金融憑證網路應用系統開發注意事項

所有網路應用系統，應遵循「金融機構辦理電子銀行業務安控作業基準」之規範。透過網際網路傳遞金融交易訊息之網路應用系統，應同時遵循本開發注意事項之規範，十一項必要措施如下：

1. 於非約定轉帳交易過程中，系統應加入操作者回應事項。
2. 於非約定轉帳交易過程中，系統應動態物件呈現。
3. 系統應有連線(Session)控制及網頁逾時(TimeOut)中斷機制。
4. 系統不得以任何形式紀錄或留存憑證密碼，每次載具連線之簽章均應輸入載具密碼。
5. 若有多網頁設計，系統應驗證前一網頁正確性。
6. 若有跨網站設計，系統應驗證網站正確性。
7. 系統應以驗章成功之原文指示訊息進行交易。
8. 元件應驗證正確網站或伺服器。
9. 元件應經過作業系統被認可之數位憑證簽章(CodeSign)。
10. 於非約定轉帳交易過程中，元件應設計需經由人工介入憑證載具動作或於同筆交易搭配額外硬體設備驗證機制。
11. 採用經本會審核通過之確認型讀卡機者，得不執行本注意事項之第 1, 2, 10 項目。採用額外硬體設備驗證機制者，得不執行本注意事項之第 1, 2 項目。