SysGillo – CSP

Descrizione generale e

Piattaforma di collaudo

Document Version 1.0.0

Document Revision History

Version	Date	Subject	Issued by	Authorized by
1.0.0	Giu. 11, 2002	Edition	V. Palazzo	A. Scognamiglio

Sommario

Premessa

L'installazione del SW "*SysGillo CSP*" rende disponibile una piatta forma applicativa MW che consente l'integrazione delle funzionalità crittografiche basate su smartcard con i livelli SW applicativi su piattaforma Windows di Microsoft.

In particolare la libreria "*SysGillo CSP*", rappresenta l'implementazione delle API Microsoft CryptoSPI (Cryptographic System Program Interface). Per maggiori dettagli vedi: http://msdn.microsoft.com/library/default.asp? url=/library/en-us/security/security/cryptographic_service_providers.asp.

Tutte le funzioni di crittografia asimmetrica che coinvolgono l'uso della chiave privata sono implementate in hardware su Smart Card.

La compatibilità di *"SysGillo CSP"* con le funzioni Microsoft CryptoSPI, consente l'utilizzo della smart card come strumento crittografico in tutte quelle applicazioni che richiedono questo standard.

Di seguito sono riportate solo alcune delle molteplici applicazioni che hanno adottato lo standard CSP come proprio "protocollo" di colloquio con i dispositivi crittografici:

- Microsoft Internet Explorer (SSL client authentication)
- Microsoft Outlook Express (SMIME firma elettronica e crittografia di e-mail)
- Microsoft Outlook (SMIME firma elettronica e crittografia di e-mail)
- Microsoft Certification Authority

Tutti i software che si basano sulle API Microsoft per la crittografia possono essere usati con il *SysGillo CSP*, incrementandone così il livello di sicurezza grazie all'integrazione trasparente della smartcard in tutte le funzionalità che coinvolgono la crittografia asimmetrica.

Requisiti di sistema

"*SysGillo CSP*" supporta i seguenti Sistemi Operativi (SO):

- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows 98Me
- Microsoft Windows NT 4.0
- Microsoft Windows 2000
- Microsoft Windows XP

Piattaforma di riferimento e collaudo

La piattaforma di riferimento che sarà utilizzata anche in fase di collaudo delle presenti librerie è descritta di seguito:

- S.O.: Microsoft® Windows® 2000 Professional + Service Pack 2
- Microsoft® Smart Card Resource Manager (Scardsvr.exe) v5.00.2134.1
- Smart Card Reader: IPM miniLector RS232 ml31
- IPM miniLector RS232 Drivers v2.06
- Internet Explorer 5.5 con Crittografia a 128 bit

Note sull'installazione

SysGillo CSP è implementato mediante due librerie a collegamento dinamico (DLL): "*sysgillocsp.dll*" e "*ipmpki32.dll*". Al termine dell'installazione del pacchetto tali file saranno presenti nella cartella "%windows%\%SystemRoot%\" del sistema.

L'installazione provvede anche alla creazione della chiave di registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\ipmcsp32`

con i seguenti valori:

Name	Type	Data
(Default)	REG_SZ	(Value not set)
Image Path	REG_SZ	"%SystemRoot%\SYSTEM32\sysgillocsp.dll
Signature	REG_BINARY	e3 87 49 08 6b ec 82 c9 51 0c fe da 79 58 59 20 6d 00 a8 01 2f 40 43 b1 fc 65 56 88 eb a0 88 5c 80 19 4b c7 45 94 62 ad 15 df a7 2d f3 d4 81 6f 79 c1 50 2d 7d 3f 68 85 8a fd 7c 2f b4 d7 92 d0 0d a4 5b 40 54 d8 44 08 2a 60 36 68 bd 24 47 b4 33 9b e5 8a 80 04 e5 55 64 d0 98 26 a1 77 0c b6 b8 97 29 0e 46 91 98 0c dc 38 80 f8 a4 9a 1b 8d f8 3c fe a0 d3 4d 1e a3 d5 9e 9d 47 0f 1c 79 b1 00 00 00 00 00 00 00 00

Funzioni CryptoSPI (CryptoAPI) implementate

La tabella che segue riporta il dettaglio delle funzioni CSP supportate in “SysGillo CSP Interfaces”.

Function	Supported
CPAcquireContext	SI
CPReleaseContext	SI
CPGetProvParam	SI
CPSetProvParam	SI, con estensioni custom
CPDeriveKey	NO
CPDestroyKey	SI
CPDuplicateKey	NO
CPExportKey	SI
CPGenKey	SI
CPGenRandom	SI
CPGetKeyParam	SI
CPGetUserKey	SI
CPImportKey	SI
CPSetKeyParam	SI
CPDecrypt	SI
CPEncrypt	SI
CPCreateHash	SI
CPDestroyHash	SI
CPDuplicateHash	SI
CPGetHashParam	SI
CPHashData	SI
CPHashSessionKey	SI
CPSetHashParam	SI
CPSignHash	SI
CPVerifySignature	SI

Il “Provider Name” è “ipmcsp32”.