如何快速開發 PKI-enabled之應用系統

中華電信研究所
資通安全研究室
江彬榮

大綱

- 應用系統之功能需求
- 應用系統之環境需求
- 安全檢查事項
- 開發技術之選擇
- 系統展示
- 程式碼展示

應用系統之功能需求

- 身份認證(Authentication)
  - 以傳送者的私鑰對某資料加簽後，伺服器端檢驗簽章成功後，才允許登入。
- 不可否認(Non-repudiation)
  - 對資料加簽 (e.g.電子公文之簽章) 。
  - 接收者檢驗簽章。
- 資料隱密性(Confidentiality)
  - 以接收者的憑證對資料加密後傳給接收者(e.g. 密文傳送)
  - 接收者以自己的私鑰來解密。

應用系統之環境需求

- 採用之技術
  - ASP & ASP.Net
  - Java (Servlet,JSP)
- 應用系統的平台
  - IIS
  - Apache、Tomcat
  - J2EE

安全檢查事項

- 決定所信賴的RootCA、CA憑證。
- 檢查RootCA與CA憑證是否已廢止?
- 檢查使用者憑證是否為信賴的CA所核發?
- 檢查使用者憑證是否已廢止?
- 檢查使用者憑證是否已過期?
- 檢查CRL是否是最新的?
- 檢查使用者的簽章是否正確?
- 使用Challenge & Response以防止Replay攻擊。
- 應使用足夠安全的對稱式加密演算法，如Triple-DES或是AES

開發技術之選擇

- 使用政府提供之HiSecure API。
- 使用OpenSSL之C函式庫。
- 使用Microsoft CryptoAPI。
  - 僅限於MicroSoft平台。
- 使用Java的JCE或是其它的Open Source如JSS、BouncyCastle等Package
- 使用商用的PKI套件(HiPKI套件)。

開發技術之選擇

	優點	缺點
Hi-Secure API	跨平台、費用較低	不易使用
OpenSSL	免費、功能強大	不易使用
CryptoAPI	免費、功能強大、普及	不易使用 僅限Windows平台
Java Package	免費、功能強大	不易使用
商用套件 (以HiPKI爲例)	簡單易用、封裝良好，可跨平台	功能限定 、 需要費用

PKI-enabled
應用系統的成功關鍵

- 信賴具有公信力的憑證管理中心。
- 做到應有的安全檢查項目。
- 金鑰儲存媒體的控制
  - IC卡。
  - 軟體金鑰(PFX)
- 良好的使用者介面
  - 防呆、防止鎖卡
  - 使用者之教育(金鑰的保護)

系統展示

- 以HiPKI Demo Site 來展示一個典型的PKI-enabled之應用系統之功能。
  - Client (IE、JavaScript、COM元件)
  - Server(IIS、JSP、COM元件)
- Secure-Login
  - IC卡
  - PFX
- 數位簽章
- 數位信封
- 憑證解析

程式碼展示

- 登入驗證及Single Sign On
  - IC卡
  - PFX
- 數位簽章
- 數位信封
- 憑證解析

Q&A

敬請指教