API改版說明 - CSP 及PKCS#11

中華電信研究所
資通安全研究室

2008/10/20

大綱

- 準備工作
- 目的
- CSP新舊版本差異
- PKCS#11新舊版本差異
- 問題反應

準備工作

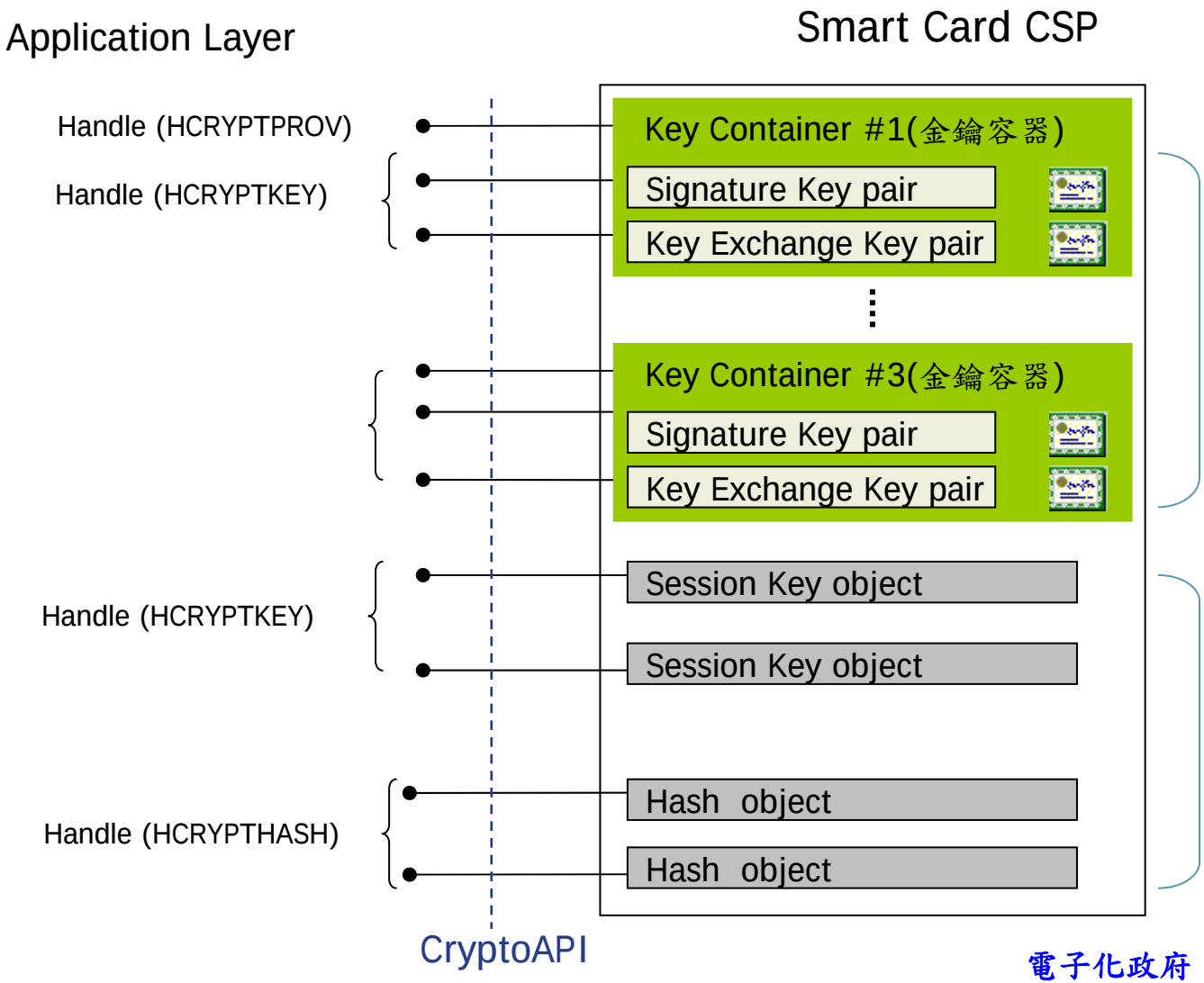
- 機關或廠商修改GPKI相關應用系統之準備工作
  - 取得2048 bits測試卡(本次說明會附贈2張)
    - 預設PIN為12345678
  - 安裝HiCOS卡片管理工具 (本次說明會附贈之光碟上含有安裝程式)
  - 安裝讀卡機(本次說明會附贈1部)
  - 連線到GTestCA 2048 bits憑證測試網頁，申請2048 bits測試憑證
    - 網址http://gtestca.nat.gov.tw/2048Main.html
    - 注意：以上GTestCA 2048 bits憑證測試網頁僅供配合API改版而修改GPKI相關應用系統機關或廠商測試使用，GTestCA官方網頁上並不會有以上網址的Hyperlink，故機關或廠商在進行改版測試時，請於瀏覽器輸入以上完整之網址，方可進入GTestCA 2048 bits憑證測試網頁

目的

- 支援未來GPKI要發的RSA 2048 bits卡
- 整合現有發行的卡片，支援現在GPKI各CA所發出來的IC卡

CSP新舊版本差異

CSP Architectural



版本差異

CSP名稱		HiCOS CSP		safeSign CSP
版本		2.0.0	2.0.1 以上	1.0.8
Full CSP Name		HiCOS PKI Smart Card Cryptographic Service Provider		safeSign CSP
支援的卡片	GP卡(1024)	●	●	●
	TP卡(1024)	●	●	
	TP卡(2048)		●	
	以後新發行的卡		●	
支援的作業系統		WIN98,ME,XP,2003,VISAT32 ,VISAT64		WIN98,ME,XP

版本差異

Supported Algorithms	HiCOS PKI Smart Card CSP	SafeSign CSP (1.0.8)
CALG_RSA_KEYX	●	●
CALG_RSA_SIGN	●	●
CALG_DES	●	●
CALG_3DES_112	●	●
CALG_3DES	●	●
CALG_RC2	●	●
CALG_RC4	●	●
CALG_SHA1	●	●
CALG_MD5	●	●
CALG_MD2		●
CALG_SSL3_SHAMD5	●	●
MAC		●
HMAC		●

版本差異

卡片種類	RSA金鑰長度 (bits)	簽章憑證		金鑰交換憑證	
		container name	KeySpec	container name	KeySpec
GP卡(1024)	1024	k1	AT_KEYEXCHANGE	k2	AT_KEYEXCHANGE
TP卡(1024)	1024	k1	AT_SIGNATURE	k1	AT_KEYEXCHANGE
TP卡(2048)	2048	k1	AT_SIGNATURE	k1	AT_KEYEXCHANGE

Acquiring a CSP Context(1)

BOOL WINAPI CryptAcquireContext (

HCRYPTPROV phProv,*	Pointer to a handle of CSP
LPCTSTR pszContainer,	金鑰容器名稱
LPCTSTR pszProvider,	CSP名稱
DWORD dwProvType,	CSP TYPE
DWORD dwFlags	Flag Values

);

HiCOS CSP 名稱: HiCOS PKI Smart Card Cryptographic Service Provider

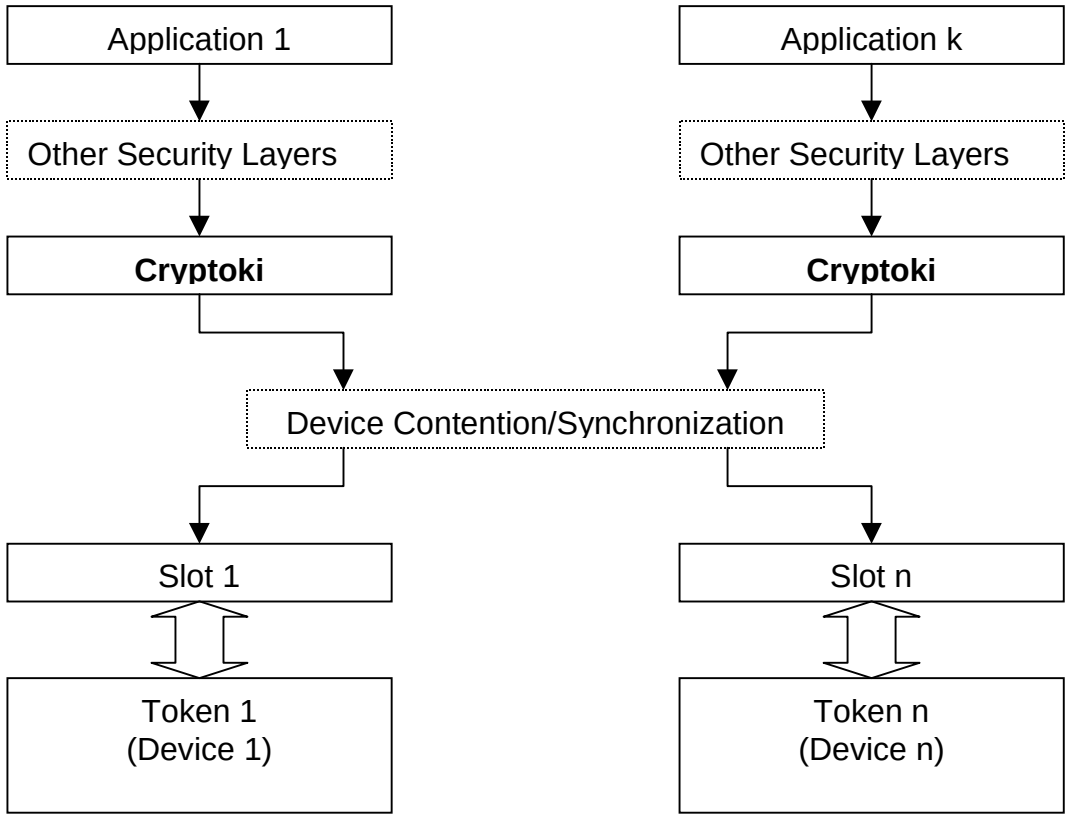
Acquiring a CSP Context (2)

範例:

```
HCRYPTPROV hCryptProv;
if(CryptAcquireContext(
    &hCryptProv,
    "HiCOS PKI Smart Card Cryptographic Service Provider",
    NULL,
    PROV_RSA_FULL,
    0) != FALSE) {
     printf("CryptAcquireContext failed.\n"); //呼叫失敗
}
else {
     printf("CryptAcquireContext succeeded.\n");//呼叫成功
}
….
….
CryptReleaseContext(hCryptProv,0);
```

PKCS#11新舊版本差異

General Cryptoki Model

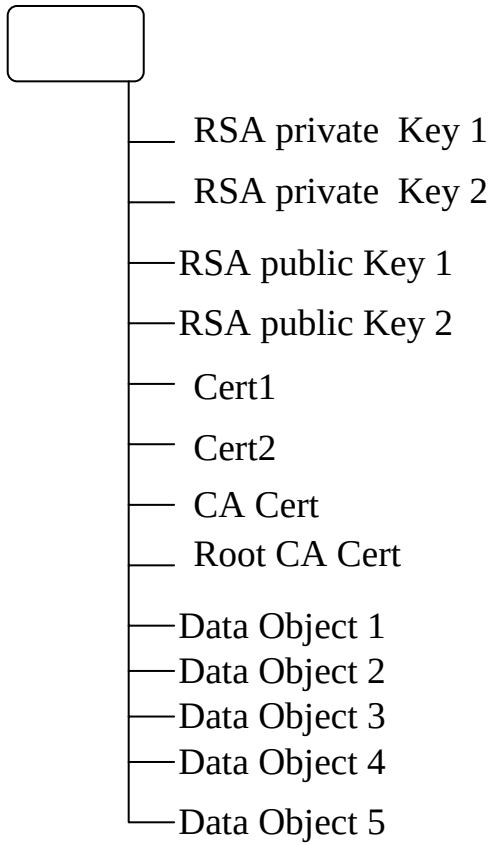


版本差異

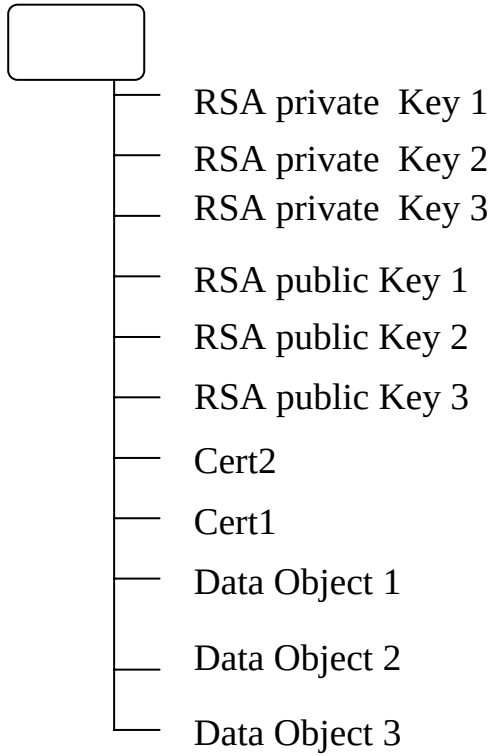
PKCS#11名稱		HiCOS PKCS#11		safeSign PKCS#11
版本		2.0.0	2.0.5 以上	1.0.8
Dll name		HiCOSPKCS11.dll		aetpkss1
支援的卡片	GP卡(1024)	●	●	●
	TP卡(1024)	●	●	
	TP卡(2048)		●	
	以後新發行的卡		●	
支援的作業系統		WIN98,ME,XP,2003,VISAT32 ,VISAT64		WIN98,ME,XP

版本差異

HiCOS卡(卡號TP開頭)



G&D卡(卡號GP開頭)



使用HiCOS PKCS#11

範例:

```
CK_FUNCTION_LIST_PTR ckFunc;

CK_RV          InitializePKCS11(){

CK_RV          rv;

HINSTANCE  hModule;

CK_C_GetFunctionList pC_GetFunctionList;

CK_C_INITIALIZE_ARGS InitArgs;


InitArgs.flags = CKF_OS_LOCKING_OK;
InitArgs.pReserved = NULL_PTR;
InitArgs.CreateMutex = NULL;
InitArgs.DestroyMutex = NULL;
InitArgs.LockMutex = NULL;
InitArgs.UnlockMutex = NULL;

hModule = LoadLibrary("HiCOSPKCS11.dll");
if ( hModule ==NULL)
     return CKR_FUNCTION_FAILED;

pC_GetFunctionList = (CK_C_GetFunctionList )GetProcAddress(hModule,"C_GetFunctionList");

if ( (rv=(*pC_GetFunctionList)(&ckFunc)) != CKR_OK)
        return rv;

rv = (*ckFunc->C_Initialize)(&InitArgs);
  return rv;

}
```

版本差異

	HiCOS PKCS#11 (2.0.5)	SafeSign PKCS#11(1.0.8.42)
支援的卡片	HiCOS卡(卡號TP開頭), G&D卡(卡號GP開頭)	G&D卡(卡號GP開頭)
Supported Algorithms		
CKM_RSA_PKCS_KEY_PAIR_GEN	●	●
CKM_RSA_PKCS	●	●
CKM_RSA_X509		●
CKM_MD5_RSA_PKCS	●	
CKM_SHA1_RSA_PKCS	●	
CKM_RC2_KEY_GEN		●
CKM_RC2_ECB		●
CKM_RC2_CBC		●
CKM_RC2_CBC_PAD		●
CKM_RC4_KEY_GEN		●
CKM_RC4		●
CKM_DES_KEY_GEN	●	●
CKM_DES_ECB		●
CKM_DES_CBC	●	●
CKM_DES_CBC_PAD	●	●
CKM_DES3_KEY_GEN	●	●
CKM_DES3_ECB		●
CKM_DES3_CBC	●	●
CKM_DES3_CBC_PAD	●	●
CKM_MD2		●
CKM_MD5	●	●
CKM_SHA1	●	●

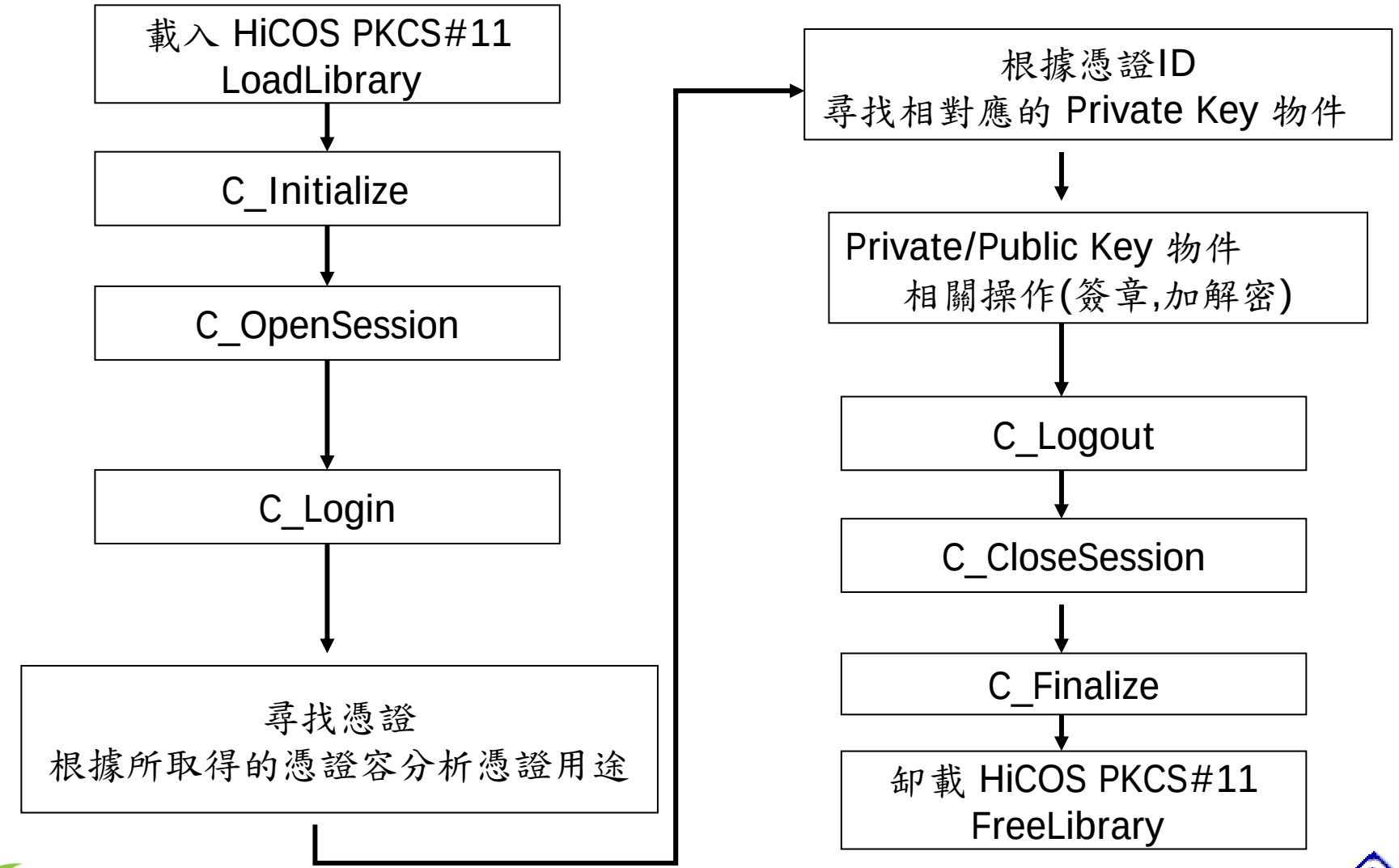
新版本功能

讀取卡片卡號

-使用C_GetTokenInfo 可讀取卡片卡號

```
typedef struct CK_TOKEN_INFO {
…
CK_CHAR       serialNumber[16];
…
}
```

PKCS#11建議呼叫流程



問題反應

- 機關或廠商在進行改版測試時，如何反應新版API問題：
  - GCA/XCA/GTestCA客服中心：
    - Mail至GCA 服務信箱egov@service.gov.tw。
    - 電話02-7738-8066
  - MOEACA客服專線：
    - 電話412-1166
      - 當地電話號碼七碼或八碼地區(含金門地區)，請撥：412-1166
      - 當地電話號碼六碼地區，請撥：41-1166
      - 外島(如馬祖,烏坵,東沙,綠島,蘭嶼等地區)及國內行動電話，請撥：(02或04或07)-412-1166
      - 國外地區，請撥：886-(2或4或7)-412-1166
  - MOICA「API問題/障礙申告」網頁：
    - 進入MOICA網站(http://moica.nat.gov.tw)，點選網頁上方的「應用服務」，然後點選網頁左方功能表的「API問題/障礙申告」

報告完畢

請多指教