




SysGillo – PKCS#11

**Descrizione generale e
Piattaforma di collaudo**

Document Version 1.0.0

<i>SysGillo – PKCS#11</i>	INCARD S.p.A. eSecurity & Systems	11/06/2002		1/9
Ver. 1.0.0				

Document Revision History

Version	Date	Subject	Issued by	Authorized by
1.0.0	Giu. 11, 2002	Edition	L.Consiglio	A.Scognamiglio

<i>SysGillo – PKCS#11</i>	INCARD S.p.A. eSecurity & Systems	11/06/2002		2/9
Ver. 1.0.0				

Sommario

DOCUMENT REVISION HISTORY	2
SOMMARIO	3
PREMESSA.....	4
REQUISITI DI SISTEMA	5
NOTE SULL'INSTALLAZIONE	6
FUNZIONI PKCS#11 IMPLEMENTATE.....	7

<i>SysGillo – PKCS#11</i>	INCARD S.p.A. eSecurity & Systems	11/06/2002		3/9
Ver. 1.0.0				

Premessa

L'installazione del SW "SysGillo PKCS#11" rende disponibile una piattaforma applicativa MW che consente l'integrazione delle funzionalità crittografiche basate su smartcard con i livelli SW applicativi.

In particolare la libreria "SysGillo PKCS#11", rappresenta l'implementazione delle API standard descritte dalla specifica "PKCS#11 v2.1: Cryptographic Token Interface Standard" (<http://www.rsasecurity.com/rsalabs/PKCS/>).

Di seguito sono riportate solo alcune delle molteplici applicazioni che hanno adottato lo standard PKCS#11 come proprio "protocollo" di colloquio con i dispositivi crittografici:

- ?? Netscape Communicator (client authentication – SSL con l'utilizzo delle smart card, firma digitale e cifratura dei messaggi di posta utilizzando smart card)
- ?? Mozilla (client authentication – SSL con l'utilizzo delle smart card, firma digitale e cifratura dei messaggi di posta utilizzando smart card)
- ?? Baltimore UniCert (richiesta certificati)
- ?? SafeLayer KeyOne (richiesta certificati)
- ?? SecGo CryptoIP (realizzazione di VPN con accesso mediante smart card)

SysGillo – PKCS#11	INCARD S.p.A.	11/06/2002		4/9
Ver. 1.0.0	eSecurity & Systems			

Requisiti di sistema


“SysGillo PKCS#11” 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
- ?? Netscape® Communicator 4.74

<i>SysGillo – PKCS#11</i>	INCARD S.p.A. eSecurity & Systems	11/06/2002		5/9
Ver. 1.0.0				

Note sull'installazione


"SysGillo - PKCS#11" espone le funzioni in una libreria dinamica (dll) contenuta nel file "ipmpki32.dll". Al termine dell'installazione automatica, tale file .dll, sarà presente nella cartella "%Windows%\%SystemRoot%" del sistema.

SysGillo – PKCS#11	INCARD S.p.A. eSecurity & Systems	11/06/2002		6/9
Ver. 1.0.0				


Funzioni PKCS#11 implementate

La tabella che segue riporta il dettaglio delle funzioni PKCS#11 supportate in “SysGillo PKCS#11”.

Function	Supported
C_Initialize	SI
C_Finalize	SI
C_GetInfo	SI
C_GetFunctionList	SI
C_GetSlotList	SI
C_GetSlotInfo	SI
C_GetTokenInfo	SI
C_GetMechanismList	SI
C_GetMechanismInfo	SI
C_InitToken	NO
C_InitPIN	NO
C_SetPIN	SI
C_OpenSession	SI
C_CloseSession	SI
C_CloseAllSessions	SI
C_GetSessionInfo	SI
C_GetOperationState	NO
C_SetOperationState	NO
C_Login	SI
C_Logout	SI
C_CreateObject	SI
C_CopyObject	NO
C_DestroyObject	SI
C_GetObjectSize	SI
C_GetAttributeValue	SI
C_SetAttributeValue	SI
C_FindObjectsInit	SI
C_FindObjects	SI
C_FindObjectsFinal	SI
C_EncryptInit	SI
C_Encrypt	SI

SysGillo – PKCS#11	INCARD S.p.A. eSecurity & Systems	11/06/2002		7/9
Ver. 1.0.0				

C_EncryptUpdate	SI
C_EncryptFinal	SI
C_DecryptInit	SI
C_Decrypt	SI
C_DecryptUpdate	SI
C_DecryptFinal	SI
C_DigestInit	SI
C_Digest	SI
C_DigestUpdate	SI
C_DigestKey	SI
C_DigestFinal	SI
C_SignInit	SI
C_Sign	SI
C_SignUpdate	NO
C_SignFinal	NO
C_SignRecoverIni	NO
C_SignRecover	NO
C_VerifyInit	SI
C_Verify	SI
C_VerifyUpdate	NO
C_VerifyFinal	NO
C_VerifyRecoverInit	SI
C_VerifyRecover	SI
C_DigestEncryptUpdate	NO
C_DecryptDigestUpdate	NO
C_SignEncryptUpdate	NO
C_DecryptVerifyUpdate	NO
C_GenerateKey	SI
C_GenerateKeyPair	SI
C_WrapKey	SI
C_UnwrapKey	SI
C_DeriveKey	NO
C_SeedRandom	SI
C_GenerateRandom	SI
C_GetFunctionStatus	NO
C_CancelFunction	NO
C_WaitForSlotEvent	SI (solo con CKF_DONT_BLOCK)

<i>SysGillo – PKCS#11</i>	INCARD S.p.A. eSecurity & Systems	11/06/2002		9/9
Ver. 1.0.0				