政府憑證入口網(GCP)　Q&A

一、GCA 憑證申辦問題

Q1：如何申請 GCA 憑證?

A：

1.請至「憑證申請」選取所需申辦項目填寫申請書。

2.填寫完申請書後將申請資料上傳申請並列印申請書。

3.將申請書連同公文函送至數位發展部。地址:100 臺北市中正區延平南路 143 號。請多利用公文電子交換方式申請。

Q2：GCA 憑證 IC 卡申請流程步驟?

A：請參考 GCA 申請流程。

Q3：請問如何得知憑證是否已經申請成功?及如何查詢憑證申請狀態?

A：於填寫憑證 IC 卡申請書後，會出現一組案件流水號，另點選列印申請書，系統會主動 mail 寄送申請書至申請時所填寫的聯絡人信箱。

憑證申請狀態可透過「憑證申請」→「申請狀態查詢」查詢憑證申辦進度。

Q4：申請政府憑證 IC 卡是否有限制張數?

A：同一政府機關、單位憑證 IC 卡，正卡僅可申請一張，附卡可按實際需求酌量申請。由於目前申請 GCA 憑證尚不需負擔費用，而係由數位發展部統籌支應，基於政府資源有限及當有效運用，各政府機關單位於申請憑證時應視實際需要提出，避免資源浪費，數位發展部於受理憑證申請時，保有審核憑證發放數量之權利。

Q5：是否可同時申請多張憑證 IC 卡?

A：1 張「憑證 IC 卡申請書」只能申請 1 張 IC 卡片。若需要 3 張憑證 IC 卡，請填寫 3 張申請書，但同一機關單位同時申請多張憑證 IC 卡，可合併於同一份公文下提出申請，公文請註明申請憑證 IC 卡之用途、申請卡別為正卡或附卡及申請張數，以利複審作業進行。

Q6：憑證申請書需要蓋關防嗎?

A：GCA 政府機關單位之憑證申請書不需要蓋關防，但憑證申請書必須隨公文函送數位發展部。

Q7：填寫完申請書發現有資料填寫錯誤怎麼辦?

A：申請書填寫有誤請至「憑證申請」→「申請書修改及補列印」之功能修改錯誤資料，重新上傳並列印。

Q8：請問何謂「政府單位憑證的併案申請服務」?

A：原本新設政府單位時，需要先發文申請單位物件識別碼(OID)與建立單位目錄服務資料，於政府憑證管理中心編訂單位物件識別碼(OID)後，再發文申請單位憑證 IC 卡。 為簡化行政作業並提供更便利之服務，於民國 100 年初新增政府單位憑證的併案申請服務，以利新設立之政府單位用戶可同時來函申請單位物件識別碼(OID)和政府單位憑證 IC 卡，減少一次的發文，縮短行政作業時間。

二、TLS 憑證相關問題

Q1：是否可以申請萬用網域? A：目前 TLS 提供單一網域及多網域憑證之申請，未提供萬用網域之申請。
Q2：主機更換或主機 IP 變更，TLS 憑證是否需要重新申請? A：若當初申請之 Domain Name 沒有異動，TLS 憑證就不需重新申請。
Q3：若是有 2 台以上主機，但是同一個 Domain Name 是否要申請 2 張憑證?一張憑證要如何匯入兩台主機? A：瀏覽器是以網站 Domain Name 是否相同來認證 SSL 憑證，因此若有多台網站伺服器，只要網站 Domain Name 相同，則只需要申請 1 張 TLS 憑證即可，完成憑證安裝後可將私密金鑰與憑證匯出或複製到其他主機上使用。 IIS：可參考「公告及儲存庫」→「儲存庫」→「TSL 類憑證請求檔製作及安裝相關手冊」中的憑證備份與還原手冊，將私密金鑰與憑證匯出成 pfx 檔案，再複製到另一台主機匯入使用即可。 Apache：複製.key、.cer/crt 到另一台主機。 Tomcat：複製.keystore 檔案到另一台主機。
Q4：若要在同一台主機上面安裝不同 Domain Name 的 TLS 憑證，主機是否能同時容納多張 TLS 憑證? A：同一台主機要安裝多張憑證，建議最好是有多個獨立 IP，各自對應一張憑證。若無，則需視主機 Web Server 是否有支援 SNI 的技術，此技術功能為讓單一 IP 主機可以安裝多張 TLS 憑證。
Q5：已下載 CER 檔案，要如何轉成 PFX 檔案? A：cer 檔案無法直接轉換成 pfx 格式，請先參考「公告及儲存庫」→「儲存庫」→「TSL 類憑證請求檔製作及安裝相關手冊」中 IIS 安裝手冊完成憑證安裝後，再參考憑證備份與還原手冊，將私密金鑰與憑證匯出成 pfx 檔案。
Q6：於 IIS 主機安裝匯入 TLS 憑證後，按 F5 重新整理後，原來匯入的 TLS 憑證會消失? A：若匯入憑證後按 F5 重新整理，憑證即消失，代表匯入之 TLS 憑證在該主機上找不到對應憑證的私密金鑰。請確認是否當初是在同一台主機上產製請求檔 CSR，如果不是，請於當初產製請求檔 CSR 的主機上進行完成憑證註冊要求。如果是，請參考檔案說明嘗試恢復私密金鑰，若以上方法皆無法成功解決，請重新產製請求檔並重新申請憑證。
Q7：申請 TLS 憑證上傳請求檔時出現「CSR 已被使用、金鑰重複請更換或案件流水號重複」等問題，該如何處理? A：此錯誤訊息表示該請求檔內的公鑰 Hash 值在資料庫已有出現過，故請重新產製請求檔，若是使用 Apache 產製，請連同 key 也要重新產製。而若是使用 Tomcat 產製，則 keystore 也要重新產製。
Q8：請問 Windows SHA2 憑證之支援性為何? A：Windows SHA2 憑證支援性：

(1)Windows2003 之 IIS 預設並不支援 SHA2 憑證，須下載微軟更新檔(更新檔編號為 KB938397 及 KB968730)，之後安裝 Patch 到 Server 上即可。 (2)Windows2000 本身無法支援 SHA2 憑證，且微軟已不提供支援，建議更換新版的 Windows Server。 (3)Windows XP 需升級到 SP3 版才支援 SHA2 憑證。
Q9：憑證即將到期，於主機安裝更換完憑證後，主機上的網站憑證顯示為新憑證，但外部連線瀏覽網站仍顯示舊的即將到期之憑證? A：此有可能是前端網路設備有安裝同一張 TLS 憑證尚未更新，目前網站連線都是由該網路設備回傳 TLS 憑證及串鍊並非由主機。 故請檢查前端網路設備(防火牆、L4/L7 交換器等)，應該會找到有安裝同一張 TLS 憑證的設備，看是要移除該設備上的憑證，或是將該設備上的 TLS 憑證更新皆可。 因為網路設備品牌與型號眾多，介面跟操作差異很大，建議詢問當初購買設備的廠商提供憑證安裝資訊或協助。
Q10：安裝完 TLS 憑證後，於電腦可正常瀏覽網站，但使用手機瀏覽卻會出現憑證不受信任? A：可使用下列網站檢測憑證串鍊(中繼憑證及根憑證)是否安裝正確 https://www.sslshopper.com/ssl-checker.html， 若檢測發現串鍊有中斷，請重新下載憑證安裝手冊，重新設定憑證串鍊。

三、憑證類別相關問題

Q1：請問學校應該向 GCA 還是 XCA 申請憑證? A： 學校(含公立及私立學校)已改由 XCA 簽發憑證，請向 XCA 申請憑證。
Q2：請問國防部所屬軍事學校該向 GCA 還是 XCA 申請憑證? A： 國防部所屬軍事學校仍由 GCA 簽發憑證，請向 GCA 申請憑證。
Q3：請問內政部所屬警察學校該向 GCA 還是 XCA 申請憑證? A： 內政部所屬警察學校仍由 GCA 簽發憑證，請向 GCA 申請憑證。
Q4：請問什麼是機關或單位非 IC 卡類憑證? A： 一般機關或單位申請憑證是將其私密金鑰與憑證存放在 IC 卡中，也有些機關或單位因為加解密速度或是其他用途，需要將私密金鑰與憑證存放於其他儲存媒體(例如：保密器、硬碟)，此類憑證即為非 IC 卡類憑證；目前最常使用的用途為機關電子關防。
Q5：請問要如何選擇非 IC 卡類憑證或專屬類伺服應用軟體憑證之金鑰產製工具與製作憑證請求檔? A：非 IC 卡類憑證與專屬類伺服應用軟體憑證之產製金鑰及憑證請求檔(Certificate Signing Request，CSR)的工具需要配合應用系統所使用的環境為何來選擇，所以憑證管理中心無法提供通用工具，而用戶在申請憑證時應自行使

用適合之工具程式來產製金鑰及 CSR，若用戶無法確定應該使用什麼工具程式，應向應用系統開發廠商詢問清楚，以免使用了錯誤之工具產製金鑰及 CSR，等憑證核發下來後，才發現產製的金鑰格式無法相容於應用系統。

Q6：請問為何要申請及使用 Server AP 憑證?

A： 為了在網路上確認伺服器應用程序(Server Application Process)之身分，確保資訊傳遞的安全，例如：TLS 類的 Server AP 憑證可讓使用者確認並信賴網站的身分，使瀏覽器與伺服器之間的通訊有安全加密的功能，確保通訊過程中的資料安全以及傳遞資料的完整性。

Q7：請問什麼是 TLS 類的 Server AP 憑證?

A： AP 係指 Application Process，使用到 TLS 通信協定的伺服器可申請 TLS 類的 Server AP 憑證，該類憑證其主體及主體別名均有註記該 Server AP 所使用的 Domain Name，例如：大型行政資訊系統電子閘門(國家發展委員會電子閘門平台案、戶役政電子閘門、工商電子閘門、稅務電子閘門、地政電子閘門、公路監理電子閘門等)或是一般電子化政府網站就常會使用到。

Q8：請問什麼是專屬類別 (Proprietary)的 Server AP 憑證?

A： AP 係指 Application Process，如果該 AP 所用之通訊協定為專屬自訂而非通用標準時，其 Common Name 使用該 Server AP 的名稱，例如：國家發展委員會建置公文電子閘道委外服務、財稅五年平台案網路報稅、電子公文交換等。

Q9：請問機關或單位非 IC 卡類憑證及伺服器應用軟體憑證有何不同?

A： 非 IC 卡類憑證其憑證主體為機關或單位，私密金鑰存放在 IC 卡以外的媒體，例如：保密器、代表機關或單位之電子關防。伺服器應用軟體憑證其憑證主體為機關或單位所擁有之伺服器應用軟體(專屬類或 SSL)，用以確認伺服器應用程序(Server Application Process)之身分，確保資訊傳遞的安全，並以下表區分其差別：

憑證類別	憑證簽發對象	憑證中的 Key Usage	憑證中 DN 的 Common Name
機關單位非 IC 卡類憑證	政府機關(構)憑證非 IC 卡類憑證 包含中央政府機關、地方政府機關、公營事業及公立機構。	Digital Signature	政府機關單位的 X.500 名稱

	政府單位憑證非 IC 卡類憑證 包含上述政府機關(構)之附屬單位，或附屬單位的附屬單位。	Key Encipherment / Data Encipherment	
TLS 類伺服器應用軟體憑證	政府機關（構）、政府單位、或醫事機構所建置的 SSL/TLS Server，例如具有 TLS 功能的 HTTP Server 等。	Key Encipherment	Domain Name
專屬類伺服器應用軟體憑證	簽發對象為政府機關（構）、政府單位、或醫事機構所建置的特殊用途之伺服應用軟體憑證，例如用來提供身分識別服務的 Server 等。	Digital Signature	Server AP 的名稱
		Key Encipherment / Data Encipherment	

四、憑證到期重新申請問題

Q1：如何查詢機關單位之前申請了幾張憑證?及如何知道每張憑證的有效期限? A： 請至「憑證管理」→「憑證查詢及下載」輸入條件即可得知機關內有幾張憑證。點選每張憑證之「詳細資料」即可得知該張憑證的效期。 或至「憑證管理」→「線上查詢機關所有憑證」插入機關單位憑證 IC 卡並輸入 IC 卡 PIN 碼即可得知機關內所有憑證資訊。
Q2：政府機關單位憑證因效期即將屆滿，重新申請憑證作業應於 GCA 網站的那一項目辦理? A： 請依照所需的憑證屬於 IC 卡、非 IC 卡類或伺服器應用軟體憑證，自網站「憑證申請」項下選取所需申辦項目辦理。 另憑證 IC 卡於屆期 60 天內，可至「憑證申請」→「憑證 IC 卡屆期插卡換發申請」直接於線上以原 IC 卡片辦理換發，毋須再發送公文與申請書至本憑證管理中心或數位發展部，簡化行政

審核作業，加速卡片核發時效。
Q3：何時可以重新申請憑證? A： GCA 機關單位正卡於到期前 60 天以內可以重新申請憑證，請於憑證聯絡人接獲系統 e-mail 通知憑證即將到期時重新申請憑證。機關單位附卡或機關單位憑證非 IC 卡類雖然不像正卡一樣有每機關只能申請 1 張之限制，但建議於憑證到期前 60 天至 15 天前期間提出申請。
Q4：憑證到期時的換發方式，是舊卡可沿用?還是要申請新卡?或者可以展期? A： GCA 所簽發之憑證到期，必須更換金鑰對，重新申請憑證。亦即若私密金鑰載具為 IC 卡者也必須重新申請新的 IC 卡，不提供展期，也無法使用舊卡。GCA 之機關單位 IC 卡金鑰對為 IC 卡晶片內部產製，私密金鑰永遠不會外洩至 IC 卡片以外，因此不允許金鑰對自外部寫入，不提供舊卡寫入新私密金鑰，因此舊卡到期自然失效，不再沿用。
Q5：憑證申請書的遞件窗口為何?憑證申請公文是否有填寫範例? A： 憑證申請書請隨公文函送數位發展部，地址:100 臺北市中正區延平南路 143 號。 請多利用公文電子交換方式申請。 憑證申請公文內容可參考「公告及儲存庫」→「儲存庫」→「文件表單資料下載—公文範例及申請書」項下之憑證申請公文範例。
Q6：憑證到期，需要原申請人重新提出申請嗎?亦或者舊卡之承辦人已離職，辦理新卡是否可以更換聯絡人資訊? A： 憑證到期由有需要憑證 IC 卡應用於電子化政府相關應用(如公文電子交換)之同仁代表機關單位提出申請，如原申請人有異動可由工作交接後之人員提出申請，如原申請人仍負責該項應用之使用且職務沒有調整，可請原申請人提出憑證申請。 每張 IC 卡在填寫憑證申請書時，皆會有憑證聯絡人之填寫欄位，新卡之憑證聯絡人可以和舊卡之憑證聯絡人不同。
Q7：辦理憑證 IC 卡屆期換發填寫申請書時，用戶代碼是否需跟舊憑證 IC 卡相同? A： 填寫申請書時，用戶代碼可重新設定，可與舊憑證 IC 卡不同。
Q8：為何申請正卡時一直不成功? A： 同一機關單位只能有一張正卡，但在正卡憑證效期即將屆滿之 60 天內允許重新申請正卡，亦即該段期間可以有新舊憑證 IC 卡並存，亦即無法成功申請正卡之原因可能是舊憑證到期日尚未在 60 天以內。
Q9:舊的憑證 IC 卡內的憑證會被憑證管理中心廢止並放到憑證廢止清冊(CRL)嗎?舊的憑證 IC 卡要如何保管? A： 依 CPS 規範，憑證 IC 卡在發出後，由用戶自行妥善保管，在憑證過期失去效力後也相同。用戶須自行保管到期的憑證 IC 卡。 CA 也不會廢止用戶到期之憑證，而是失去效力，所以依時間的流逝，逐漸有更多 IC 卡片失去效用，

無法使用於應用系統。
到期的憑證依 X.509 的規範並不會放到憑證廢止清冊(CRL)中，如前所述憑證的自然到期並不會被視為廢止，再者如有在未到期之前已做憑證廢止者，則在該憑證到期後，將自 CRL 中被移除。對於應用系統來說，則 CRL 檔案有可能會變小。
請妥善保管憑證 IC 卡，工作轉調時需列入業務移交，無論已過期或仍有效力之憑證 IC 卡，均勿損毀或丟棄。
用戶如果有以舊 IC 卡片加密的檔案，應先做解密，以免卡片的晶片在更久的將來損毀，而無法做檔案的解密。至於解密的電子文件的安全保存方法，可重新申請一張新的憑證 IC 卡做檔案加密，或是以其他加密的方法做保存。

五、憑證管理作業相關問題

Q1：如何開卡?
A：收到憑證 IC 卡後，請至「憑證管理」→「IC 卡開卡作業」進行開卡作業。取得 PIN 碼，即開卡完成。

Q2： 逾期未開卡?
A：收到憑證 IC 卡後，請於發卡日期後 90 天內，完成開卡作業，如逾期未開卡，本中心將逕行停用憑證。

Q3：使用應用服務系統前，若未開卡?
A：請勿在卡片尚未開卡前，就直接將卡片使用於應用服務系統，這樣將造成卡片永久損壞，無法再使用。

Q4：為何會鎖卡?如何進行鎖卡解碼?
A：為安全起見，當使用憑證 IC 卡於應用服務系統時，會要求輸入 IC 卡的 PIN 碼，輸入 PIN 碼 3 次都驗證失敗時會自動鎖卡，此時卡片持有者便無法正常使用此卡，請至「憑證管理」→「鎖卡解碼/重設 PIN 碼」進行鎖卡解 PIN 碼作業。
注意：請勿使用 SafeSign CSP 軟體中『Unlock PIN』的功能來解鎖卡，以免造成 IC 卡永久鎖卡。

Q5：如執行鎖卡解碼作業時，用戶代碼被鎖了，怎麼辦?
A：若於執行鎖卡解 PIN 碼時，因遺忘用戶代碼或鍵入用戶代碼 3 次錯誤，造成卡片被鎖定，也無法再進行解 PIN 碼時，請先至「憑證管理」→「用戶代碼重設」申請重新設定用戶代碼後再執行鎖卡解 PIN 碼作業。

Q6：忘記 PIN 碼怎麼辦?
A：請至「憑證管理」→「鎖卡解碼/重設 PIN 碼」將卡片插入讀卡機，輸入用戶代碼進行重新設定 PIN 碼作業。

Q7：忘記用戶代碼怎麼辦?
A：當忘記用戶代碼時，線上憑證相關作業將不能使用，請至「憑證管理」→

「用戶代碼重設」申請重新設定用戶代碼。
流程如下：
1.請填寫用戶代碼重設申請書。
2. 請將用戶代碼重設申請書傳真至 02-33930708 或 Email 至 egov@service.gov.tw 客服中心辦理重設。
3.MAIL 通知新的用戶代碼。
4.將申請書及公文函送至數位發展部辦理或是將申請書蓋上關防寄至政府憑證管理中心，並需於一個月內繳回重設申請書，否則憑證將逕行停用。

Q8：用戶代碼有何用途?
A：在線上憑證作業內會使用到用戶代碼的有以下作業：
1. 申請狀態查詢作業
2. 申請書修改及補列印作業
3. 憑證接受作業
4. 鎖卡解碼/重設 PIN 碼作業
5. 憑證停用/復用作業
用戶代碼非常重要，請勿遺忘。並務必妥善保管用戶代碼函，如有洩漏或遺忘時，請參考用戶代碼重設說明。

Q9：憑證聯絡人的用途為何?
A：申請憑證時，需填寫憑證聯絡人資料，以利憑證中心郵寄憑證 IC 卡，若有後續訊息通知(例如憑證到期訊息等)，將以所留的電子郵件、電話、傳真等資料進行聯絡。

Q10：如何更改憑證 IC 卡聯絡人?
A：若職務異動或聯絡資料變更，請至「憑證管理」→「憑證 IC 卡連絡人修改」進行憑證 IC 卡聯絡人修改作業。
注意：需先完成 IC 卡開卡作業，並將 IC 卡插入讀卡機，輸入 PIN 碼後，才能進行修改作業。

Q11：使用憑證發生問題時，該如何確認憑證是否有效?
A：請至「憑證管理」→「憑證查詢及下載」查詢目前憑證的有效狀態，若憑證狀態屬於「有效」代表憑證沒有問題，應是應用服務系統認證上出現異常，煩請聯絡該應用服務客服人員。

Q12：如何檢視憑證 IC 卡資訊?
A：請至「憑證管理」→「憑證 IC 卡資訊檢視」並將卡片置入讀卡機中，點選偵測卡片並選擇卡片，即可查詢憑證 IC 卡資訊(卡號、卡片持有者資訊、卡片效期、憑證核發單位)。

Q13：憑證 IC 卡遺失時該如何處理?
A：若發現憑證 IC 卡遺失時，請先至「憑證管理」→「憑證停用／復用」進行憑證停用作業。後續確定遺失無法找回時，請辦理廢止憑證，以防止憑證 IC 卡被他人盜用。而若確認 IC 卡並無遺失，請進行憑證復用作業，恢復憑證使用

功能。 注意：憑證一旦廢止即無法再做復用，僅能重新申請憑證。
Q14：如何停用/復用憑證? A：請至「憑證管理」→「憑證停用／復用」進行線上憑證停用或復用作業。
Q15：憑證停用可以停用多久? A：憑證停用的最長期限為自憑證開始時間到憑證到期時間。
Q16：如何廢止憑證? A：請至「憑證管理」→「憑證廢止」申請廢止憑證。 注意：憑證一旦廢止即無法再做復用，僅能重新申請憑證。

六、OID 相關問題

Q1：何謂 OID(Object Identity Object Identifier，OID)? A： OID 主要是用來做為資訊物件的唯一識別符號，讓資訊在網際網路上傳遞更為方便與安全，目前許多技術規格都定義必須使用 OID(如：X509(v3) …等)。為了電子化政府的長遠發展，有鑑於政府機關單位沒有一個統一的唯一識別符號來做應用識別，所以採用物件 OID 化以統一識別及管理。
Q2：OID 的編碼原則為何? A：我國 OID 國碼為 2.16.886，政府領域 OID 保留範圍為 2.16.886.0-2.16.886.999。
Q3：憑證與 OID 的關係為何? A：依據國際標準，公鑰憑證擴充欄位中皆需一組 OID 來識別，機關或單位 OID 會放在憑證的用戶目錄屬性延伸欄位中，因此在申請憑證 IC 卡時，必須有機關(單位)的 OID。
Q4：如何查詢 OID? A：請至 OID 網站查詢 https://oid.nat.gov.tw
Q5：申請或異動機關 OID 的流程為何? A：請參考網站「憑證申請」→「OID 新增及異動申請服務」相關說明。
Q6：如何分辨機關及單位? A：機關：由行政院人事行政總處統一管理，並編有機關代碼者，具有預算人事等權力，稱為機關，如行政院(A00000000A)、內政部(301000000A)、內政部警政署(A01010000C)等。 單位 ：行政院人事行政總處授權由各機關自行管理，無統一之代碼者，稱為單位，如行政院秘書處、外交部部長辦公室等。
Q7：如何查詢目前有多少機關編有 OID，多少單位編有 OID? A：請至 OID 網站左方功能選項「物件識別碼統計資料」查詢。
Q8：OID 申請之公文從數位發展部收文後多久會處理完成? A：數位發展部會內 OID 公文處理不超過 7 天，OID 建檔平均處理天數不超

過 2 天。

七、讀卡機相關問題

Q1：請問憑證申請時是否提供讀卡機?

A： 讀卡機請自備(可參考內政部憑證管理中心自然人讀卡機選購方式)。