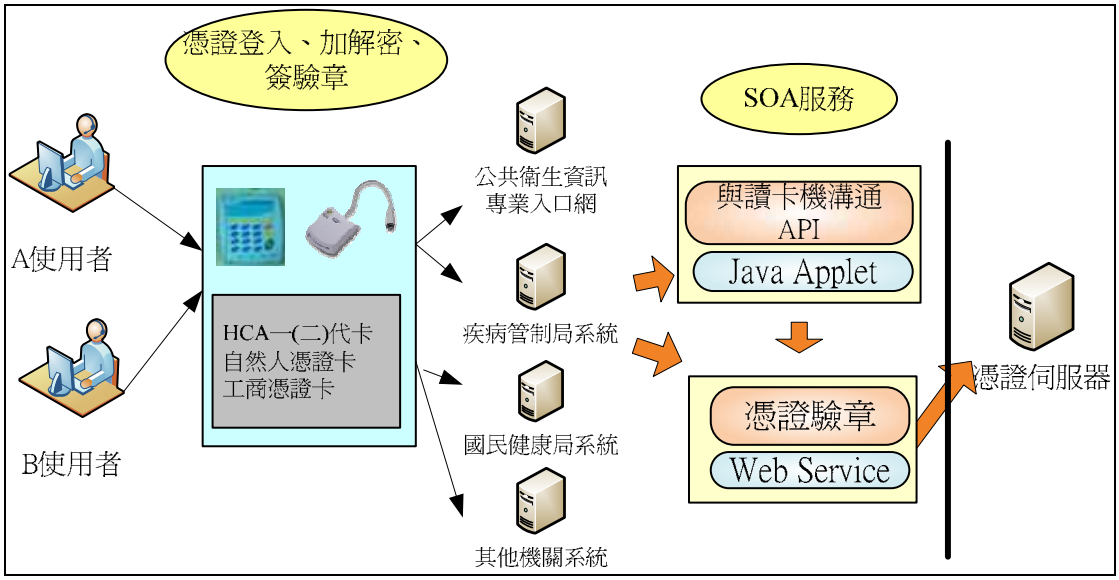
電子憑證服務使用說明

壹、前言

提供簡易之電子憑證服務進行身分認證與機密性資料傳遞的加解密，以提升資訊安全強度。



貳、主要功能

一、憑證登入

使用卡片登入，並與驗證伺服器確認檢查憑證的合法性(是否為信任的 CA 所發、憑證是否到期以及憑證是否在黑名單中)，驗證成功後，從卡片取得 ID 來登入系統。

二、憑證加解密

使用憑證進行加解密。

三、憑證簽驗章

使用憑證進行簽驗章。

參、使用說明

為了能讓 Client 端使用者使用卡片登入、加解密、簽驗章等動作，Client 端使用者必須下載安裝 Java 版的 uPKI 元件，Server 端需要在應用系統跟目錄下放至 SCardApplet.jar 檔案。

在網頁內加入以下使用 Applet 的語法

```
</SCRIPT>
</head>
<!--Java Applet程式-->
<APPLET CODE="tk.pki.applet.HCACardApplet.class"
        ARCHIVE="./SCardApplet.jar"
                WIDTH=0 HEIGHT=0
        NAME="HCACardApplet" MAYSCRIPT=true>
</APPLET>

<body >
<center>
```

- CODE：指出所要使用的 Applet 類別完整路徑以及檔案，若使用 HCA 卡請寫入”tk.pki.applet.HCACardApplet.class”，其他卡別如自然人憑證...等，請使用”tk.pki.applet.OTHCardApplet.class”。
- ARCHIVE：指出 Applet 的 jar 檔實際擺放位置，程式設計者須在指定的位置上放置 SCardApplet.jar 檔案，以供 Client 端瀏覽該網頁時下載該 jar 檔。
- NAME：宣告此 Applet 的變數名稱，在網頁中若要使用此 Applet，均需使用此名稱，這邊使用” HCACardApplet”(名稱可自訂)。

以 JavaScript 的方式呼叫 Applet 的 function

```
<SCRIPT>
  //呼叫Java Applet的函式,登入
  function signICCard() {
        document.HCACardApplet.Login(document.certForm.ticket.value);

        if (document.HCACardApplet.resultCode==0){
            alert("登入成功!!");
        }else{
            alert(document.HCACardApplet.resultMessage());
        }
  }//End 登入
  //取得卡片資訊
  function cardInfo() {
        document.HCACardApplet.CardInfo(document.certForm.ticket.value);//取得前端輸入的pinecode
        if (document.HCACardApplet.resultCode==0){
            //alert(document.HCACardApplet.getID());//取得ID
            //alert(document.HCACardApplet.getNAME());//取得名稱
            msg=document.HCACardApplet.CardString();
            mmm.innerHTML=msg;
        }else{
            msg=document.HCACardApplet.resultCode+")"+document.HCACardApplet.resultMessage();
            alert(msg);
        }
  }//End 取得卡片資訊
</SCRIPT>
```

宣告此 Applet 的變數名稱

applet提供的function

肆、Applet Function 列表

function	傳入參數	回傳值說明	說明	備註
不分卡別共用函數				
String getVer()	無	版本序號	取得 Applet 版本序號	
boolean Login(String pineCode)	卡片密碼	True:成功 False:失敗	IC 卡片登入	
boolean CardInfo()	無	True:成功 False:失敗	取得卡片資料	整個流程只需要呼叫一次
String Sign(String ticket)	欲加簽字串	加簽後字串	字串簽章	必須先 Login()
String SignVerify(String signedData)	加簽後字串	原始加簽字串		必須先 Login()
boolean SignFile(String sourcepath)	欲簽章的檔案完整位置	True:成功 False:失敗 若成功，會產生一個原檔案加上.sign 的簽章檔案	檔案簽章	必須先 Login()
boolean VerifyFile(String filepath)	加簽後字串	True:成功 False:失敗 若成功，會產生一個與原檔案相同檔名之檔案，若檔名重複，則以(數字)接在檔名後端	字串驗章	必須先 Login()

function	傳入參數	回傳值說明	說明	備註
String Encode(String data)	原始資料字串	加密後字串	字串加密	必須先 Login()
String Decode(String encodeddata)	加密後字串	解密後字串	字串解密	必須先 Login()
boolean EncodeFile(String filepath)	原始檔案路徑	True:成功 False:失敗 若成功，會產生一個原檔案加上.p7e 的加密檔案	檔案加密	必須先 Login()
boolean DecodeFile(String encodedfilepath)	加密後檔案路徑	True:成功 False:失敗 若成功，會產生一個與原檔案相同檔名之檔案，若檔名重複，則以(數字)接在檔名後端	檔案解密	必須先 Login()
HCA 卡片取基本資料函數				
String getID()	無	卡片 ID	取得卡片 ID	必須先 CardInfo()
String getNAME()	無	人員姓名或機構名稱	取得名稱	必須先 CardInfo()
String getCardVERSION()	無	1:一代卡 2:二代卡	取得卡片版本	必須先 CardInfo()
getCardTYPE()	無	0:機構卡	取得卡片別	必須先 CardInfo()

function	傳入參數	回傳值說明	說明	備註
		1:人員卡		
String getOWNER()	無			必須先 CardInfo()
String getADDRESS()	無	地址	取得地址	必須先 CardInfo()
String getTEL()	無	電話	取得電話	必須先 CardInfo()
String getENAME()	無	英文名字	取得英文名字	必須先 CardInfo()
String getSEX()	無	性別	取得性別	必須先 CardInfo()
String getBIRTHDAY()	無	人員生日	取得生日	必須先 CardInfo()
String getCHBIRTHDAY()	無	人員民國生日	取得民國年生日	必須先 CardInfo()
String getCATEGORY()	無			必須先 CardInfo()
String getCertificate1BASE64()	無	簽章憑證	取得簽章憑證,取出值為 BASE64 字串	必須先 CardInfo()
String getCertificate2BASE64()	無	加密憑證	取得加密憑證,取出值為 BASE64 字串	必須先 CardInfo()
String getCACertificateBASE64()	無	CA 憑證	取得 CA 憑證,取出值為 BASE64 字串	必須先 CardInfo()
自然人憑證等卡片				

function	傳入參數	回傳值說明	說明	備註
String getID()	無	身分證後四碼	取得身分證後四碼	必須先 CardInfo()
String getNAME()	無	人員姓名	取得名稱	必須先 CardInfo()
String getISSURE()	無	憑證發行者	取得憑證發行者	必須先 CardInfo()
String getCERTIFICATEID()	無	憑證 ID	取得憑證 ID	必須先 CardInfo()
String getORGAIZATIONID()	無	組織代碼	取得組織代碼	必須先 CardInfo()
String getSUBJECT()	無	憑證主旨	取得憑證主旨	必須先 CardInfo()
String getSN()	無	憑證序號	取得憑證序號	必須先 CardInfo()
String getDATESTART()	無	憑證啟始日期	取得憑證啟始日期	必須先 CardInfo()
String getDATEEND()	無	憑證終止日期	取得憑證終止日期	必須先 CardInfo()
String getCertificate1BASE64()	無	簽章憑證	取得簽章憑證,取出值為 BASE64 字串	必須先 CardInfo()

伍、驗章 Web Service

驗章時，除了可使用 Applet 的驗章 function 與 PKI 伺服器溝通外，亦可使用 Web Service 來驗章。

一、測試 WSDL 位置(以實際介接時所提供的 IP 為主)

http://203.65.17.143:8080/PKIService/PortTypeBndPort?WSDL

二、輸入:

欄位名稱	資料型態	說明
SignData	string	簽章後資料

三、輸出(XML String):

欄位名稱	資料型態	說明
ID	string	憑證 ID
ISSURE	string	憑證發行者
SUBJECT	string	憑證主旨
SN	string	憑證序號
DATESTART	string	憑證啟始日期
DATEEND	string	憑證終止日期
ENCODED	string	憑證(base64)
CONTENT	string	被簽章的原始資料(base64)
CERT_VERIFIED	string	憑證有效性
SIGNATUREVERIFIED	string	簽章驗證結果
DESC	string	驗證結果說明
MESSAGE	string	服務訊息
XML 範例如下：		

```
<?xml version="1.0" encoding="UTF-8"?>
<VerifyResult>
    <ID>XXX5675</ID>
    <ISSURE>OU=內政部憑證管理中心, O=行政院, C=TW</ISSURE>
    <SUBJECT></SUBJECT>
    <SN>00a6cdd48f330a4caaeb22396528bd139d</SN>
    <DATESTART>2006/05/01 15:05:31</DATESTART>
    <DATEEND>2011/05/01 15:05:31</DATEEND>
    <ENCODED>MIIEIjCCAwqgAwIBAgIRAKbN1I81Ck5ZSi…</ENCODED>
     <CONTENT>ttt</CONTENT>
    <CERT_VERIFIED>true</CERT_VERIFIED>
    <SIGNATUREVERIFIED>true</SIGNATUREVERIFIED>
    <DESC>驗證成功</DESC>
    <MGE>
</VerifyResult>
```