

檔 號：

保存年限：

教育部 函

機關地址：100217 臺北市中正區中山南路5號

承辦人：陳淑雅

電話：(02)77129037

電子信箱：csy0131@mail.moe.gov.tw

受文者：國立聯合大學

發文日期：中華民國111年8月9日

發文字號：臺教資(五)字第1110076412號

速別：普通件

密等及解密條件或保密期限：

附件：原函、GCA及XCA第三代憑證路徑安裝及設定說明 (附件一

d9d7231723ab7e7c99299a6e0f472736_A09000000E_1110076412_senddoc1_
Attach1.PDF、附件二 d9d7231723ab7e7c99299a6e0f472736_A09000000E_
1110076412_senddoc1_Attach2.pdf)

主旨：請於111年12月31日前完成GCA(XCA)第三代憑證驗證路
徑安裝及相關設定，詳如說明，請查照。

說明：

- 一、依據國家發展委員會111年8月2日發資字第1111501246號
函辦理。
- 二、政府憑證總管理中心(以下簡稱GRCA)、政府憑證管理中
心(以下簡稱GCA)、組織及團體憑證管理中心(以下簡稱
XCA)，私密金鑰使用期限即將屆期，國家發展委員會已
產製第三代金鑰，並提升GCA及XCA金鑰長度至RSA
4096 bits，以加強金鑰之安全強度。
- 三、112年1月1日起，GCA及XCA將以第三代金鑰簽發用戶憑
證，貴機關(校)開發或維運之應用系統如有使用GCA或
XCA簽發之憑證，請配合於111年12月31日前完成第三代
憑證驗證路徑安裝及相關設定，以確保使用者持新簽發
之憑證操作應用系統時能正常運作。
- 四、有關憑證驗證路徑安裝及相關設定，說明如下(詳細說明



訂

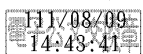
線

如附件)：

- (一)至GRCA網站(<https://grca.nat.gov.tw/01-06.html>及<https://grca.nat.gov.tw/01-05.html>)下載新的GRCA、GCA、XCA第三代憑證，進行安裝設定。
- (二)依應用系統之憑證驗證方式新增新的CRL及CARL，或設定新的OCSP服務(載點詳附件)。
- (三)國家發展委員會已提供憑證測試平臺環境，貴機關如有測試需要，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。

五、如有任何問題請洽電子化政府基礎建設客戶服務中心(電話：(02)21927111；Email：egov@service.gov.tw)。

正本：部屬機關(構)及國家運動訓練中心(教育部國民及學前教育署除外)、各公私立大專校院、各國立大學附設醫院及農林場、本部各駐境外機構(含派駐人員)(駐大阪辦事處派駐人員、駐福岡辦事處派駐人員除外)、大陸臺商子弟學校與海外臺灣學校、財團法人法鼓山文教基金會、財團法人普仁青年關懷基金會、財團法人體育運動發展促進基金會、財團法人高等教育評鑑中心基金會、財團法人海崇文教基金會、財團法人中華運動禁藥防制基金會、財團法人高等教育國際合作基金會、技專校院招生委員會聯合會、財團法人嘉新兆福文化基金會、技專校院招生策略委員會、身心障礙學生升學大專校院甄試委員會、財團法人人本教育文教基金會、財團法人中華民國私立學校教職員退休撫卹離職資遣儲金管理委員會、財團法人技專校院入學測驗中心基金會、財團法人唐獎教育基金會、財團法人林堉璘宏泰教育基金會、財團法人崇友文教基金會、財團法人台灣省中小學校教職員福利文教基金會、財團法人新台灣人文教基金會、社團法人中華民國大專校院資訊服務協會、財團法人創新智庫暨企業大學基金會台南辦公室、財團法人大學入學考試中心基金會、財團法人中鼎教育基金會、財團法人佳音教育基金會、財團法人周大觀文教基金會、財團法人仰望教育基金會、財團法人民間公民與法治教育基金會、財團法人歐都納戶外體育基金會、財團法人立賢教育基金會、財團法人信誼基金會、財團法人中華勞資關係研究所、財團法人台灣發展研究院、財團法人彭婉如文教基金會、財團法人味丹文教基金會

副本：



國家發展委員會 函

地址：100223 臺北市中正區寶慶路3號
承辦人：周佑穎
電話：(02)23165300分機6821
傳真：(02)23942165
電子信箱：timothyzhou@ndc.gov.tw

受文者：教育部

發文日期：中華民國111年8月2日
發文字號：發資字第1111501246號
速別：普通件
密等及解密條件或保密期限：

附件：GRCA、GCA及XCA第三代憑證路徑安裝及設定說明（GRCA、GCA及XCA第三代憑證路徑安裝及設定說明.pdf）

主旨：貴機關如有使用GCA或XCA憑證之應用系統，請於111年12月31日前完成第三代憑證驗證路徑安裝及相關設定，詳如說明，請查照並轉知所屬。

說明：

- 一、政府憑證總管理中心(以下簡稱GRCA)、政府憑證管理中心(以下簡稱GCA)、組織及團體憑證管理中心(以下簡稱XCA)，私密金鑰使用期限即將屆期，本會已產製第三代金鑰，並提升GCA及XCA金鑰長度至RSA 4096 bits，以加強金鑰之安全強度。
- 二、112年1月1日起，GCA及XCA將以第三代金鑰簽發用戶憑證，貴機關開發或維運之應用系統如有使用GCA或XCA簽發之憑證，請配合於111年12月31日前完成第三代憑證驗證路徑安裝及相關設定，以確保使用者持新簽發之憑證操作應用系統時能正常運作。
- 三、有關憑證驗證路徑安裝及相關設定，說明如下(詳細說明如附件)：



(一)至GRCA網站(<https://grca.nat.gov.tw/01-06.html>及
<https://grca.nat.gov.tw/01-05.html>)下載新的GRCA、
GCA、XCA第三代憑證，進行安裝設定。

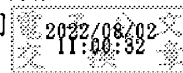
(二)依應用系統之憑證驗證方式新增新的CRL及CARL，或設定
新的OCSP服務(載點詳附件)。

(三)本會已提供憑證測試平臺環境，貴機關如有測試需要，
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。

四、如有任何問題請洽電子化政府基礎建設客戶服務中心(電
話：(02)21927111；Email：egov@service.gov.tw)。

正本：總統府、立法院、司法院、監察院、考試院、行政院各部會行總處署(台灣美國
事務委員會除外)、各直轄市政府、各縣市政府、各縣市議會

副本：本會資訊管理處、中華電信股份有限公司資訊技術分公司



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：

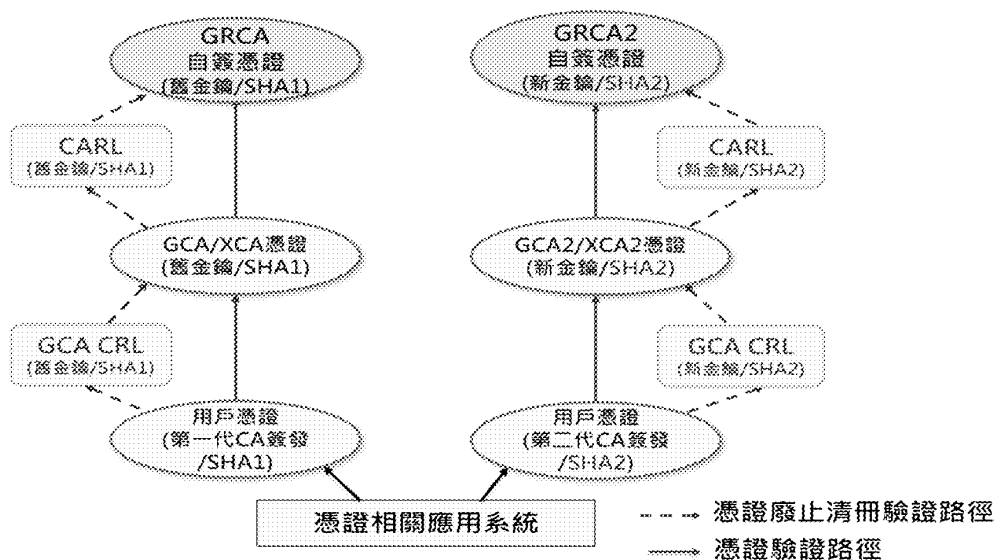
1. 下載第三代 GRCA、GCA 或 XCA 憑證進行安裝設定。
2. 新增下載新的憑證機構憑證廢止清冊(CARL)及憑證廢止清冊(CRL)。
3. 應用系統若使用 OCSP 服務進行憑證狀態驗證，則需設定新的 OCSP 服務連結。



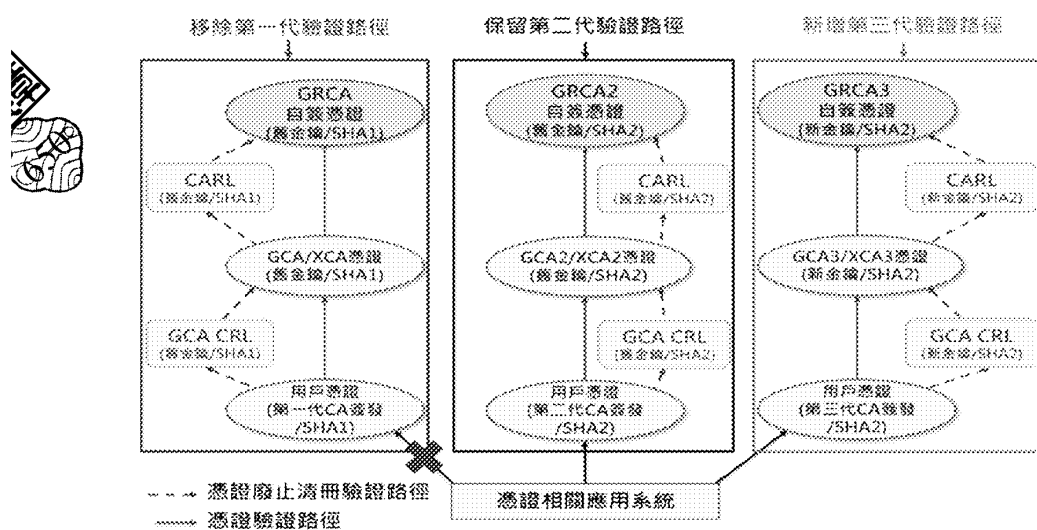
四、第三代憑證驗證路徑設定說明：

(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>)

