NSECURED
友 盈 智 慧 科 技

個人資料
隱私保護的需求與建議

新時代來臨，「個資利用與隱私保護」是針對政府爲公共利益之必要，依據法規考量個人資料與隱私保護，機關發佈任何統計資料，應採用「代碼化、遮除、概略化、亂數化」相關的資訊技術，以充份保障個人資料及隱私權、增進公衆互信的架構。實務上的建議如下：

- 技術上任何可逆之編碼方式，不應稱爲「**代碼化**」。
- 結合HSM加密金鑰之不可逆編碼方式，可以稱爲「**代碼化**」。
- 機關儲存個人資料時，必須將可識別數字符號「**代碼化**」以增進資訊安全。
- 身分證字號應該代碼化、醫療診斷碼ICD-10值也應一律遮除、出生年月日概略化。

代碼化技術

代碼化技術是一種保護資料隱私的技術，可以將原始資料轉換成代碼，從而避免機敏資料被未經授權的人士查看或使用。代碼化技術可以應用在各種資訊的保護中，例如個人身份證、銀行信用卡號碼等。

通用型 HSM

通用型 HSM (Hardware Security Module) 是一種硬體安全模組，具有高度的安全性和可靠性。它可以產生並儲存私鑰，將其用於加密、解密和驗證數字簽名等，在安全的環境中保障機敏資料。

代碼化技術和HSM技術結合使用

代碼化技術是一種保護資料隱私的技術，可以將原始資料轉換成代碼，從而避免機敏資料被未經授權的人士查看或使用。代碼化技術可以應用在各種資訊的保護中，例如個人身份證、銀行信用卡號碼等。

代碼化技術的應用

舉例來說，代碼化技術可被應用於以下幾個場景：

1.信用卡資料
代碼化技術可用於保護信用卡資料，例如信用卡號、有效月年和安全號碼

2.醫療健保資料
代碼化技術可用於保護醫療保健資料，例如病歷、處方、醫療保險和患者個人資訊。

3.個人身分資訊
代碼化技術可用於保護個人身分資訊，例如身分證號碼、健保卡號和駕照號碼。

台北
台北市內湖區洲子街79號7樓 | +886-2-2627-1135 | www.nsecured.com

通用型HSM的應用

通用型HSM可以在以下場景中被廣泛應用：

1.數位身份驗證
通用型HSM可用於建立、驗證數位簽名，以確認身份驗證和授權。

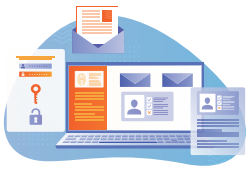
2.金融交易
通用型HSM可保護金融交易，爲信用卡資料和銀行交易數據進行加密。

3.通訊傳輸
通用型HSM可爲通訊傳輸內容進行加密，TLS和VPN即是常見的應用範例。

4.密碼管理
通用型HSM可用於妥善保存資料、應用程式和系統的密碼。

代碼化技術和HSM的結合將爲數位化政府扮演要角

如今，數位化政府已成趨勢，各種國民的資訊都在進行數位化。代碼化技術和 HSM 的結合將爲未來的數位化政府解決以下問題：



1.個人隱私保護
將個人身份識別資訊(如身分證字號、駕照號碼等)轉換成代碼並將其私鑰存儲在 HSM 中，以保護個人資料隱私。

2.資料儲存和傳輸
將機敏資料(如銀行信用卡號、身分證號碼等)轉換成代碼並將其私鑰存儲在 HSM 中，以減少資料儲存和傳輸時的風險。

3.身份驗證
使用代碼化技術進行身份驗證，結合儲存在HSM的金鑰，以確保身份識別資訊的安全性。

4.大數據分析
將數據資料以代碼化技術做匿名化後進行分析，以保護個人隱私和資料安全。

通用型HSM的硬體規格

尺寸：1U或2U機架式伺服器
處理器：多核心處理器
記憶體：通常爲16GB以上
存儲：通常爲1TB以上的硬碟空間
網路介面：通常具備多個乙太網路介面
安全模組：包含加密卡和硬體安全模組
支援的演算法：包括AES、RSA、ECC、SHA等對稱和非對稱加密演算法
安全認證：FIPS 140-2 Level 3、CC EAL4+

代碼化技術的硬體規格

尺寸：1U或2U機架式伺服器
處理器：多核心處理器
記憶體：通常爲16GB以上
存儲：通常爲1TB以上的硬碟空間
網路介面：通常具備多個乙太網路介面
安全模組：包含加密卡和硬體安全模組
支援的代碼化演算法：包括Tokenization、Data Masking等

台北
台北市內湖區洲子街79號7樓 | +886-2-2627-1135 | www.nsecured.com