GRCA、GCA及XCA第三代憑證路徑安裝及設定說明

數位發展部

111年9月

大綱

- 緣起
- CA金鑰更換規劃說明
- CA金鑰更換影響範圍
- 應用系統配合辦理事項
- 新舊憑證驗證路徑說明
- 公鑰憑證安全檢查表說明
- GTestCA測試功能說明
- 宣導事項

緣起

緣起

■ 金鑰生命週期安全性考量

非對稱式密碼演算法之金鑰對自其公開金鑰對外公開使用起，他人即可嘗試利用大量電腦運算反推其私密金鑰，故私密金鑰於使用一段期間後即應更換之，以確保其安全性。尤其「憑證機構本身之私密金鑰」牽涉整個PKI之信賴基礎，更應嚴格依照預定之金鑰生命週期進行更換。

■ 我國憑證政策更換金鑰之規定

我國「政府公開金鑰基礎建設憑證政策」中規定，

- GRCA之私密金鑰用於簽發下屬憑證機構憑證或交互憑證時，使用期限至多為10年。
- 下屬憑證機構之私密金鑰用於簽發用戶憑證時，使用期限至多10年。

因本會管理之政府憑證總管理中心(GRCA)、政府憑證管理中心(GCA)及組織及團體憑證管理中心(XCA)私密金鑰將屆使用期限，因此進行第三代GRCA、GCA、XCA新金鑰產製及新CA憑證簽發作業，以確保我國GPKI之安全性。

GPKI各CA之私鑰使用期限

憑證管理中心	私密金鑰使用期限	主管機關
政府憑證總管理中心(GRCA)	**111年09月28日**	**數位部**
政府憑證管理中心(GCA)	**112年01月31日**	**數位部**
組織及團體憑證管理中心(XCA)	113年01月02日	數位部
工商憑證管理中心(MOEACA)	**112年01月31日**	**經濟部**
內政部憑證管理中心(MOICA)	113年01月02日	內政部
醫療憑證管理中心(HCA)	117年08月14日	衛福部

將屆使用期限

CA金鑰更換規劃說明

CA金鑰長度提升

- 國際間相關文獻針對RSA金鑰長度之評估，多數認為RSA金鑰長度提升至RSA 3072 bits以上將是相對安全之作法。

- 本會召開之金鑰風險評估小組，各委員一致認為應提升金鑰長度以增加安全性。

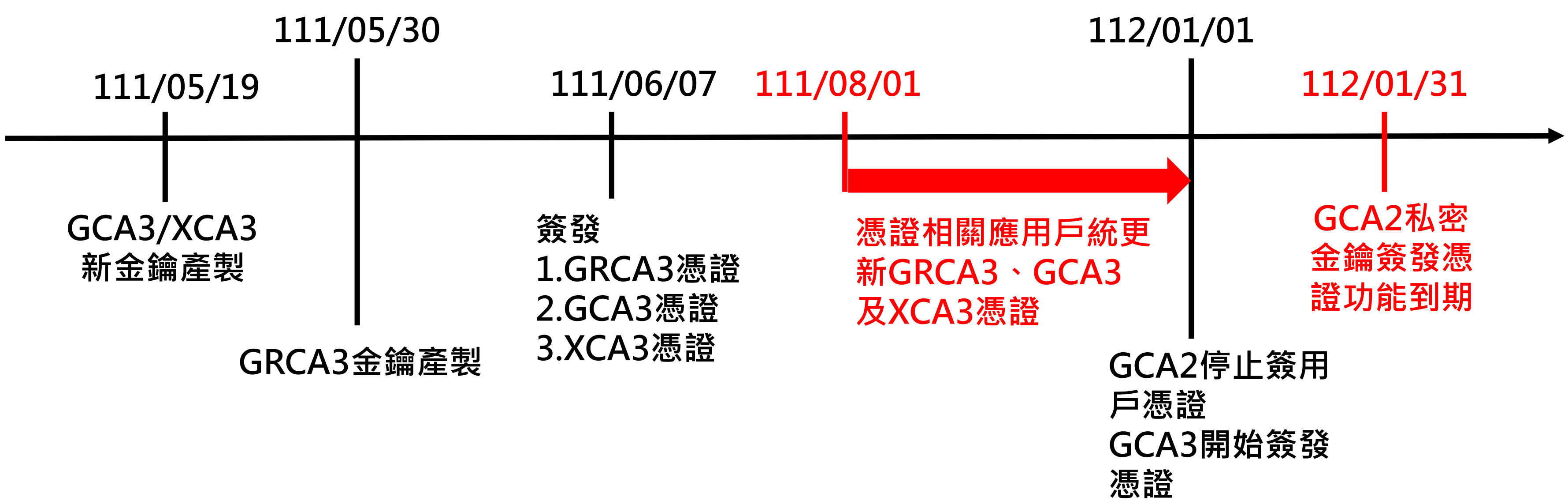
- 本次CA金鑰更換作業，將同時提升GCA及XCA之CA金鑰對長度，由RSA 2048 bits提升至RSA 4096 bits，藉此提升金鑰之安全性。

本次CA金鑰更換時程規劃

憑證管理中心	私密金鑰使用期限	預計完成更換日期	說明
GRCA	**111年09月28日**	**111年6月**	111年5月30日完成新金鑰產製。 111年6月7日正式啟用新金鑰。 111年6月7日完成自簽憑證簽發。
GCA	**112年01月31日**	**112年1月**	111年5月19日完成新金鑰產製。 111年6月7日取得CA憑證。 112年1月1日正式啟用簽發用戶憑證。
XCA	**113年01月02日**	**112年1月**	為統一管理數位部主管之CA金鑰生命週期，節省行政成本及提升效率，規劃提前產製第三代XCA金鑰(期程同GCA)。

重要時間點

- 第三代GRCA自簽憑證(根憑證)，已於111年6月7日正式啟用進行下屬憑證機構憑證簽發。
- 本部擬於112年1月1日起正式啟用第三代GCA及第三代XCA金鑰進行用戶憑證簽發，各機關負責開發或管理之應用系統如有使用GCA或XCA憑證進行登入或操作，應於112年1月1日前完成新憑證驗證路徑設定，以確保使用者持新簽發之GCA或XCA憑證操作應用系統時能正常運作。



CA金鑰更換影響範圍

對應用系統及憑證用戶影響

對象	影響說明
憑證應用系統	1. 應用系統須新增第三代憑證驗證路徑及CRL或OCSP服務，未如期完成設定將導致應用系統無法順利驗證新的用戶憑證。 2. 憑證驗證路徑以及憑證廢止清冊載點之設定方式與現行運作之方式相同，**應用系統依照現行之設定方式進行新增設定即可**。 3. 憑證管理中心於GtestCA提供測試平台讓應用系統提前進行測試。
用戶	無影響

※本次CA金鑰更換因為僅更換金鑰長度，相關作業相對單純，且憑證安裝設定、驗證方式也與現行方式相同，應用系統依照現行系統設定方式進行即可。

憑證相關應用系統(舉例)

機關	應用系統
開發或維護電子公文交換平台之機關單位(ex 檔管局、金管會、教育部、經濟部)	電子公文交換系統
國家發展委員會檔案管理局	檔案管理系統
銓敘部	銓敘業務網路作業系統
國家發展委員會	我的E政府入口網
立法院	立法院質詢系統
法務部行政執行署	法務部行政執行署共同辦理健保費行政執行案件資料交換系統
司法院	法院囑託限制登記網路作業中心
監察院	監察院財產申報人職務異動通報平臺
內政部移民署	內政部移民署線上服務應用系統機關帳號管理
內政部移民署	內政部移民署公務員赴陸許可線上申請系統
勞動部勞工保險局	勞動部勞工保險局e化服務系統
中央健康保險署	中央健康保險署多憑證網路承保作業系統

憑證相關應用系統(舉例)

機關	應用系統
臺灣銀行	公教人員保險網路作業e系統
行政院公共工程委員會	政府電子採購網
交通部民用航空局	交通部民用航空局無人機管理資訊系統
內政部地政司	地政資訊網際網路系統管理
內政部地政司	內政部地籍存摺系統作業
臺北市政府	臺北市政府MyDoc電子文件服務平台
臺灣集中保管結算所	股東e票通電子投票平台
經濟部	公司負責人及主要股東資訊申報平臺
財政部	財政部電子發票整合服務平台
財政部關務署	商品資料倉儲系統
行政院人事行政總處	行政院人事行政總處「事求人機關徵才系統」
行政院人事行政總處	行政院人事行政總處人事服務網
內政部營建署	建築物公共安全檢查網路申報系統
中華郵政	中華郵政通訊地址遷移通報服務系統
行政院公共工程委員會	技師與工程技術顧問公司管理資訊系統

應用系統配合辦理事項

主要作業

1. 應用系統應於112年1月1日前，完成下述作業：
   - ✓ 取得GRCA、GCA及XCA第3代憑證，並進行憑證路徑設定
   - ✓ 取得GRCA第3代CA金鑰簽發之憑證機構廢止清冊(CARL)以及GCA與XCA第3代CA金鑰簽發之憑證廢止清冊(CRL)
   - ✓ 設定OCSP查詢服務URL(若應用系統有使用此查詢服務)

2. 第3代CA金鑰並未異動金鑰與簽章演算法，相關API或元件仍可持續支援，對憑證用戶不會產生影響

CA憑證相關資訊公布

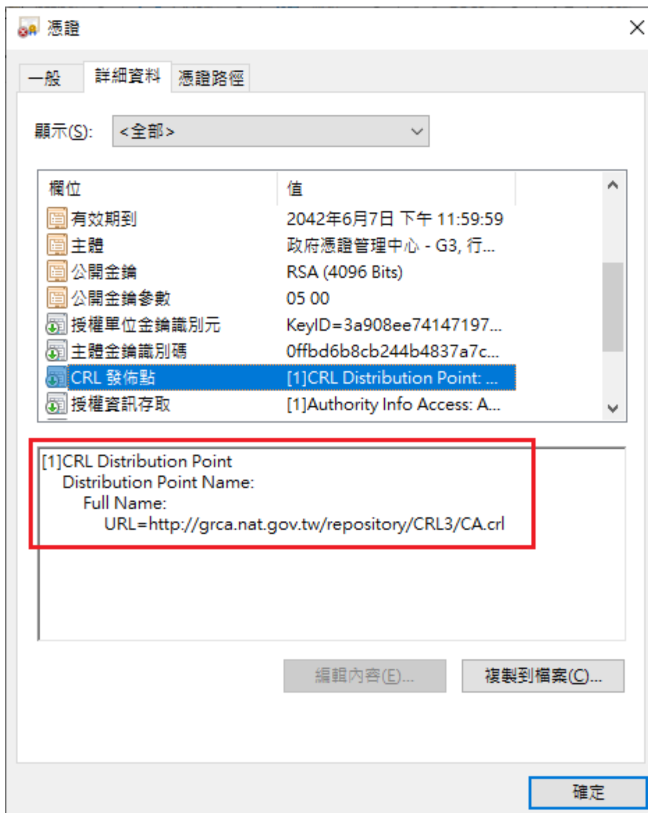
- **第三代GRCA憑證**
  - 憑證公布點：https://grca.nat.gov.tw/01-06.html
  - CARL載點：http://grca.nat.gov.tw/repository/CRL3/CA.crl
  - OCSP服務URL：http://ocsp.grca.nat.gov.tw/OCSP

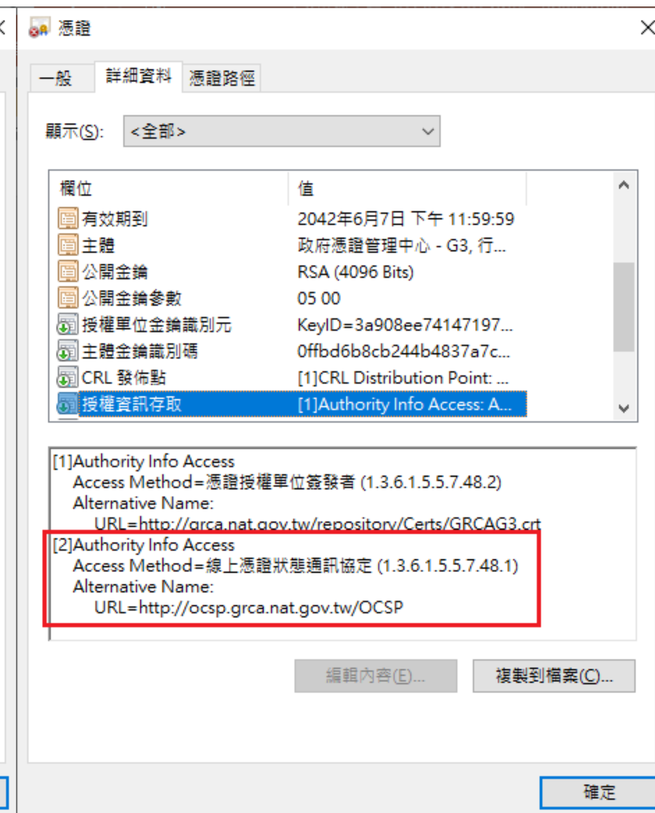
- **第三代GCA憑證**
  - 憑證公布點：https://grca.nat.gov.tw/01-05.html
  - CRL載點：http://gca.nat.gov.tw/repository/GCA/CRL3/complete.crl
  - OCSP服務URL：http://gca.nat.gov.tw/cgi-bin/OCSP3/ocsp_server

- **第三代XCA憑證**
  - 憑證公布點：https://grca.nat.gov.tw/01-05.html
  - CRL載點：http://xca.nat.gov.tw/repository/XCA/CRL3/complete.crl
  - OCSP服務URL：http://xca.nat.gov.tw/cgi-bin/OCSP3/ocsp_server

其他取得CA憑證相關資訊管道

- 日後可從第3代GCA(XCA)所簽發之用戶憑證IC卡匯出GRCA自簽憑證及其GCA(XCA)之CA憑證。
- 由用戶憑證及CA憑證中之CRL發佈點與授權資訊存取擴充欄位可查詢CRL/CARL載點及OCSP服務位址。





注意事項

1. 應用系統如有使用政府機關憑證(GCA憑證IC卡、非IC卡類憑證、專屬類憑證)或組織及團體憑證((XCA憑證IC卡、非IC卡類憑證)需要配合辦理。

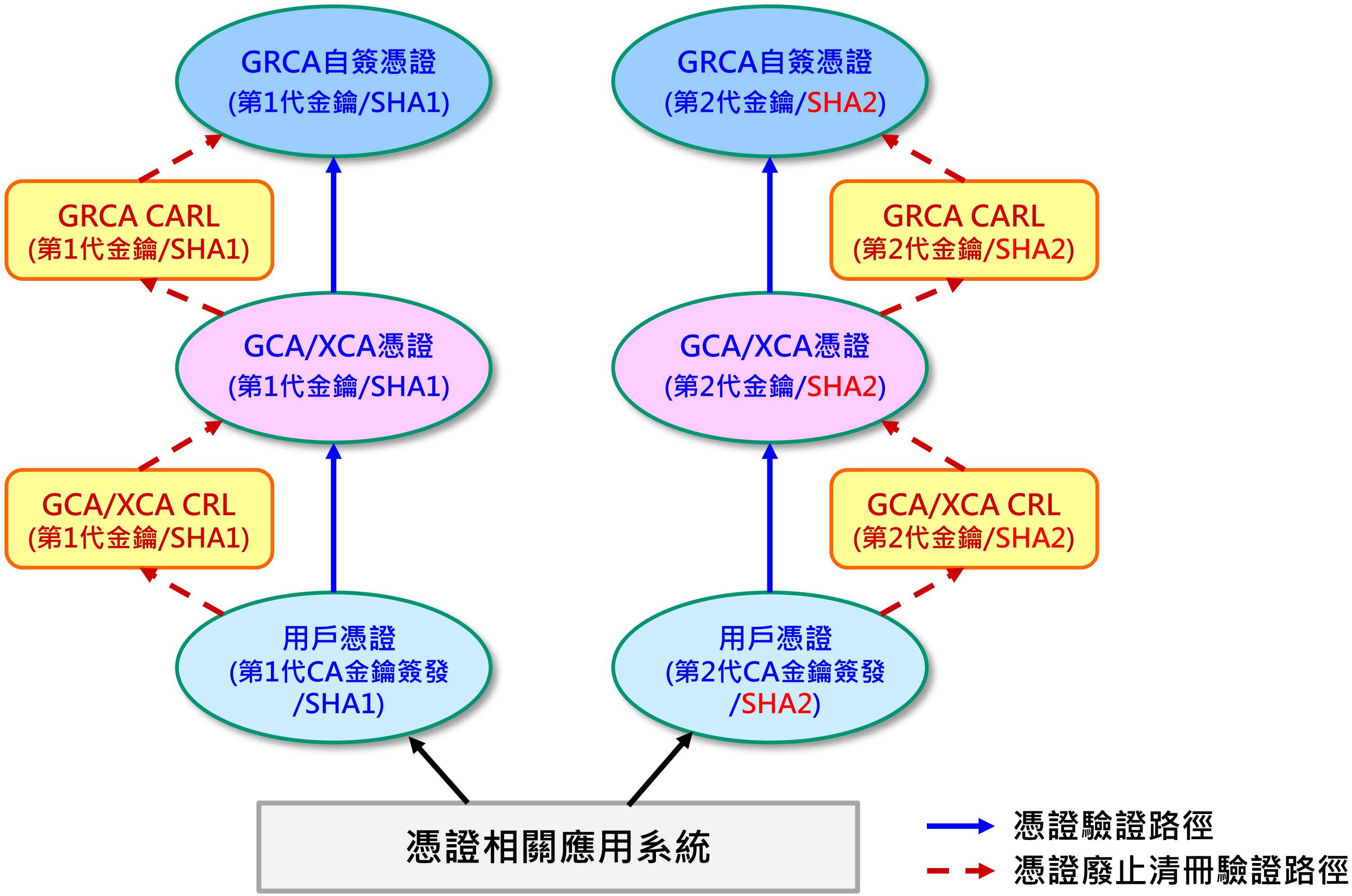
2. 目前政府網站之TLS憑證為GTLSCA所簽發之憑證，不在本次更新範圍，因此無須進行更新。

3. 第二代GCA及XCA之金鑰將於112年1月1日停止簽發用戶憑證(改由第三代GCA、XCA簽發)，但於112年1月1日之前所簽發之用戶憑證仍有效，用戶仍可持續使用至憑證到期為止，憑證驗證服務將須持續提供，故應用系統仍需保留第二代憑證驗證路徑，以利用戶可正常使用。

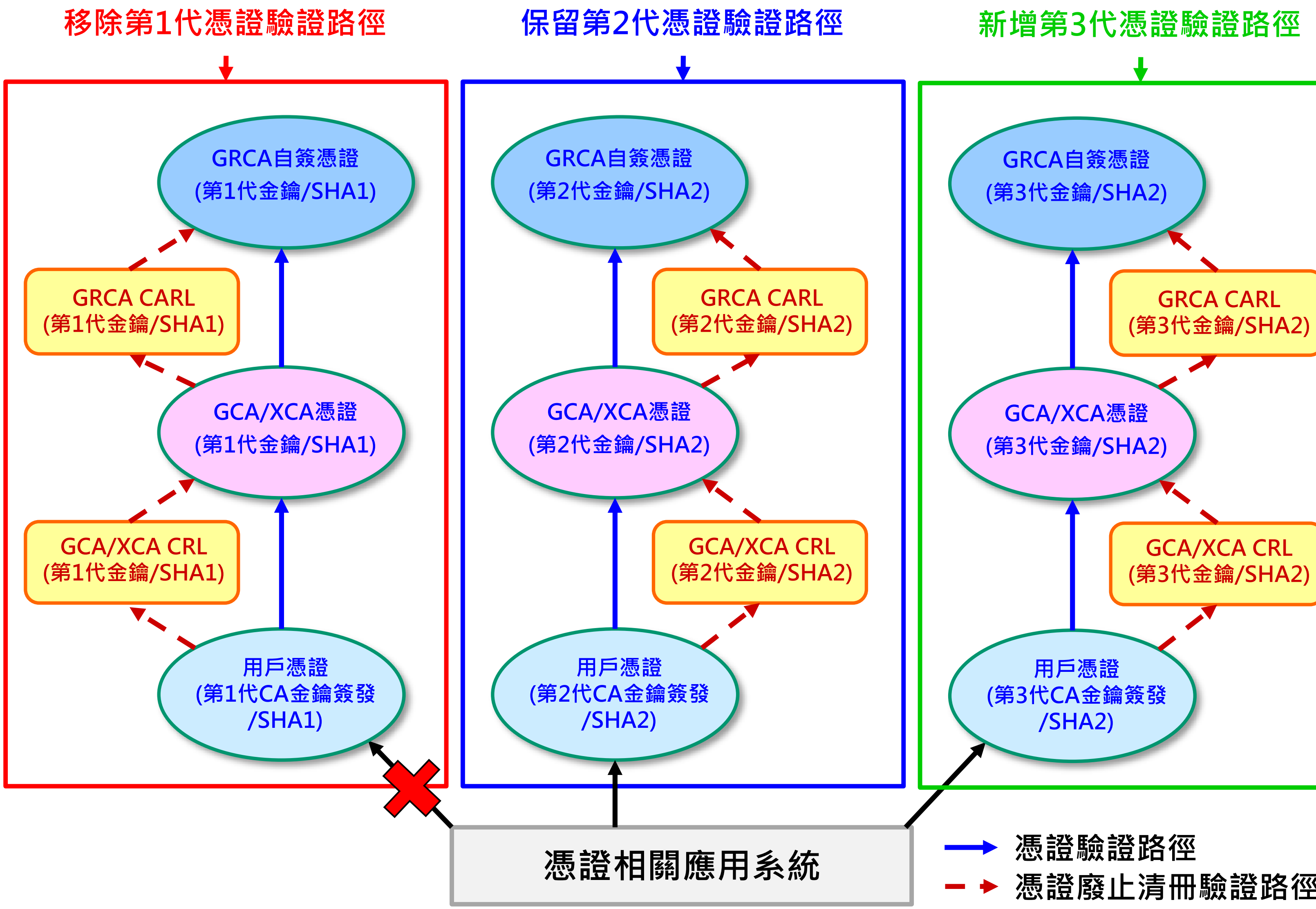
4. 本次CA金鑰更換不影響用戶憑證，用戶可持續使用手中的憑證直到憑證屆期。

新舊憑證驗證路徑說明

現行憑證驗證路徑


GRCA自簽憑證
(第1代金鑰/SHA1)
GRCA自簽憑證
(第2代金鑰/SHA2)
GRCA CARL
(第1代金鑰/SHA1)
GRCA CARL
(第2代金鑰/SHA2)
GCA/XCA憑證
(第1代金鑰/SHA1)
GCA/XCA憑證
(第2代金鑰/SHA2)
GCA/XCA CRL
(第1代金鑰/SHA1)
GCA/XCA CRL
(第2代金鑰/SHA2)
用戶憑證
(第1代CA金鑰簽發
/SHA1)
用戶憑證
(第2代CA金鑰簽發
/SHA2)
憑證相關應用系統
憑證驗證路徑
憑證廢止清冊驗證路徑

新增第三代CA金鑰後之憑證驗證路徑

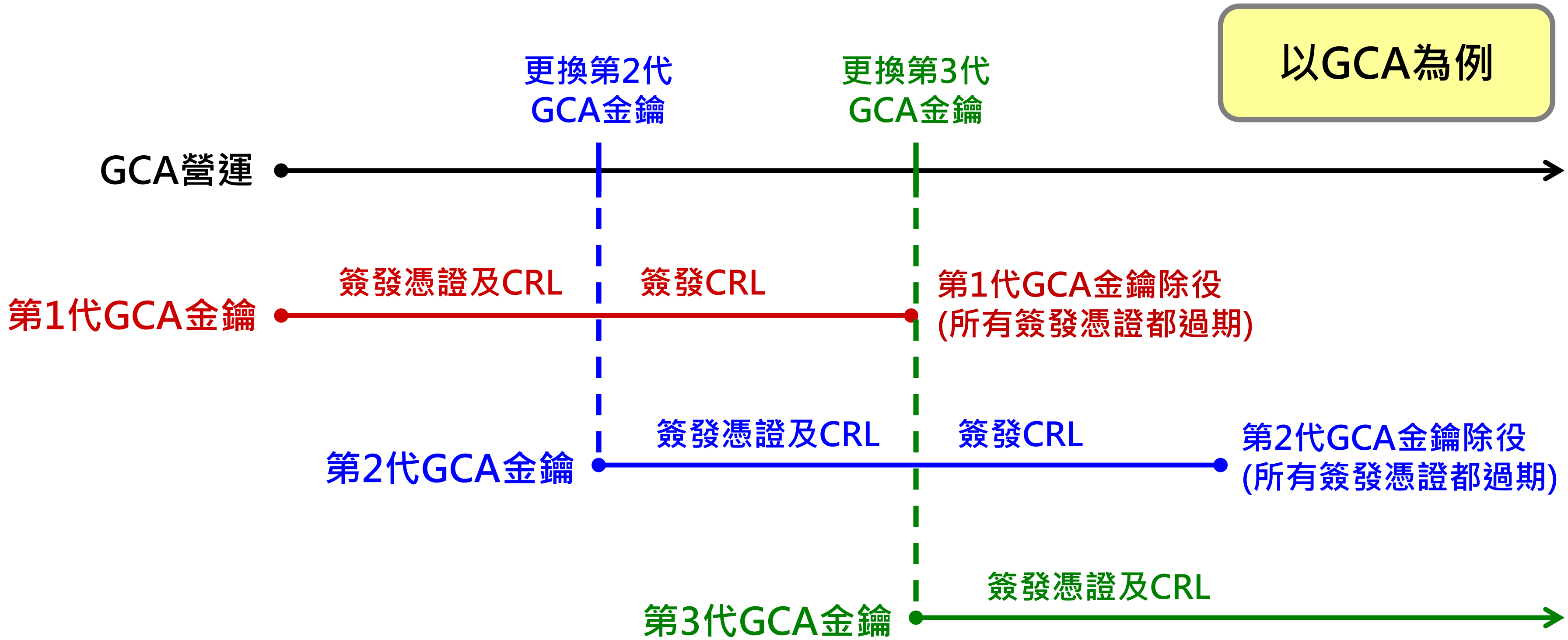


更換第3代CA金鑰後之用戶憑證驗證流程

- 取得用戶憑證後，先確認其簽發該憑證之下屬CA為何
- 使用HiSecure API或其他工具，建立憑證驗證路徑
  - 進行用戶憑證及其下屬CA之第2代與第3代CA憑證之匹配檢查
    - 比對CA憑證主體資訊與用戶憑證簽發者資訊是否相符
    - 比對CA憑證記載之主體金鑰識別元與用戶憑證記載之授權單位金鑰識別元是否相符
    - 使用CA憑證檢驗用戶憑證之簽章資訊
    - 檢驗憑證內之憑證保證等級、金鑰使用方法等資訊是否正確
  - 參考前述方式，確認下屬CA憑證所屬之GRCA憑證
- 驗證憑證路徑中所有憑證之狀態有效性
  - 檢驗CA憑證與用戶憑證之效期是否仍有效
  - 使用下屬CA提供之CRL或OCSP查詢服務驗證用戶憑證之狀態
  - 使用GRCA提供之CARL或OCSP查詢服務驗證CA憑證之狀態

更換第3代CA金鑰後之金鑰使用生命週期

- CA營運與其新舊金鑰運作週期關係
  - 第1代CA金鑰停止簽發CRL
  - 第2代CA金鑰停止簽發憑證，僅用於簽發CRL
  - 第3代CA金鑰開始簽發憑證及其CRL



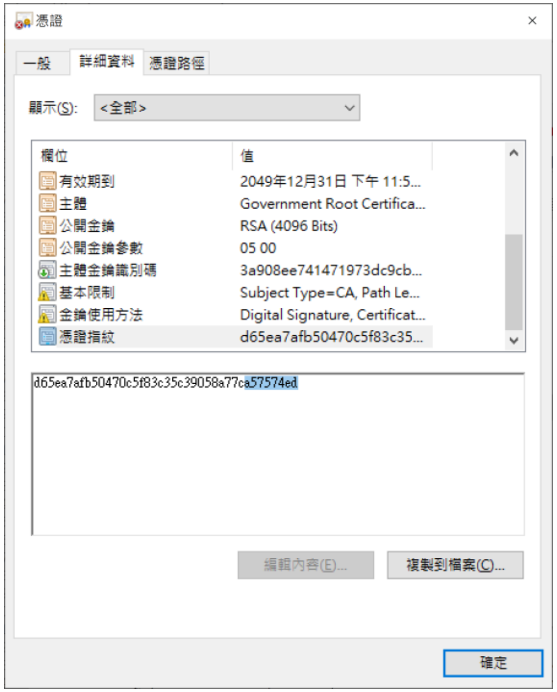
正確驗證憑證路徑之重要性

- 應用系統取得用戶憑證後，應建立其所屬之憑證路徑，並使用CRL或OCSP查詢服務，驗證憑證路徑所有憑證之有效性，若未正確驗證用戶憑證所屬憑證路徑。
  - 輕則憑證簽章驗證失敗(用戶無法登入或使用系統服務)
  - 重則該用戶憑證已廢止或停用，但仍驗為有效 (恐造成允許未授權用戶存取應用系統，造成系統資安漏洞)

- 正確驗證憑證之要點，可參考「公鑰憑證處理安全檢查表」。

第三代GPKI憑證資訊

- GRCA3
  - Base64末碼：7vo20rSy0=
  - 姆指紋末碼：a57574ed
- GCA3
  - Base64末碼：vzBmPLtw8=
  - 姆指紋末碼：df065ccb
- XCA3
  - Base64末碼：h6d5vUTQ==
  - 姆指紋末碼：59c74dcb



第一代GPKI憑證資訊

- GRCA1
  - Base64末碼：AlpYYsfPQS
  - 姆指紋末碼：882b40b9
- GCA1
  - Base64末碼：YGE9C7rg==
  - 姆指紋末碼：cb5112bb
- XCA1
  - Base64末碼：RJr1ZsI00=
  - 姆指紋末碼：c9797a00

公鑰憑證安全檢查表說明

使用憑證相關功能

功能分類	功能概述
資料加解密	對稱與非對稱
數位簽章與驗證	SHA256 with RSA / SHA256 with ECDSA
憑證資訊的取得	• 憑證序號 • 主體與簽發者DN • 主體與授權單位金鑰識別元 • 憑證效期 • 簽章演算法物件識別碼 • 主體別名 • 憑證政策 • CRL發佈點 • 授權資訊存取 • 主體目錄屬性資訊
憑證廢止驗證	CRL與OCSP

公鑰憑證處理安全檢查表介紹(1/3)

- 應用系統使用公鑰憑證處理之安全檢查表(參見附錄1)
  - 條列18項應用系統於處理憑證時應注意之基本安全事項
  - 應用系統上線前應逐項檢查，並確認皆符合後始可上線
- 憑證最重要的三個檢查項目
  - 憑證內之CA簽章值是否正確
  - 檢查憑證的時間(Validity)欄位是否仍在有效期限
  - 檢查憑證是否已被廢止(可藉由查詢CRL或是執行OCSP函式)
- 檢查方式
  - 由HiSecure API函式介面處理
    - CA憑證的檢驗
    - 用戶憑證的檢驗
  - 由AP端開發者處理

公鑰憑證處理安全檢查表介紹(2/3)

- 由HiSecure API函式介面處理
  - 系統需設定信賴的憑證保證等級(2)
  - 驗證憑證內簽章(3,9)
  - 檢驗憑證內之金鑰使用用途是否正確(4,10)
  - 檢驗憑證有效期限(5,11)
  - 使用CRL來驗證憑證廢止狀態(6,12)
  - 檢驗CRL是否為正確且最新的(7,8,13,14)
  - 對傳送之訊息加簽電子簽章以驗證用戶身份—Challenge and Response (15)

CA憑證與用戶憑證的檢驗

公鑰憑證處理安全檢查表介紹(3/3)

- 由AP開發者處理
  - 安全取得Root CA憑證(1)
  - 系統的設計應以Challenge-Response或是Nonce機制來防範重送攻擊(16)
  - 對用戶私密資料應以強度128bits以上的安全通道來保護(17)
  - 系統應定期校時，以確保系統時間之正確性(18)

GTestCA測試功能說明

GTestCA網站異動說明(1/3)

- 模擬GPKI更換第3代CA金鑰，新增GTestCA第5代CA金鑰及其CRL，並提供憑證申請、停用、復用及廢止等憑證申辦異動服務
- GTestCA第5代CA憑證與CRL可從儲存庫或下述連結取得
  - GTestRCA
    - 自簽憑證 http://gtestca.nat.gov.tw/repository/Certs/testGRCA5.cer
    - CARL http://gtestca.nat.gov.tw/repository/CRL5/CA.crl
  - GTestCA
    - 自身憑證 http://gtestca.nat.gov.tw/repository/Certs/testGTestCA5.cer
    - CRL http://gtestca.nat.gov.tw/crl/GTestCA5/complete.crl

GTestCA網站異動說明(2/3)

- GTestCA網站提供之憑證串鏈路徑
  - 第1代憑證串鏈：RSA+SHA1 (模擬GPKI第1代金鑰)
  - 第2代憑證串鏈：RSA+SHA256 (模擬GPKI第2代金鑰)
  - 第4代憑證串鏈：ECC+SHA384
  - 第5代憑證串鏈：RSA+SHA256 (模擬GPKI第3代金鑰) **新增**
- GTestCA第2代憑證串鏈與第5代憑證串鏈之差異
  - 第5代GTestCA所使用之CA金鑰長度升級為RSA 4096位元
  - 第5代GTestCA簽發之用戶憑證，其RSA金鑰長度可支援2048位元與3072位元(新增)

GTestCA網站異動說明(3/3)

■ 調整後之系統架構

原有憑證串鏈			新增憑證串鏈
第1代憑證串鏈 (模擬GPKI第1代金鑰)	第2代憑證串鏈 (模擬GPKI第2代金鑰)	第4代憑證串鏈	第5代憑證串鏈 (模擬GPKI第3代金鑰)
GTestRCA (RSA 4096+SHA1)	GTestRCA (RSA 4096+SHA256)	GTestRCA (ECC 384+SHA384)	GTestRCA (RSA 4096+SHA256)
GTestCA (RSA 2048+SHA1)	GTestCA (RSA 2048+SHA256)	GTestCA (ECC 384+SHA384)	GTestCA (RSA 4096+SHA256)
用戶憑證 (RSA 1024+SHA1) (RSA 2048+SHA1)	用戶憑證 (RSA 1024+SHA256) (RSA 2048+SHA256)	用戶憑證 (ECC 384+SHA384)	用戶憑證 (RSA 2048+SHA256) (RSA 3072+SHA256)

GTestCA網站操作說明-前置作業(1/2)

- 安裝跨平台網頁元件
  - 此元件用於支援IC卡類載具於IE、Chrome及Firefox等瀏覽器進行憑證申請、廢止、停用/復用以及IC卡相關作業
  - 安裝說明
    - 安裝時機
      - 第一次使用GTestCA網站進行IC卡類憑證作業或IC卡相關作業前
    - 下載位置
      - 跨平台網頁元件下載頁面 https://api-hisecurecdn.cdn.hinet.net/HiPKILocalSignServer/downloadMain.html
      - GTestCA網站儲存庫→跨平台網頁元件
    - 注意事項
      - 安裝完成後以及進行IC卡類憑證相關作業與IC卡相關作業前，建議執行IC卡元件自我檢測(http://localhost:61161/selfTest.htm)，確認IC卡、讀卡機和跨平台網頁元件等狀態皆正常

GTestCA網站操作說明-前置作業(2/2)

■ IC卡元件自我檢測成功畫面(參考)

IC卡功能檢測		
檢測項目	結果	檢測內容
1.瀏覽器版本	V	Chrome 51.0.2704.103
2.已安裝元件版本	V	1.3.4.b5
3.已安裝子元件版本	V	ListInfo.exe:2.0.2 HiPKISign.exe:2.0.1 HiPKIDecrypt.exe:2.0.1
4.PKCS#11版本資訊	V	HiCOS PKI Smart Card P#11 3.0.0, ver 3
5.選擇讀卡機及卡片	V	CASTLES EZ100PU 0 卡號:[Test0000RSA2330t] ▼
6.輸入PIN碼並開始檢測	V	········· 開始檢測
7.簽章驗證測試	V	簽章驗證功能成功
8.簽章憑證資訊	V	憑證主體:C=TW,CN=測試自然人 1,serialNumber=3758105775101612 憑證序號:7469456DBE7E435AA32E772BCC9A111B 憑證效期:自2016年7月13日 至 2017年1月13日 金鑰用途:digitalSignature
9.加密憑證資訊	V	憑證主體:C=TW,CN=測試自然人 1,serialNumber=4678625552083968 憑證序號:44F1E8DE5682B5E88184EABBC129851E 憑證效期:自2016年7月13日 至 2017年1月13日 金鑰用途:keyEncipherment|dataEncipherment
重新開始檢測		重新開始檢測

GTestCA網站操作說明-憑證申請(1/4)

- 可選取之CA金鑰與簽章演算法
  - 第1代CA金鑰(RSA金鑰)+SHA1WithRSA
  - 第2代CA金鑰(RSA金鑰)+SHA256WithRSA
  - 第4代CA金鑰(ECC金鑰)+SHA384WithECDSA
  - 第5代CA金鑰(RSA金鑰)+SHA256WithRSA
- 可簽發之測試憑證類別

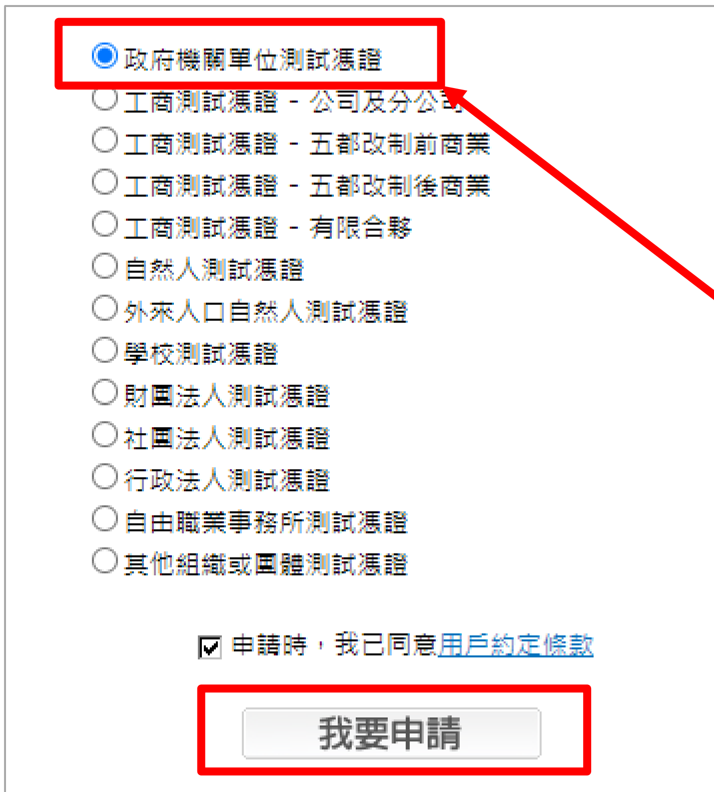
IC卡類憑證	非IC卡類憑證	伺服器應用軟體類憑證
• 政府機關單位憑證	• 政府機關單位憑證	• 伺服器應用軟體憑證(SSL類)
• 工商憑證(公司及分公司)	• 工商憑證(公司及分公司)	• 伺服器應用軟體憑證(專屬類)
• 工商憑證(五都改制前商業)	• 工商憑證(五都改制前商業)	
• 工商憑證(五都改制後商業)	• 工商憑證(五都改制後商業)	
• 工商憑證(有限合夥)	• 一站式專屬授權憑證(公司)	
• 自然人憑證	• 一站式專屬授權憑證(商業)	
• 外來人口自然人憑證	• 一站式專屬授權憑證(有限合夥)	
• 學校憑證	• 財團法人憑證	
• 財團法人憑證	• 自由職業事務所憑證	
• 社團法人憑證		
• 行政法人憑證		
• 自由職業事務所憑證		
• 其他組織或團體憑證		

GTestCA網站操作說明-憑證申請(2/4)

- **以申請IC卡類政府機關單位測試憑證為例**
  - 選取「我要申請IC卡類憑證」

GTestCA網站操作說明-憑證申請(3/4)

- 以申請<u>IC卡類政府機關單位測試憑證</u>為例(續)
  - 選取欲申請的測試憑證，並點選「我要申請」



GTestCA網站操作說明-憑證申請(4/4)

- **以申請IC卡類政府機關單位測試憑證為例(續)**
  - 進入申請資料填寫頁面後，選取【讀卡機及卡片】以及欲使用的【CA金鑰與簽章演算法】，填妥憑證申請所需之資料，並點選【憑證申請】，即可進行憑證申請作業

GTestCA網站操作說明-憑證廢止(1/4)

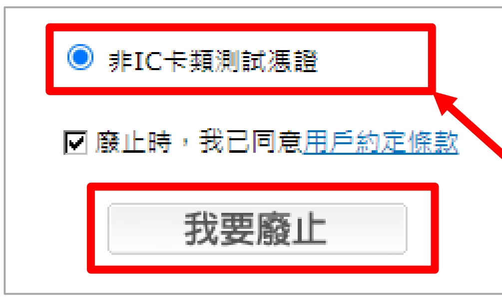
- 各憑證皆依其所屬之憑證類別進行廢止，例如：
  - 廢止IC卡類政府機關單位憑證，請選取【我要廢止IC卡類憑證】
  - 廢止非IC卡類財團法人憑證，請選取【我要廢止非IC卡類憑證】
  - 廢止伺服器應用軟體類憑證(專屬類)，請選取【我要廢止伺服器應用軟體類憑證】
- 憑證廢止事前準備
  - 廢止IC卡類憑證時，請備妥欲進行廢止作業的憑證IC卡
  - 廢止非IC卡類憑證與伺服器應用軟體類憑證時，請備妥欲進行廢止作業的憑證檔案

GTestCA網站操作說明-憑證廢止(2/4)

- **以廢止非IC卡類財團法人測試憑證為例**
  - 選取「我要廢止非IC卡類憑證」

GTestCA網站操作說明-憑證廢止(3/4)

- **以廢止非IC卡類財團法人測試憑證為例(續)**
  - 選取非IC卡類測試憑證，
    並點選「我要廢止」



GTestCA網站操作說明-憑證廢止(4/4)

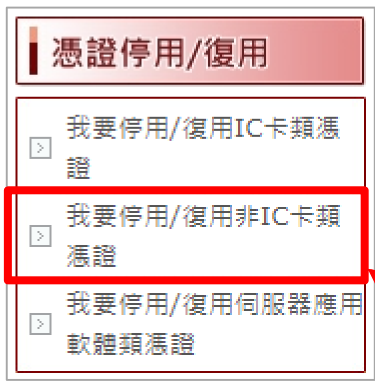
- **以廢止非IC卡類財團法人測試憑證為例(續)**
  - 進入廢止憑證頁面後，選取欲廢止的憑證檔案以及憑證廢止原因後，點選【廢止憑證】，即可進行憑證廢止作業

GTestCA網站操作說明-憑證停/復用(1/4)

- 各憑證皆依其所屬之憑證類別進行停用/復用，例如：
  - 停用/復用IC卡類政府機關單位憑證，請選取【我要停用/復用IC卡類憑證】
  - 停用/復用非IC卡類財團法人憑證，請選取【我要停用/復用非IC卡類憑證】
  - 停用/復用伺服器應用軟體類憑證(專屬類)，請選取【我要停用/復用伺服器應用軟體類憑證】
- 憑證停用/復用事前準備
  - 停用/復用IC卡類憑證時，請備妥欲進行停用/復用作業的憑證IC卡
  - 停用/復用非IC卡類憑證與伺服器應用軟體類憑證時，請備妥欲進行停用/復用作業的憑證檔案

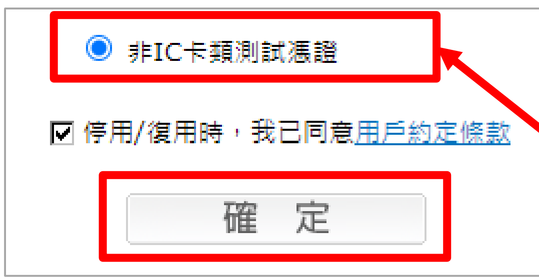
GTestCA網站操作說明-憑證停/復用(2/4)

- 以停用/復用非IC卡類財團法人測試憑證為例
  - 選取「我要停用/復用IC卡類憑證」



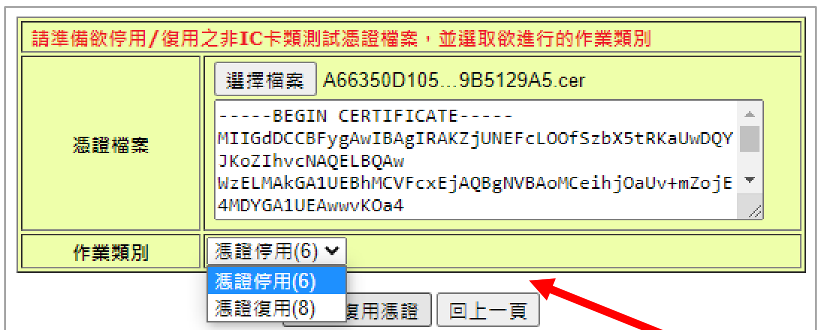
GTestCA網站操作說明-憑證停/復用(3/4)

- **以停用/復用非IC卡類財團法人測試憑證為例(續)**
  - 選取非IC卡類測試憑證，並點選「確定」



GTestCA網站操作說明-憑證停/復用(4/4)

- 以停用/復用非IC卡類財團法人測試憑證為例(續)
  - 進入停用/復用憑證頁面後，選取欲停用/復用的憑證檔案以及欲執行的作業類別，點選【停用/復用憑證】，即可進行憑證停用/復用作業



宣導事項

配合組織調整之更改

- 本憑證管理中心之業務將於111年8月27日由國家發展委員會移轉至數位發展部，憑證相關申請及公文書請改送至數位發展部。

報告完畢
謝謝指教

客服專線 02-21927111
客服信箱 egov@service.gov.tw

附錄1、應用系統使用公鑰憑證處理之安全檢查表

公鑰憑證處理安全檢查表項目(1/5)

項次	安全檢查項目
1	系統應由安全管道取得Root CA的自簽憑證(Self-Signed Certificate)，並妥善安全保存於系統中
2	系統應設定所信賴的憑證保證等級，並檢查憑證之憑證政策(Certificate Policies)欄位所記載的Policy OID是否符合憑證保證等級的要求，對於不符保證等級之憑證應拒絕存取(例如正式上線系統應對測試等級的憑證加以拒絕)
3	系統應檢查CA本身憑證確為Root CA所簽發的憑證 (至少需檢查憑證的Issuer Name (DN)是否與Root CA自簽憑證的Subject Name(DN)相符，並以Root CA自簽憑證所記載的Public Key檢驗CA本身憑證的簽章)
4	系統應檢查CA本身憑證確實為合法的CA憑證(Basic Constraints欄位標示為CA憑證)，且憑證之金鑰用途(KeyUsage)欄位允許keyCerSign及cRLSign的用途

公鑰憑證處理安全檢查表項目(2/5)

項次	安全檢查項目
5	系統應檢查CA本身憑證是否在效期內(例如檢查系統時間是否仍落在憑證所記載的validity時間範圍內) 注意：憑證是以世界標準時間(UTC，或稱格林威治時間)來記載Validity時間範圍，因此系統不應拿本地時間(Local Time)直接與憑證Validity時間範圍相比較
6	系統應檢查CA本身憑證是否已被廢止(例如定期下載Root CA簽發的憑證機構廢止清冊(CARL)檢查憑證廢止狀態)
7	系統應檢查CARL是否確實是Root CA所簽發(至少需檢查CARL的Issuer Name (DN)是否與Root CA自簽憑證的Subject Name(DN)相符，並以Root CA自簽憑證所記載的Public Key檢驗CARL的簽章)
8	系統應檢查是否為最新的CARL(當天公布的CARL) 注意：CARL的更新時間是以世界標準時間來記載，因此系統不應拿本地時間直接與CARL的更新時間相比較

公鑰憑證處理安全檢查表項目(3/5)

項次	安全檢查項目
9	系統應檢查用戶的憑證為合法CA所簽發(至少需檢查用戶憑證的Issuer Name (DN)是否與CA憑證的Subject Name(DN)相符，並以CA憑證所記載的Public Key檢驗用戶憑證的簽章)
10	系統應檢查用戶憑證金鑰用途(KeyUsage)欄位所記載的金鑰用途符合使用目的(簽章/驗簽，或加密/解密)
11	系統應檢查用戶的憑證是否在效期內(例如檢查系統時間是否仍落在憑證所記載的validity時間範圍內) 注意：憑證是以世界標準時間來記載，因此系統不應拿本地時間直接與憑證Validity時間範圍相比較
12	系統應檢查用戶的憑證是否已被廢止(例如定期下載CA簽發的憑證廢止清冊(CRL)檢查憑證廢止狀態，或透過OCSP來檢查憑證廢止狀態)

公鑰憑證處理安全檢查表項目(4/5)

項次	安全檢查項目
13	系統應檢查CRL是合法CA所簽發(至少需檢查CRL的Issuer Name (DN)是否與CA本身憑證的Subject Name(DN)相符，並以CA本身憑證所記載的Public Key檢驗CRL的簽章)，如果使用OCSP查詢，則本項不適用
14	系統應檢查是否為最新公佈的CRL(當天公布的CRL)，如果使用OCSP查詢，則本項不適用 注意：CRL的更新時間是以世界標準時間來記載，因此系統不應拿本地時間直接與CRL的更新時間相比較
15	系統應要求用戶對傳送的訊息加簽電子簽章以驗證用戶身分
16	系統應具備防止用戶加簽之訊息遭到非法重送(Replay)之功能(例如在加簽訊息中加入Challenge-Response或Nonce機制)

公鑰憑證處理安全檢查表項目(5/5)

項次	安全檢查項目
17	系統傳送用戶隱私資料時應以強度128 bits以上的安全通道進行保護(例如使用SSL安全通道或是對傳送的訊息以數位信封加密)，若系統未涉及傳送用戶隱私資料時，則本項不適用
18	系統應定期校時，以保持系統時間之正確性(例如定期透過NTP自動校時)

資料來源：XCA網站提供之公鑰憑證安全檢查表 (https://xca.nat.gov.tw/data/AP_CHECKLIST.pdf)