電子化政府應用系統支援 2048 位元憑證修正作業檢查表

版本:1.0 (98.05.26)

說明：

因應資訊網路環境電腦硬體效能提升，為防範憑證應用之各類密碼演算法遭破解，並依據政府機關公開金鑰基礎建設（Government Public-Key Infrastructure，GPKI）推行小組決議，所轄之各憑證管理中心(GCA、XCA、MOEACA 及 MOICA) 陸續於 98 年 7 月起停發 1024 位元憑證，並開始提供安全性較高的 2048 位元憑證及 IC 智慧卡，預估 GPKI 1024 位元憑證將於民國 104 年全部到期。

為提升既有支援 1024 位元憑證的 PKI-enabled 應用系統，能夠同時相容於現有 1024 位元憑證及 IC 智慧卡，並支援 2048 位元憑證及 IC 智慧卡，須使用新版之應用程式介面（Application Programming Interface，API）或中介軟體（Middleware）進行改版，並於 98 年 6 月 30 日前，正式切換到新版應用系統，以確保新持有 2048 位元憑證及 IC 智慧卡之用戶可正常使用該應用系統。

依據以上說明，提供改版或新開發之電子化政府 PKI-enabled 應用系統對 2048 位元憑證及 IC 智慧卡之相容性檢查項目如下：

1. 伺服器端之檢查項目：

項次	檢查項目	檢查結果
1.1	**所使用之密碼模組是否支援 2048 位元之 RSA 金鑰及運算？** **說明 1：**密碼模組可以是硬體密碼模組（Hardware Security Module，HSM）或軟體密碼模組，若有使用多種密碼模組，請確定所使用的密碼模組皆支援 2048 位元（含）以上之 RSA 金鑰及運算（含簽驗章或加解密運算）。 **說明 2：**應用系統可能不會直接介接底層的密碼模組，而是透過 API 或 Middleware 來介接底層之密碼模組，若有此種狀況，請向 API 或 Middleware 之提供者洽詢其所提供的 API 或 Middleware 版本及底層的密碼模組是否支援 2048 位元（含）以上之 RSA 金鑰及運算。GPKI 官方提供之 HiCOS PKCS#11 2.0.8 版（含）以上、HiCOS CSP 2.1.0 版（含）以上、HiSecure C/C++ API 6.0 版（含）以上、及 HiSecure Java API 2.0 版（含）以上，皆可支援 2048 位元（含）以上之 RSA 金鑰及運算。	□ 是　□ 否
1.2	**資料庫用來存放憑證的欄位是否足以容納 2048 位元憑證？** 說明：若未使用資料庫欄位來儲存憑證，則請勾選「不適用」	□ 是　□ 否 □ 不適用
1.3	資料庫用來存放公開金鑰的欄位是否足以容納 2048 位元公開金鑰？ **說明：**有些應用系統可能會將公開金鑰由憑證中取出，存放於資料庫欄位中，若您的應用系統並未使用資料庫欄位來儲存公開金鑰，則請勾選「不適用」。	□ 是　□ 否 □ 不適用

項次	檢查項目	檢查結果
1.4	**資料庫用來存放私密金鑰的欄位是否足以容納 2048 位元私密金鑰？** **說明：**當應用系統係使用軟體密碼模組時，可能會將私密金鑰存放於資料庫欄位中，若您的應用系統並未使用資料庫欄位來儲存私密金鑰，則請勾選「不適用」。	□ 是 □ 否 □ 不適用
1.5	**資料庫用來存放簽章資料的欄位是否足以容納 2048 位元 RSA 金鑰所簽署的資料？** **說明：**若未使用資料庫欄位來儲存簽章資料，則請勾選「不適用」。	□ 是 □ 否 □ 不適用
1.6	**資料庫用來存放加密資料的欄位是否足以容納 2048 位元 RSA 金鑰所加密的資料？** **說明：**若未使用資料庫欄位來儲存加密資料，則請勾選「不適用」。	□ 是 □ 否 □ 不適用
1.7	**程式中用來存放憑證的記憶區塊（Memory Block 或 Buffer）是否足以容納 2048 位元憑證？** **說明 1：**程式中若未使用記憶區塊來存放憑證，則請勾選「不適用」。 **說明 2：**一般而言，PKI-enabled 應用系統應該都會需要在記憶區塊中存放憑證，若程式本身並沒有直接存取憑證，而是透過 API 或 Middleware 來存取憑證及處理憑證資料，則請向 API 或 Middleware 之提供者洽詢其所提供的 API 或 Middleware 版本中所預留的記憶區塊是否足以容納 2048 位元憑證。 **說明 3：**若程式、API 或 Middleware 係使用動態配置記憶區塊的方式來存放憑證，則亦必須確認動態配置的記憶區塊大小確實足以容納 2048 位元憑證。GPKI 官方提供之 HiCOS PKCS#11 2.0.8 版（含）以上、HiCOS CSP 2.1.0 版（含）以上、HiSecure C/C++ API 6.0 版（含）以上、及 HiSecure Java API 2.0 版（含）以上，皆可支援 2048 位元憑證。	□ 是 □ 否 □ 不適用
1.8	**程式中用來存放公開金鑰的記憶區塊是否足以容納 2048 位元公開金鑰？** **說明 1：**程式中若未使用記憶區塊來存放公開金鑰，則請勾選「不適用」。 **說明 2：**一般而言，PKI-enabled 應用系統應該都會需要在記憶區塊中存放公開金鑰以便進行驗章或加密運算，若程式本身並沒有直接進行公開金鑰運算，而是透過 API 或 Middleware 來存取憑證並進行公開金鑰相關運算，則請向 API 或 Middleware 之提供者洽詢所提供的 API 或 Middleware 版本中所預留的記憶區塊是否足以容納 2048 位元公開金鑰。 **說明 3：**若程式、API 或 Middleware 係使用動態配置記憶區塊的方式來存放公開金鑰，則亦必須確認動態配置的記憶區塊大小確實足以容納 2048 位元公開金鑰。GPKI 官方提供之 HiCOS PKCS#11 2.0.8 版（含）以上、HiCOS CSP 2.1.0 版（含）以上、HiSecure C/C++	□ 是 □ 否 □ 不適用

項次	檢查項目	檢查結果
	API 6.0 版（含）以上、及 HiSecure Java API 2.0 版（含）以上，皆可支援 2048 位元公開金鑰。	
1.9	**程式中用來存放私密金鑰的記憶區塊是否足以容納 2048 位元私密金鑰？** **說明 1：**當應用系統係使用軟體密碼模組時，可能會將私密金鑰存放於資料庫欄位中，若您的程式並未使用記憶區塊來存放私密金鑰，則請勾選「不適用」。 **說明 2：**若程式本身並沒有直接進行私密金鑰運算，而是透過 API 或 Middleware 來存取密碼模組並進行私密金鑰相關運算，則請向 API 或 Middleware 之提供者洽詢其所提供的 API 或 Middleware 版本中所預留的記憶區塊是否足以容納 2048 位元私密金鑰。 **說明 3：**若是程式、API 或 Middleware 係使用動態配置記憶區塊的方式來存放公開金鑰，則亦必須確認動態配置的記憶區塊大小確實足以容納 2048 位元私密金鑰。	□ 是　□ 否 □ 不適用
1.10	**程式中用來存放簽章資料的記憶區塊是否足以容納 2048 位元 RSA 金鑰所簽署的資料？** **說明 1：**程式中若未使用記憶區塊來存放簽章資料，則請勾選「不適用」。 **說明 2：**一般而言，PKI-enabled 應用系統進行簽驗章運算時，應該都會需要在記憶區塊中存放簽章資料，若程式本身並沒有直接進行簽驗章運算，而是透過 API 或 Middleware 來存取憑證並進行簽驗章運算，則請向 API 或 Middleware 之提供者洽詢所提供的 API 或 Middleware 版本中所預留的記憶區塊是否足以容納 2048 位元 RSA 金鑰所簽署的資料。 **說明 3：**若程式、API 或 Middleware 係使用動態配置記憶區塊的方式來存放公開金鑰，則亦必須確認動態配置的記憶區塊大小確實足以容納 2048 位元 RSA 金鑰所簽署的資料。目前 GPKI 官方提供之 HiCOS PKCS#11 2.0.8 版（含）以上、HiCOS CSP 2.1.0 版（含）以上、HiSecure C/C++ API 6.0 版（含）以上、及 HiSecure Java API 2.0 版（含）以上，皆可支援 2048 位元簽驗章運算。	□ 是　□ 否 □ 不適用
1.11	**程式中用來存放簽章資料的記憶區塊是否足以容納 2048 位元 RSA 金鑰所加密的資料？** **說明 1：**程式中若未使用記憶區塊來存放加密資料，則請勾選「不適用」。 **說明 2：**一般而言，PKI-enabled 應用系統進行加解密運算時，應該都會需要在記憶區塊中存放加密資料，若程式本身並沒有直接進行加解密運算，而是透過 API 或 Middleware 來存取進行加解密運算，則請向 API 或 Middleware 之提供者洽詢所提供的 API 或 Middleware 版本中所預留的記憶區塊是否足以容納 2048 位元 RSA	□ 是　□ 否 □ 不適用

項次	檢查項目	檢查結果
	金鑰所加密的資料。 **說明 3：**若程式、API 或 Middleware 係使用動態配置記憶區塊的方式來存放加密，則亦必須確認動態配置的記憶區塊大小確實足以容納 2048 位元 RSA 金鑰所加密的資料。GPKI 官方提供之 HiCOS PKCS#11 2.0.8 版(含)以上、HiCOS CSP 2.1.0 版(含)以上、HiSecure C/C++ API 6.0 版（含）以上、及 HiSecure Java API 2.0 版（含）以上，皆可支援 2048 位元加解密運算。	

2. 用戶端之檢查項目：

項次	檢查項目	檢查結果
2.1	**用戶端程式是否是透過 GPKI 官方提供之 HiCOS PKCS#11 2.0.8 版（含）以上或 HiCOS CSP 2.1.0 版（含）以上之應用程式介面存取用戶之 IC 智慧卡？** **說明 1：**若用戶端程式係使用軟體密碼模組及軟體金鑰，而並沒有使用 IC 智慧卡，則請勾選「不適用」。 **說明 2:**原先GPKI官方所提供之SafeSign Client 1.0.8版之PKCS#11及CSP，或是廠商或機關另外提供的其他版本之 SafeSign Client 之 PKCS#11 及 CSP，並無法存取 GPKI 各憑證管理中心所發的 2048 位元 IC 智慧卡，GPKI 官方即將停止對於 SafeSign Client 之 PKCS#11 及 CSP 提供技術支援，因此用戶端程式如須存取用戶 IC 智慧卡，則不論是 1024 位元 IC 智慧卡或 2048 位元 IC 智慧卡，請皆透過 HiCOS PKCS#11 2.0.8 版（含）以上、HiCOS CSP 2.1.0 版（含）以上之應用程式介面來進行存取。即使是面對 1024 位元 IC 智慧卡，亦請透過 HiCOS PKCS#11 2.0.8 版(含)以上、HiCOS CSP 2.1.0 版（含）以上之應用程式介面來進行存取。 **說明 3：**若用戶端程式並不是直接透過 PKCS#11 或 CSP 應用程式介面來存取 IC 智慧卡，而是透過 API 或 Middleware 來介接存取 IC 智慧卡，則請向 API 或 Middleware 之提供者洽詢其所提供的 API 或 Middleware 版本是否可透過 HiCOS PKCS#11 2.0.8 版（含）以上或 HiCOS CSP 2.1.0 版（含）以上之應用程式介面來存取 GPKI 各憑證管理中心所發的用戶 IC 智慧卡。 **說明 4：**若用戶端程式所使用的應用程式介面為 HiSecure API，則請確定是否為 HiSecure C/C++ API 6.0 版（含）以上、及 HiSecure Java API 2.0 版(含)以上，新版之 HiSecure C/C++ API 及 HiSecure Java API 之底層係透過 HiCOS PKCS#11 2.0.8 版（含）以上或 HiCOS CSP 2.1.0 版（含）以上之應用程式來介接 IC 智慧卡，而舊版之 HiSecure API 並無法支援 2048 位元 IC 智慧卡。 **說明 5:**本檢查表中所謂「GPKI 各憑證管理中心所發之 IC 智慧卡」不包含衛生署醫事憑證管理中心（HCA）所發的 IC 智慧卡，HCA	□ 是　□ 否 □ 不適用

項次	檢查項目	檢查結果
	雖然已正式加入 GPKI，但為配合健保之應用，HCA 所發的 IC 智慧卡為 Java 卡，其規格與 GPKI 中其他憑證管理中心所發之 IC 智慧卡不同，且衛生署另有提供一套 HCA 醫事憑證 IC 智慧卡專用之 API，因此應用系統如須介接 HCA 醫事憑證 IC 智慧卡，請洽衛生署取得 HCA 醫事憑證 IC 智慧卡專用之 API。	
2.2	**應用系統之網頁或使用者手冊是否明確地告知用戶必須下載並安裝最新版「HiCOS 卡片管理工具」？** **說明 1：**若用戶端程式係使用軟體密碼模組及軟體金鑰，而並沒有使用 IC 智慧卡，則請勾選「不適用」。 **說明 2：**「HiCOS 卡片管理工具」內含 HiCOS PKCS#11 及 HiCOS CSP，而這兩個應用程式介面為 GPKI 官方支援之 IC 智慧卡存取介面，因此「HiCOS 卡片管理工具」可視為用戶 IC 智慧卡之「驅動程式」，用戶要在應用程式中正常使用 IC 智慧卡，首先就必須安裝正確版本之「驅動程式」。 **說明 3：**為確保用戶可於應用系統中正常使用 GPKI 各憑證管理中心所發的 IC 智慧卡（含 1024 位元 IC 智慧卡及 2048 位元 IC 智慧卡，但不包含 HCA 所發之 IC 智慧卡），應用程式應該於其網頁或使用者手冊明確地告知用戶必須下載並安裝最新版「HiCOS 卡片管理工具」，並提供憑證管理中心網站的網址或連結，以方便用戶下載「HiCOS 卡片管理工具」。 **說明 4：**HiCOS PKCS#11 及 HiCOS CSP 是用戶端正常使用 IC 智慧卡不可或缺的兩個應用程式介面，而用戶應自行至憑證管理中心網站下載最新版之「HiCOS 卡片管理工具」的安裝程式進行安裝，此為 GPKI 官方所支援之安裝方式。「HiCOS 卡片管理工具」安裝時並附帶安裝 CHT up2date agent 程式，CHT up2date agent 程式可以不定時連線到 CHT up2date 軟體更新伺服器檢查是否有新版 HiCOS 卡片管理工具、HiCOS PKCS#11、或 HiCOS CSP，未來 GPKI 如果有其他種類的 IC 智慧卡或是發現 HiCOS 卡片管理工具或 HiCOS PKCS#11 及 HiCOS CSP 等軟體有 Bug 或安全漏洞時，都將透過此管道通知用戶更新其 HiCOS 卡片管理工具、HiCOS PKCS#11、或 HiCOS CSP。 **說明 5：**HiCOS PKCS#11 及 HiCOS CSP 係內含於「HiCOS 卡片管理工具」，授權 GPKI 之憑證用戶可自行由 GPKI 各憑證管理中心下載及安裝，並未授權應用程式自行散播 HiCOS PKCS#11 及 HiCOS CSP。由於應用系統如果自行散播 HiCOS PKCS#11 及 HiCOS CSP 到用戶端，而不是透過 HiCOS 卡片管理工具安裝，則用戶將不會經由 CHT up2date 管道獲得更版之通知，因此不建議應用程式自行散播 HiCOS PKCS#11 及 HiCOS CSP。但應用系統如有特殊原因必須自行散播 HiCOS PKCS#11 及 HiCOS CSP 相關檔案	□ 是　□ 否 □ 不適用

項次	檢查項目	檢查結果
	至用戶端，請洽 GPKI 各憑證管理中心客服中心。	
2.3	**用戶端是否同時支援 2048 位元 IC 智慧卡及 1024 位元 IC 智慧卡？** **說明 1：**若用戶端程式係使用軟體密碼模組及軟體金鑰，而並沒有使用 IC 智慧卡，則請勾選「不適用」。 **說明 2：**由於現有 1024 位元憑證及 IC 智慧卡將繼續使用到該憑證過期為止，而 GPKI 用戶之 1024 位元憑證的效期為 5 年，所以預估 GPKI 將於 104 年全面過渡到 2048 位元憑證及 IC 智慧卡。在此過渡期間，應用系統必須能夠同時相容於現有 1024 位元憑證及 IC 智慧卡，因此系統上線前請檢查是否同時支援 2048 位元 IC 智慧卡及 1024 位元 IC 智慧卡兩種卡片。	□ 是 □ 否 □ 不適用
2.4	**用戶端如果同時裝了「HiCOS 卡片管理工具」2.1.0 版（含）以上或是 SafeSign Client（任何版本），則應用程式是否仍可正常存取 2048 位元 IC 智慧卡及 1024 位元 IC 智慧卡？** **說明 1：**若用戶端程式係使用軟體密碼模組及軟體金鑰，而並沒有使用 IC 智慧卡，則請勾選「不適用」。 **說明 2：**由於用戶可能使用數個 PKI-enabled 應用系統，因此用戶之個人電腦中可能同時安裝不同 PKI-enabled 應用系統之用戶端軟體，而由於各應用系統改版及新版上線的時程可能不同，因此同一個用戶電腦中可能同時有新版系統必須透過新版 HiCOS PKCS#11 或 HiCOS CSP 存取 2048 位元 IC 智慧卡及 1024 位元 IC 智慧卡，而同時又有尚未改版之應用系統需要透過原有之 SafeSign PKCS#11 或 SafeSign CSP 存取 1024 位元 IC 智慧卡的情況，所以應用系統上線前必須測試看看在這樣的環境下是否能夠正常運作。 **說明 3：**「HiCOS 卡片管理工具」2.1.0 版（含）以上之安裝程式在進行安裝時，並不會自動將用戶電腦中原先已安裝的任何版本之 SafeSign Client 予以移除，即是考慮到用戶端電腦在過渡時期可能會有同時需要使用新舊版本之應用程式介面的情況。	□ 是 □ 否 □ 不適用
2.5	**資料庫用來存放憑證的欄位是否足以容納 2048 位元憑證？** 說明：若未使用資料庫欄位來儲存憑證，則請勾選「不適用」	□ 是 □ 否 □ 不適用
2.6	**資料庫用來存放公開金鑰的欄位是否足以容納 2048 位元公開金鑰？** **說明：**有些應用系統可能會將公開金鑰由憑證中取出，存放於資料庫欄位中，若您的應用系統並未使用資料庫欄位來儲存公開金鑰，則請勾選「不適用」。	□ 是 □ 否 □ 不適用
2.7	**資料庫用來存放私密金鑰的欄位是否足以容納 2048 位元私密金鑰？** **說明：**當應用系統係使用軟體密碼模組時，可能會將私密金鑰存放於資料庫欄位中，若您的應用系統並未使用資料庫欄位來儲存私密金鑰，則請勾選「不適用」。	□ 是 □ 否 □ 不適用

項次	檢查項目	檢查結果
2.8	**資料庫用來存放簽章資料的欄位是否足以容納 2048 位元 RSA 金鑰所簽署的資料？** **說明：**若未使用資料庫欄位來儲存簽章資料，則請勾選「不適用」。	□ 是 □ 否 □ 不適用
2.9	**資料庫用來存放加密資料的欄位是否足以容納 2048 位元 RSA 金鑰所加密的資料？** **說明：**若未使用資料庫欄位來儲存加密資料，則請勾選「不適用」。	□ 是 □ 否 □ 不適用
2.10	**程式中用來存放憑證的記憶區塊（Memory Block 或 Buffer）是否足以容納 2048 位元憑證？** **說明 1：**程式中若未使用記憶區塊來存放憑證，則請勾選「不適用」。 **說明 2：**一般而言，PKI-enabled 應用系統應該都會需要在記憶區塊中存放憑證，若程式本身並沒有直接存取憑證，而是透過 API 或 Middleware 來存取憑證及處理憑證資料，則請向 API 或 Middleware 之提供者洽詢其所提供的 API 或 Middleware 版本中所預留的記憶區塊是否足以容納 2048 位元憑證。 **說明 3：**若程式、API 或 Middleware 係使用動態配置記憶區塊的方式來存放憑證，則亦必須確認動態配置的記憶區塊大小確實足以容納 2048 位元憑證。GPKI 官方提供之 HiCOS PKCS#11 2.0.8 版（含）以上、HiCOS CSP 2.1.0 版（含）以上、HiSecure C/C++ API 6.0 版（含）以上、及 HiSecure Java API 2.0 版（含）以上，皆可支援 2048 位元憑證。	□ 是 □ 否 □ 不適用
2.11	**程式中用來存放公開金鑰的記憶區塊是否足以容納 2048 位元公開金鑰？** **說明 1：**程式中若未使用記憶區塊來存放公開金鑰，則請勾選「不適用」。 **說明 2：**一般而言，PKI-enabled 應用系統應該都會需要在記憶區塊中存放公開金鑰以便進行驗章或加密運算，若程式本身並沒有直接進行公開金鑰運算，而是透過 API 或 Middleware 來存取憑證並進行公開金鑰相關運算，則請向 API 或 Middleware 之提供者洽詢所提供的 API 或 Middleware 版本中所預留的記憶區塊是否足以容納 2048 位元公開金鑰。 **說明 3：**若程式、API 或 Middleware 係使用動態配置記憶區塊的方式來存放公開金鑰，則亦必須確認動態配置的記憶區塊大小確實足以容納 2048 位元公開金鑰。GPKI 官方提供之 HiCOS PKCS#11 2.0.8 版（含）以上、HiCOS CSP 2.1.0 版（含）以上、HiSecure C/C++ API 6.0 版（含）以上、及 HiSecure Java API 2.0 版（含）以上，皆可支援 2048 位元公開金鑰。	□ 是 □ 否 □ 不適用
2.12	**程式中用來存放私密金鑰的記憶區塊是否足以容納 2048 位元私密金鑰？** **說明 1：**當應用系統係使用軟體密碼模組時，可能會將私密金鑰存	□ 是 □ 否 □ 不適用

項次	檢查項目	檢查結果
	放於資料庫欄位中，若您的程式並未使用記憶區塊來存放私密金鑰，則請勾選「不適用」。 **說明 2：**若程式本身並沒有直接進行私密金鑰運算，而是透過 API 或 Middleware 來存取密碼模組並進行私密金鑰相關運算，則請向 API 或 Middleware 之提供者洽詢其所提供的 API 或 Middleware 版本中所預留的記憶區塊是否足以容納 2048 位元私密金鑰。 **說明 3：**若是程式、API 或 Middleware 係使用動態配置記憶區塊的方式來存放公開金鑰，則亦必須確認動態配置的記憶區塊大小確實足以容納 2048 位元私密金鑰。	
2.13	**程式中用來存放簽章資料的記憶區塊是否足以容納 2048 位元 RSA 金鑰所簽署的資料？** **說明 1：**程式中若未使用記憶區塊來存放簽章資料，則請勾選「不適用」。 **說明 2：**一般而言，PKI-enabled 應用系統進行簽驗章運算時，應該都會需要在記憶區塊中存放簽章資料，若程式本身並沒有直接進行簽驗章運算，而是透過 API 或 Middleware 來存取憑證並進行簽驗章運算，則請向 API 或 Middleware 之提供者洽詢所提供的 API 或 Middleware 版本中所預留的記憶區塊是否足以容納 2048 位元 RSA 金鑰所簽署的資料。 **說明 3：**若程式、API 或 Middleware 係使用動態配置記憶區塊的方式來存放公開金鑰，則亦必須確認動態配置的記憶區塊大小確實足以容納 2048 位元 RSA 金鑰所簽署的資料。目前 GPKI 官方提供之 HiCOS PKCS#11 2.0.8 版（含）以上、HiCOS CSP 2.1.0 版（含）以上、HiSecure C/C++ API 6.0 版（含）以上、及 HiSecure Java API 2.0 版（含）以上，皆可支援 2048 位元簽驗章運算。	□ 是　□ 否 □ 不適用
2.14	**程式中用來存放簽章資料的記憶區塊是否足以容納 2048 位元 RSA 金鑰所加密的資料？** **說明 1：**程式中若未使用記憶區塊來存放加密資料，則請勾選「不適用」。 **說明 2：**一般而言，PKI-enabled 應用系統進行加解密運算時，應該都會需要在記憶區塊中存放加密資料，若程式本身並沒有直接進行加解密運算，而是透過 API 或 Middleware 來存取進行加解密運算，則請向 API 或 Middleware 之提供者洽詢所提供的 API 或 Middleware 版本中所預留的記憶區塊是否足以容納 2048 位元 RSA 金鑰所加密的資料。 **說明 3：**若程式、API 或 Middleware 係使用動態配置記憶區塊的方式來存放加密，則亦必須確認動態配置的記憶區塊大小確實足以容納 2048 位元 RSA 金鑰所加密的資料。GPKI 官方提供之 HiCOS PKCS#11 2.0.8 版(含)以上、HiCOS CSP 2.1.0 版(含)以上、HiSecure	□ 是　□ 否 □ 不適用

項次	檢查項目	檢查結果
	C/C++ API 6.0 版（含）以上、及 HiSecure Java API 2.0 版（含）以上，皆可支援 2048 位元加解密運算。	

註：

(1) 以上檢查表係假設 PKI-enabled 應用系統分為伺服端（Server Side）及用戶端（Client Side），此為最常見的型態，但如果您的應用系統是一個 standalone system，並沒有分成伺服端及用戶端兩個部分，則請將此 standalone system 視為既是伺服端又是用戶端，而填寫以上兩個表格即可。

(2) 其他有關 2048 位元憑證及IC智慧卡相關資訊及Q&A，可至政府憑證憑證中心網站(http://gca.nat.gov.tw)「2048 位元改版專區」參閱最新訊息。