09/2010

CKA\_CLASS, CKA\_LABEL, CKA\_TOKEN, CKA\_PRIVATE, CKA\_ID, CKA\_SENSITIVE, CKA\_ENCRYPT, CKA\_DECRYPT, CKA\_WRAP, CKA\_UNWRAP, CKA\_SIGN, CKA\_VERIFY, CKA\_VALUE, CKA\_CERTIFICATE\_TYPE, CKA\_ISSUER, CKA\_SERIAL\_NUMBER, CKA\_SUBJECT, CKA\_START\_DATE, CKA\_END\_DATE, CKA\_KEY\_TYPE, CKA\_MODULUS, CKA\_MODULUS\_BITS, CKA\_PUBLIC\_EXPONENT, CKA\_PRIVATE\_EXPONENT, CKA\_NEVER\_EXTRACTABLE, CKA\_MODIFIABLE, CKA\_EXTRACTABLE, CKA\_LOCAL.

**C\_SetAttributeValue** (pag. 135) è possibile scrivere i seguenti attributi:

CKA\_LABEL, CKA\_ID, CKA\_SUBJECT.

**C\_FindObjectsInit** (pag. 136), è possibile cercare oggetti per i seguenti attributi:

CKA\_CLASS, CKA\_CERTIFICATE\_TYPE, CKA\_KEY\_TYPE, CKA\_LABEL, CKA\_SUBJECT, CKA\_ID, CKA\_VALUE.

**C\_FindObjects** (pag. 137).

**C\_FindObjectsFinal** (pag. 138).

#### 2.1.6 ENCRYPTION FUNCTIONS

**C\_EncryptInit** (pag. 139) supportati CKM\_AES\_ECB, CKM\_AES\_CBC, CKM\_DES3\_CBC\_PAD.

**C\_Encrypt** (pag. 140) supportati CKM\_AES\_ECB, CKM\_AES\_CBC, CKM\_DES3\_CBC\_PAD.

#### 2.1.7 DECRYPTION FUNCTIONS

**C\_DecryptInit** (pag. 144) supportati CKM\_AES\_ECB, CKM\_AES\_CBC, CKM\_DES3\_CBC\_PAD.

**C\_Decrypt** (pag. 145) supportati CKM\_AES\_ECB, CKM\_AES\_CBC, CKM\_DES3\_CBC\_PAD.

#### 2.1.8 MESSAGE DIGEST FUNCTIONS

**C\_DigestInit** (pag. 148) sono implementati i seguenti algoritmi: CK\_MD2, CKM\_MD5, CKM\_SHA1.

**C\_Digest** (pag. 148) sono implementati i seguenti algoritmi: CK\_MD2, CKM\_MD5, CKM\_SHA1.

**C\_DigestUpdate** (pag. 150) sono implementati i seguenti algoritmi: CK\_MD2, CKM\_MD5, CKM\_SHA1.

Specifiche tecniche per l'utilizzo della firma elettronica con il Soft Token PKCS#11  
Interoperabilità SISTRI

Prot. N.:	SISTRI-TN_SIS-001
Versione:	1.0
Data:	28/09/2010

**C\_DigestFinal** (pag. 151) sono implementati i seguenti algoritmi: CK\_MD2, CKM\_MD5, CKM\_SHA1.

#### **2.1.9 SIGNING FUNCTIONS**

**C\_SignInit** (pag. 157).

**C\_Sign** (pag. 158).

#### **2.1.10 FUNCTIONS FOR VERIFYING SIGNATURES**

**C\_VerifyInit** (pag. 157).

**C\_Veirfy** (pag. 158).

#### **2.1.11 KEY MANAGEMENT FUNCTIONS**

**C\_GenerateKey** (pag. 175), sono supportati: CKM\_AES\_KEY\_GEN, CKM\_DES3\_KEY\_GEN.

**C\_GenerateKeyPair** (pag. 176) supportato: CKM\_RSA\_PKCS\_KEY\_PAIR\_GEN.

#### **2.1.12 RANDOM NUMBER GENERATION FUNCTIONS.**

**C\_SeedRandom** (pag. 184).

**C\_GenerateRandom** (pag. 184).

### **2.2 COMPORTAMENTI SPECIFICI EXTRA STANDARD**

Il SoftToken implementa funzione di crittografia, e conservazione sicura di chiavi e dati multiutente.

Al fine di poter utilizzare un token da parte di molteplici persone fisiche il token implementa particolari funzioni crittografiche che provvedono a generare dei "p11\_datastore".

Non esistono funzioni a livello di libreria per selezionare l'utente per il quale svolgere le funzioni di firma cifra etc. Nel caso il token sia stato personalizzato in modalità multiutente la libreria provvederà a richiedere interattivamente all'utente stesso la propria USERID dopo la richiesta di passphrase.