20220607B2B交易架構與經營模式(續)

(五)B2B交易架構(Busyness To Busyness)   
 **SHIFT+滑鼠左鍵可增加選取繪圖物件，接著可將之群組化為一物件**

上游廠商

金融機構

2報價

6撥款

4確認

5付款

企業網站

1詢價

7商品托送

3下單

物流業者

8商品配送

下游廠商

例如「台塑關係企業網電子市集」及「鼎新電腦網站」商用軟體租用

20220607EC安全機制

(一)線上交易安全威脅：  
資料傳輸過程會有資料洩漏或被竄改、  
網路攻擊來入侵網站或阻斷服務。

(二)EC網路安全要求：要能確保機密性、  
完整性、認證性、不可否認、可用性。

(三)對稱加密：使用同一把金鑰來加密或解密。

甲🡪明文🡪加密(用金鑰A)🡪密文🡪送出  
🡪乙方收到密文🡪解密(用金鑰A)🡪明文

如DES(Data Encryption Standard)及  
AES(Advanced Encryption Standard)加密技術。

(四)非對稱加密：使用公鑰(由CA認證並公佈在網路上)  
及私鑰(用戶自行保管)來加解密。

(4-1)秘密通訊：

甲🡪明文🡪用乙的公鑰加密🡪密文🡪傳送

🡪乙收到密文🡪用乙的私鑰解密🡪明文

(4-2)數位簽章(Digital Signature)：

甲🡪明文🡪用雜湊函數算出🡪訊息摘要a🡪  
用甲的私鑰加密🡪數位簽章🡪送出🡪  
乙收到數位簽章🡪用甲的公鑰解密🡪訊息摘要b  
甲🡪明文🡪送出  
🡪乙收到明文🡪也用雜湊函數算出🡪訊息摘要c

如上訊息摘要b及訊息摘要c比對如有一致，  
則收到的明文完整、可信。