華碁資訊
eTruServe

1.使用PKI機制時因token需與PC相連,且金鑰啓動密碼固定,請教您若在輸入金鑰啓動密碼時,是否有被側錄或被植入木馬的風險?
Anawer： 是。只要是static password，都有可能被木馬程式攔截盜取，因此PKI仍有此安全疑慮。有一種說法是PKI啓動密碼若採用OTP認證才是最安全的機制。

2. OTP 機制的token作業時,無需與PC相連,且回應的6位數密碼每次不同且有時效性.是否就無被側錄或被植入木馬的風險?
Answer: OTP 具一次有效的特性，因此即使被木馬程式攔截也無法再次使用。
所謂"有時效性"應該是Time-based OTP，event-based OTP則無時效性。
VASCO提供time-based OTP。

3. OTP 機制的token本身有啓動密碼嗎? 若無,那拾獲者是否利用該OTP token owner 的交易權限,即可將交易核可至下一層或是放行送出至銀行?
Answer: VASCO提供各種型態的token, Digipass Go3, Go6系列爲單鍵型token, 沒有啓動密碼，但是價格比較低。若選用Digipass 260, 270系列token，則具備啓動密碼之功能，但是價格稍高。

4. 若無法提供交易來源可辨識性及不可否認性,OTP機制是否就只能用於認證用途,而無法取代PKI機制除認證外,並可用於交易放行?
Answer: VASCO Digipass 260/270數字鍵盤型token除了可以產製認証使用的OTP，也可以輸入交易內容(帳號、金額)並產製交易簽章功能的OTP，並具有時效性(time-based OTP)，可以替代PKI機制。但電子簽章法之規範只涵蓋PKI技術，因此需要看主管機關是否有相關規定。

5. 金管會會要求電子金融交易於交易放行時,一定要使用PKI機制嗎?
Answer:金管會相關規定對於較大金額的交易好像有規定要PKI，這部份待查。

6. PKI機制大多採用RSA非對稱性加解密技術,因此有換KEY及憑證展期問題,而OTP機制大多利用AES或3DES 對稱性加解密技術,因此無換KEY及憑證展期問題,user也省去了憑證展期時需支付的費用,若上述無誤,請問OTP機制若無需換KEY及憑證展期,不會有交易風險嗎?
Answer: 所述無誤。每一個OTP token都有唯一性的 128 bit secret，經過加密且安全的儲存在認證伺服器資料庫中。Secret資料若受到嚴格保護，就不會發生安全風險。

7. PKI機制的token費用較OTP機制的token費用高,且需憑證展期費,似乎OTP機制較具競爭力,請教目前金融保險業的應用是2者取其一或2者並行?
Answer: OTP除了價格競爭力，維護成本也低，不需要太多客服、技術支援，始用者端不需要安裝任何軟件，具備100%可攜性。一般金融機構評估高風險交易仍以PKI爲主，這跟主管機關規定有關。其他國家規定比較彈性，交給銀行自行決定交易風險以及解決方案，這產生的結果是大多數採用OTP技術。例如VASCO在全球有超過1200家金融客戶使用於e-Banking。