GRCA、GCA及XCA第三代憑證路徑安裝及設定說明

國家發展委員會111年7月

一、緣起

本會所轄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)已依照相關規範進行金鑰對更換，並提升GCA及XCA第三代金鑰對至RSA 4096 bits，以加強金鑰之安全強度。

本會將於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111年12月31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。

二、使用GCA、XCA憑證之應用系統範圍

因使用憑證之應用系統繁多，各機關仍須盤點所開發或管理之系統是否有使用GCA或XCA憑證，本會列舉部分系統如下:

機關	應用系統
各機關	電子公文交換系統
立法院	立法院質詢系統
司法院	法院囑託限制登記網路作業中心
考試院銓敘部	銓敘業務網路作業系統
監察院	監察院財產申報人職務異動通報平臺
行政院人事行政總處	「事求人機關徵才系統」登錄徵才公告系統
行政院人事行政總處	人事服務網
行政院公共工程委員會	政府電子採購網
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
國家發展委員會	我的E政府入口網
國家發展委員會檔案管理局	檔案管理系統
內政部營建署	建築物公共安全檢查網路申報系統
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	公務員赴陸許可線上申請系統
內政部地政司	地政資訊網際網路系統管理
內政部地政司	地籍存摺系統作業
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
交通部民用航空局	無人機管理資訊系統
勞動部勞工保險局	e 化服務系統
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
衛生福利部中央健康保險署	多憑證網路承保作業系統
臺北市政府	臺北市政府 MyDoc 電子文件服務平台
中華郵政	中華郵政通訊地址遷移通報服務系統
臺灣銀行	公教人員保險網路作業 e 系統
臺灣集中保管結算所	股東 e 票通電子投票平台

三、GCA、XCA 更換金鑰之影響及對應說明:

本次金鑰更換，因演算法仍為 RSA，且 API 及憑證元件皆未更動，因此對於憑證用戶不會造成影響，憑證相關應用系統僅需完成新憑證驗證路徑設定即可，主要作業項目如下:

1.下載第三代 GRCA、GCA 或 XCA 憑證進行安裝設定。

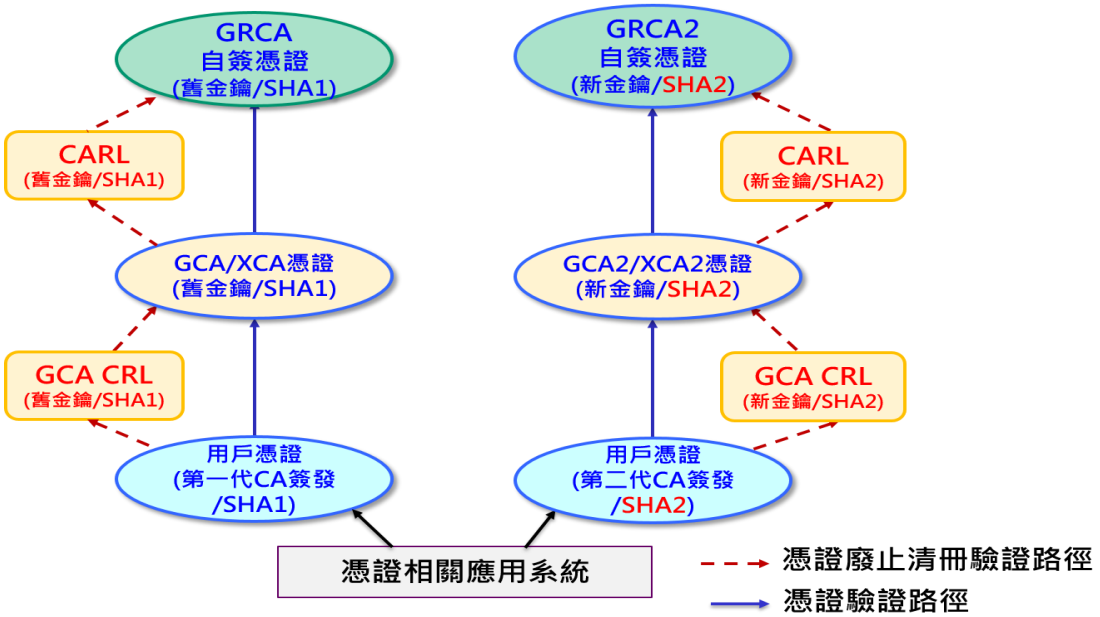
2.新增下載新的憑證機構憑證廢止清冊(CARL)及憑證廢止清冊(CRL)。

3.應用系統若使用 OCSP 服務進行憑證狀態驗證，則需設定新的 OCSP 服務連結。

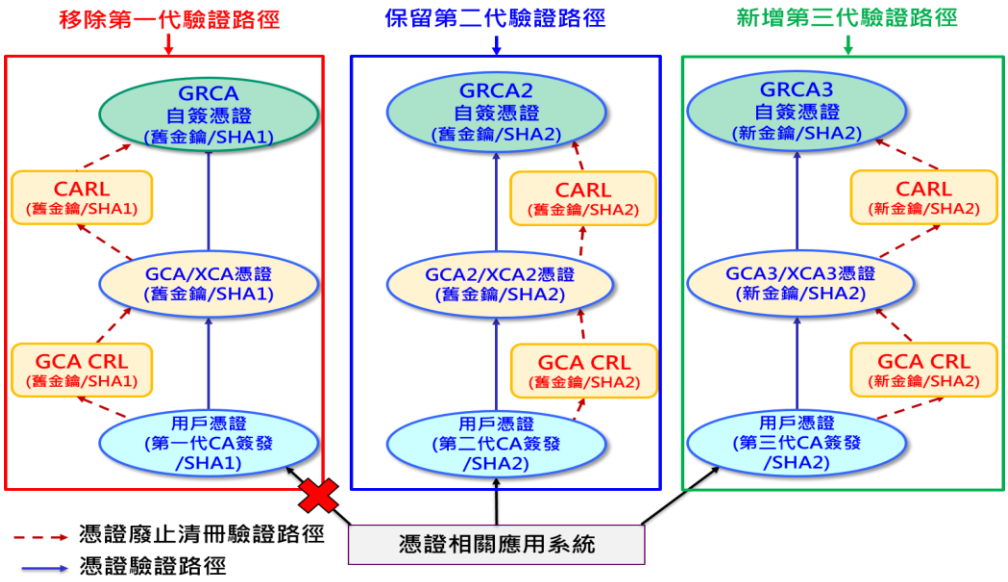
四、第三代憑證驗證路徑設定說明:

(一)現行憑證驗證路徑說明

現行憑證相關應用系統設定之憑證驗證路徑如下圖所示，應用系統會先判別用戶憑證是由第一代 CA 簽發或第二代 CA 簽發，藉此決定憑證驗證路徑。



(二)第三代 CA 憑證啟用後之憑證驗證路徑說明



1.移除第一代憑證驗證路徑

目前第一代 GCA 及 XCA 所簽發之用戶憑證已全數屆期，因此應用系統應移除此路徑相關設定。

2.保留第二代憑證驗證路徑

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，但由於之前所簽發之用戶憑證仍有效，因此將持續提供憑證驗證服務，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。

3.新增第三代憑證驗證路徑

第三代 GCA 及 XCA 金鑰於112年1月1日開始簽發用戶憑證，請應用系統提前於111年12月31日前新增第三代憑證驗證路徑。

(三)第三代 CA 憑證安裝及設定說明

第三代 GRCA、GCA 及 XCA 憑證已簽發並公告於憑證管理中心官方網站，各機關可自行下載取得憑證，相關資訊載點如下：

1.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

2.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

3.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

(四) 測試憑證平臺

各機關如有測試需要，可自政府憑證測試管理中心(以下簡稱 GTestCA)網站之「儲存庫」(https://gtestc.nat.gov.tw)下載 GTestCA 第五代憑證，並申請測試憑證進行憑證路徑驗證、憑證廢止清冊下載等功能。

測試憑證申請網址如下:

- IC 卡類測試憑證
  (https://gtestca.nat.gov.tw/03-01.html)
- 非 IC 卡類測試憑證
  (https://gtestca.nat.gov.tw/03-02.html)
- 伺服器應用軟體類憑證
  (https://gtestca.nat.gov.tw/03-03.html)