組織及團體憑證管理中心入口網(XCA)　Q&A

一、憑證到期重新申請問題

Q1:如何查詢組織團體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 XCA 網站首頁點選上方白底黑字「憑證作業」，再點選左方功能選項「憑證查詢及下載」，輸入條件即可得知組織團體內有幾張憑證。點選每張憑證之「詳細資料」即可得知該張憑證的效期。 或至 XCA 網站首頁點選上方白底黑字「憑證作業」，再點選左方功能選項「線上查詢機關所有憑證」，插入組織團體憑證 IC 卡並輸入 IC 卡 PIN 碼即可得知組織團體內所有憑證資訊。
Q2：組織及團體憑證因效期即將屆滿，重新申請憑證作業應於 XCA 網站的那一項目辦理? A：請依照所需的憑證屬於 IC 卡、非 IC 卡類憑證，自 XCA 網站首頁點選常用連結之「憑證申請」項下選取所需申辦項目辦理。
Q3：何時可以重新申請憑證? A： 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 或接獲通知憑證即將到期時重新申請憑證。附卡憑證雖然不像正卡一樣有每一組織或團體只能申請 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：憑證到期時的申請方式，是舊卡可沿用?還是要申請新卡?或者可以展期? A： XCA 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。 XCA 之組織團體 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所屬登記立案主管機關(初審窗口)進行初審。憑證申請公文內容可參考 XCA 網站首頁上方白底黑字「資料下載」的「常用表單下載」項下之憑證申請公文範例。
Q6：舊卡之承辦人已離職，辦理新卡是否可以更換承辦人及 EMAIL? A： 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：XCA 所簽發之憑證到期，重新申請憑證，管理中心會核發新的 IC 卡，故用戶代碼可重新設定，不需一定要與舊卡一樣。
Q8：申請正卡時，一直不成功? A： 同一組織團體只能有一張正卡，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：憑證到期，需要原申請人重新提出申請嗎? 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)之同仁代表組織團體提出申請，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。
Q10： 請問舊的憑證 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。

二、憑證申辦問題

Q1：請問什麼是憑證 IC 卡? A：憑證 IC 卡的主要功能為提供網路身分驗證、並防止資料在傳輸與交換的過程中被偽造或竄改。所以，常有人把憑證 IC 卡和網路身份證劃上等號。而因為憑證用戶的身份和角色有所不同，通常也都必須申請所對應的憑證類別，來作為網路身份認證使用。目前較為國人所熟知的憑證 IC 卡有內政部的自然人憑證 IC 卡、經濟部的工商憑證 IC 卡和數位發展部的政府憑證 IC 卡。
Q2：請問什麼是組織及團體憑證 IC 卡? A：組織及團體憑證 IC 卡，為數位發展部在推動電子化政府各項創新服務和線上申辦作業時，簽發給各級公私立學校、財團法人、社團法人、行政法人、自由職業事務所及其他組織或團體等 6 類憑證用戶所使用的憑證 IC 卡。
Q3：請問哪些組織及團體適合申請組織及團體憑證 IC 卡? A：如果您是已經合法登記立案的學校、財團法人、社團法人、行政法人、自由職業事務所或其他組織或團體，您都可以申請組織及團體憑證 IC 卡，申

請對象列表：

憑證種類	申請對象
學校	大學院校、技專院校、高中職、國民中小學、幼兒園
財團法人	各目的事業主管機關主管的各類財團法人
社團法人	合作社、農漁會、工會、教育會、工業會、政黨等
行政法人	依法成立之行政法人
自由職業事務所	會計師、建築師、地政士、專業技師、藥劑師、記帳業者等自由職業所設立的事務所、藥局
其他組織或團體	上述幾種以外的組織或團體，在相關的政府主管機關有登記立案但不具法人身分，例如：寺廟、協會、學會、教師會、宗親會、同鄉會、公寓大廈管委會

Q4：請問如何申請 XCA 憑證 IC 卡?

A：

1.連結至 XCA 網站，點選網頁上方黑底白字「憑證申請」項下選取所需申辦項目填寫申請書。

2.填寫完申請表後將申請資料上傳申請並列印申請表。

3.繳費。

4.於申請書蓋上組織團體立案時原留之登記印鑑及負責人印鑑，將申請書寄送至所屬登記立案主管機關(初審註冊窗口)進行審查。

Q5：請問該申請正卡還是附卡?

A：組織及團體憑證 IC 卡，係採單一正卡、多張附卡政策，可提供組織及團體因應內部作業方式，提供不同承辦人員或應用於不同系統時分開使用，減少卡片共用的情況。

正卡僅可申請一張，附卡可以申請多張，使用期限均為發卡日期後六年。用戶可依需求進行申請。

Q6：請問申請 XCA 憑證 IC 卡所需費用?

A：組織及團體憑證 IC 卡工本費每張新臺幣 420 元(含郵寄費用)。

Q7：請問如何得知所申請的憑證 IC 卡目前進度狀況為何?

A：請至 XCA 網站首頁「申請狀態查詢」點選「進度查詢」或首頁上方白底黑點選「憑證申請」，再點選左方功能選項點選「申請狀態查詢」，可線上查詢申請進度。若查詢結果為憑證已簽發，但您仍未收到卡片，你可打電話至客服電話 02-2192-7111，我們將幫您查詢郵局投遞狀況。

Q8：請問申請組織及團體憑證是否有限制張數?

A：組織及團體憑證 IC 卡，正卡僅可申請一張，附卡可按實際需求申請。
Q9：XCA 憑證申請流程步驟? A：請參考 XCA 網站憑證申請作業流程說明。

三、主管機關(初審註冊窗口)問題

Q1：為何需要初審註冊窗口? A：為配合電子化政府相關應用，數位發展部已建置組織及團體憑證管理中心(簡稱 XCA)，負責核發學校、財團法人、社團法人、行政法人、自由職業事務所及其他組織或團體之憑證 IC 卡，需由各類憑證用戶之主管機關或授權單位設立初審註冊窗口負責憑證申請者之身分識別相關作業。
Q2：設立初審註冊窗口的依據為何? A：依據組織及團體憑證管理中心(簡稱 XCA)之憑證實務作業基準規定，由各類憑證用戶之主管機關或授權單位設立初審註冊窗口負責憑證申請者之身分識別相關作業，各類憑證用戶之主管機關說明請參考 XCA 憑證用戶主管機關一覽表。
Q3：何謂憑證註冊審驗人員(RA Officer, RAO)? A：憑證註冊審驗人員(RA Officer, RAO)，係指各類憑證用戶主管機關(初審註冊窗口)中，負責受理憑證申辦身分認證相關作業之承辦人員。一個初審註冊窗口可能有多位憑證註冊審驗人員。
Q4：如何申請設立組織及團體憑證管理中心初審註冊窗口? A：請至 XCA 網站首頁點選上方白底黑字「初審註冊窗口專區」，再點選左方功能選項「如何成為初審註冊窗口」，請依照成立窗口說明辦理。
Q5：初審註冊窗口承辦人員有異動如何處理? A：為簡化初審窗口作業流程，取消憑證註冊初審窗口人員申請規定，窗口人員新增異動無需來文申請由各主管機關自行派任。
Q6：初審註冊窗口之工作項目包含哪些? A：書面審查憑證用戶提出之申請案件，將審查通過之案件函送至數位發展部，審查項目包含組織(團體)名稱、填表資料及圖記是否正確等。
Q7：初審註冊窗口承辦人員是否需要操作組織及團體憑證管理中心(XCA)的資訊系統嗎? A：初審註冊窗口工作項目分為兩項，主要以書面審查資料為主，無須操作 XCA 的資訊系統。
Q8：初審註冊窗口承辦人員需要主動通知組織(團體)識別碼(OID)建立進度嗎? A：數位發展部完成組織(團體)識別碼(OID)建立作業後，將主動寄發電子郵件至組織(團體)聯絡人員信箱，請聯絡人員確認資料，同時將以電子郵件通知承辦人員該次組織(團體)識別碼處理情形，承辦人員可以不需通知組織(團體)識

別碼(OID)建立進度。

Q9：初審註冊窗口承辦人員需要主動通知組織(團體)憑證申請進度嗎?

A：數位發展部收到初審註冊窗口函送之申請案件後，即會進行 IC 卡發卡作業，IC 卡發卡完成後系統將自動寄發電子郵件信箱給憑證申請人，如憑證用戶申請資料需要更正時，系統將以電子郵件通知用戶退件原因與處理方式，憑證用戶亦可自行在 XCA 網站上查詢申辦進度，承辦人員可以不需通知組織(團體)憑證申請進度。

四、繳費相關問題

Q1：申請組織及團體憑證是否需要費用?費用為多少?

A：申請憑證 IC 卡之工本費用(含掛號郵資)，無論「正卡」或「附卡」皆為新台幣 420 元，非 IC 卡類憑證新台幣 320 元，若憑證遺失、損壞、自行辦理憑證廢止、憑證到期失去效用、組織更名導致憑證失效或憑證內容變動，請重新申請並需再次繳納費用。

Q2：憑證申請投單後是否可要求退費?該如何進行?

A：憑證一旦核發後將不接受退費，申請資料請務必填寫正確，憑證核發前仍可進行資料更改或申請退費，有關退費問題可撥打客服電話 02-2192-7111 詢問。

Q3：於 XCA 網站申請憑證時我該如何繳納費用呢?

A：

1.組織及團體憑證申請過程中，會引導您至憑證付費系統，請於憑證付費系統中，以該申請案之「案件流水號」及「用戶代碼」進入後，選擇您要付費的方式，並填寫發票資料及依指示完成繳款動作。

2.目前本管理中心提供的付費方式：信用卡付費、ATM 或臨櫃繳款。

3.請勿重複繳款。

Q4:於 XCA 網站申請憑證時選擇以 ATM 或臨櫃繳款付費，繳款期限為 30 天，過期了該怎麼辦?

A：選擇以 ATM 或臨櫃繳款付費時，於繳款資訊中會列出繳款期限，超過期限後請勿進行繳費，逾期後繳款帳號將自動失效，請再次至憑證付費系統重新取得繳款資訊，在尚未繳款成功前，您也可以選擇再次更換為其他種付費方式。

Q5：申請組織及團體憑證繳費後會有發票嗎?沒有收到發票該怎麼辦呢?

A：您於繳費完成後，本憑證管理中心將委託「中華電信股份有限公司資訊技術分公司」進行電子發票開立(約需 3-5 個工作天，非繳費當天開立)，若電子發票資訊有填寫統一編號則會平信郵寄紙本至發票指定寄送地址。若您於繳費後 1 個月仍未收到電子發票證明聯，可撥打客服電話 02-2192-7111 詢問。

Q6:已收到申請組織及團體憑證所開立的電子發票證明聯，但發現統一編號有誤，請問可以變更統一編號嗎?

A：若您確認有修改之需求，請來電客服專線 02-2192-7111，經諮詢服務人員確認相關資料後，請備妥欲修改之電子發票證明聯正本，並檢附正確之組織團體基本資料及聯絡人相關資訊後，掛號寄回組織及團體憑證管理中心(郵寄地址：100 台北市中正區信義路一段 21 號數據通信大樓 4 樓；收件者：組織及團體憑證管理中心收)進行修改。

五、憑證作業相關問題

Q1：如何開卡? A： 收到憑證 IC 卡後，請至 XCA 網站首頁常用連結點選「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，請於發卡日起 90 天內完成開卡，如逾期未開卡憑證將逕行停用。
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 XCA 網站首頁常用連結點選「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，請至 XCA 網站首頁常用連結點選「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：重設 PIN 碼時出現「Initial Card」之錯誤訊息，應該如何解決? A：請您先行確認幾項事情： 1.確認讀卡機裝置是否正確(驅動程式是否已正確安裝完成)。 2.IC 卡是否有插入讀卡機內，插入方向是否無誤。
Q7：忘記用戶代碼? A：當忘記用戶代碼時，線上憑證相關作業將不能使用，請至 XCA 網站首頁常用連結點選「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.將申請書正本郵寄至組織及團體憑證管理中心，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.修改及補列印申請書作業
3.開卡作業
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，請至 XCA 網站首頁常用連結點選「用戶代碼重設」，申請重新設定用戶代碼。

Q9：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 XCA 網站首頁點選上方白底黑字「憑證作業」，再點選左方功能選項「憑證 IC 卡聯絡人修改」，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。

Q10：欲確認所使用的憑證 IC 卡是否有效沒有問題?
A：
1.請至 XCA 網站首頁點選上方白底黑字「憑證作業」，再點選左方功能選項「憑證查詢及下載」，確認憑證狀態是否為「有效」。
2.再點選左方功能選項「檢視憑證 IC 卡資訊」，以確認讀卡機讀取到 IC 卡資料。
3.更改 PIN 碼，以確認 PIN 碼是否正確。
以上的操作流程如果皆正確無誤，代表您所持有的卡片沒有問題，若有出現任何異常或是錯誤，請電洽 02-2192-7111 專線洽詢。

Q11：若使用憑證發生問題，如何確認憑證是否有效?
A：請至 XCA 網站首頁點選上方白底黑字「憑證作業」，再點選左方功能選項「憑證查詢及下載」，查詢目前的憑證有效狀態，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?
A：請至 XCA 網站首頁點選上方白底黑字「憑證作業」，再點選左方功能選項「檢視憑證 IC 卡資訊」，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：若發現憑證 IC 卡遺失時該如何處理? A：若發現憑證 IC 卡遺失時，請先至 XCA 網站首頁點選上方白底黑字「憑證作業」，再點選左方功能選項「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，請點選「憑證停用/復用」，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：要如何停用/復用憑證? A：請至 XCA 網站首頁點選上方白底黑字「憑證作業」，再點選左方功能選項「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：要如何廢止憑證? A：請至 XCA 網站首頁點選上方白底黑字「憑證作業」，再點選左方功能選項「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、憑證類別問題

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：部會直接設立的學校該向 GCA 還是 XCA 申請憑證? A：部會因特殊目的所設立的學校，例如僑委會所設立的「中華函授學校」，這些部會直接設立的學校歸由 GCA 負責簽發憑證，簽發的憑證為政府機關(構)憑證，而不是由 XCA 簽發學校憑證。國防部所設立的軍事學校、內政部所設立的警察學校及其他部會特殊目的所設立的學校，雖然都具有學校之名，也兼受教育部指導，但是這些學校依據相關組織條例或教育條例，是直屬於這些部會的附屬機關(構)，因此歸由 GCA 負責簽發政府機關(構)憑證，而不是由 XCA 簽發學校憑證。
Q5：外國僑民學校可否申請 XCA 憑證嗎? A：外國僑民學校可申請 XCA 憑證。
Q6：請問幼兒園該向 GCA 還是 XCA 申請憑證? A：公私立幼兒園之管理法規是幼稚教育法，主管機關是教育部及地方政府教育局處，請向 XCA 申請憑證。

Q7：請問外商在臺代表辦事處、外國駐臺經濟文化商務辦事處能否申請 XCA 憑證?

A：外商在臺代表辦事處、外國駐臺經濟文化商務辦事處可申請 XCA 憑證。其中外商在臺代表辦事處為配合勞健保系統註冊使用，憑證管理中心會於組織主體名稱後加註(在臺辦事處)之字樣。

Q8：醫療機構如何向 GPKI 各 CA 申請憑證?

A：

醫療機構		核發憑證的 CA	憑證類別	醫療機構舉例
醫療法人		XCA	財團法人或社團法人	如：長庚醫療財團法人、秀傳醫療社團法人
法人附設醫療機構		XCA	其他組織或團體	如：長庚醫療財團法人林口長庚紀念醫院、阮綜合醫療社團法人阮綜合醫院、醫療財團法人台灣血液基金會台中捐血中心
私立醫學院校附設醫院		XCA	其他組織或團體	如：中山醫學大學附設醫院
公司或商號附設醫療機構		MOEACA	公司或商號附卡	如：中華電信股份有限公司醫務室
私立醫療機構		XCA	其他組織或團體	如：博仁綜合醫院、診所、聯醫病理中心
公立醫療機構	衛生福利部、國防部、國軍退除役官兵輔導委員會所屬醫院	GCA	機關構單位憑證	如：行政院衛生福利部臺北醫院、三軍總醫院、臺北榮民總醫院
	縣（市）立醫院	GCA	機關構單位憑證	如：臺北市立仁愛醫院
	公立醫學院校附設醫院	XCA	其他組織或團體	如：國立臺灣大學醫學院附設醫院

Q9：請問學校是否能夠申請伺服器應用軟體憑證?

A：目前 XCA 沒有對各組織或團體發放其伺服器應用軟體憑證，若為組織團體內部應用所需，可選用現有免費或商用軟體產製伺服器應用軟體金鑰對與簽發所需憑證。或使用民間 CA 所簽發之伺服器應用軟體憑證。

七、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，將相關資訊物件給予 OID 編碼以利統一識別及管理。
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，組織(團體)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，必須有組織(團體)的 OID。
Q4：申請或異動 OID 的流程為何? A：請參考 XCA 網站首頁點選上方白底黑字「憑證申請」，再點選左方功能選項「OID 新增及異動申請服務」之說明，或 OID 網站左方欄位中「組織及團體物件識別碼」選項下之「物件識別碼(OID)申請」之說明。
Q5：組織(團體)名稱變更或聯絡資料異動，需要異動 OID 嗎? A：請至 XCA 網站首頁點選上方白底黑字「憑證申請」，再點選左方功能選項「OID 新增及異動申請服務」，請依照 OID 申請異動說明辦理，名稱變更時將重新編列 OID，並需廢止憑證 IC 卡。
Q6：組織(團體)可以自行提出 OID 申請嗎? A：需由主管機關(初審註冊窗口)代為申請，組織(團體)可向主管機關(初審註冊窗口)提出請求。
Q7：組織(團體)OID 申請異動需要多久處理時間? 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。 建檔後將以電子郵件通知主管機關窗口或組織(團體)聯絡人處理結果。

八、其他相關應用

Q1：請問安全保密函式庫之作用？ A：安全保密函式庫依據 GPKI 技術規範、憑證及憑證廢止清冊格式剖繪、公鑰憑證處理安全事項檢查表以及相關國際相關標準，提供開發電子認證應用系統所需之安全保密函式，可呼叫編譯後提供數位簽章以及檢驗簽章、加密與解密、憑證解析、憑證廢止清冊查訊下載與檢驗、憑證線上狀態查詢等功能。以

解決資訊安全上身份鑑別、資料完整性、系統真確性、機密性、不可否認性、存取控制、可歸責性之問題。
Q2：請問安全保密函式庫之語言及編譯平台版本？ A：GPKI 安全保密函式庫使用 C 語言與 Java 語言撰寫，都可在 Windows 與 Linux 平台編譯。GPKI 安全保密函式庫最新版本名稱為 HiSECURE v6.1.0，C 語言版本係使用 C++語言開發，並提供跨平台支援能力，包括 Java(透過 JNI 的呼叫方式)、Win32(直接使用或是再包裝成 DLL、ActiveX COM 元件均可)、LINUX 等系統(提供相同函式介面之該平台 API)環境均可支援。以下為編譯環境： (a)Windows 平台之編譯環境：Windows 作業系統 Visual Studio C++ 6.0 (b) LINUX 平台之編譯環境：Linux CentOS 2.6.18-92.el5 gcc version 4.1.2 20071124 (Red Hat 4.1.2-42) 安全保密函式庫 Java 語言版本 2.1 可以適用於 Win32/Linux 環境。 編譯環境包含： (a)Windows 平台之編譯環境：JDK1.4.2 以上 (b)LINUX 平台之編譯環境：JDK1.4.2 以上
Q3：請問 GPKI 安全保密函式庫標準版的版權與函式散布？ A：GPKI 安全保密函式庫標準版係由中華電信研究所開發，匯集了先進的網路安全標準與多年的資訊安全及密碼學之研發經驗，其智慧財產權屬於中華電信公司所有。為配合電子化政府基礎建設的網路安全需求，使眾多植基於政府機關公開金鑰基礎建設的應用系統能儘速進行開發測試，授權提供數位發展部 GPKI 專案使用，由各機關發文向數位發展部提出申請，函式庫的散布由數位發展部控管。
Q4：請問安全保密函式庫在申請與下載時之版本控制機制為何？ A： GPKI 安全保密函式庫標準版-HiSECURE SDK(6.1.0 版)目前雖為成熟的產品，但仍因為需求的變更與相關技術的演進而有版本更新的機會。目前函式庫是集中透過 https://gpkiapi.nat.gov.tw/此網站進行下載。下載之機關單位需事先向數位發展部發文提出申請，並說明準備開發之電子化政府應用相關資料，公文經核准後可取得帳號密碼下載。網站上面也會放置最近的兩個版本供下載，並且只有通過身分驗證的授權使用者才可以進入此網站並經過 SSL 安全機制下載函式庫，並提供檔案完整性比對工具，如此可以有效杜絕不明版本的散佈與流傳。
Q5：請問 GPKI 安全保密函式庫與 GTESTCA 應用發展套件之差異。 A：GTESTCA 發展套件除了提供相同之 GPKI 安全保密函式庫（內含使用手冊及範例程式），還提供已制式化處理與印刷的 RSA IC 卡片 6 張，以及 USB 介面 IC 卡讀卡機兩部，開發人員可使用安全保密函式庫進行系統開發作業，並以 RSA IC 卡片至政府測試憑證管理中心進行憑證申請等相關作業，以利進行系統測試。建議申請機關/單位請先向政府測試憑證管理中心申購 GTESTCA

發展套件，等系統測試一切正常後，再申請正式憑證及安全保密函式庫標準版(建議系統正式上線前一至兩個月至 GCA 網站之安全保密函式庫提出申請。請於線上填寫安全保密函式庫申請書，填寫完畢列印安全保密函式庫申請書及保密切結書，以公文書方式函送數位發展部，若核准將提供帳號與密碼供下載安全保密函式庫。)
Q6：安全保密函式庫每個模組可以被同時開啟幾次？ A：不同的模組有不同的限制；不過並不建議這樣使用。由於起始一個密碼模組之後可以執行多次的密碼模組運算，因此程式設計應減少複雜性，不要起始過多的模組。
Q7：輸入 IC 卡 PIN 碼三次錯誤後被鎖卡，在啟始模組或起始 Session 時，會得到哪些 Return Code？ A： 若 IC 卡已鎖卡，在起始 Session 時，InitSession 函式將傳回十六進位為 0xDB011204 的錯誤代碼值。錯誤代碼定義於 errortable.h 之內(#define Smard_Card_Pin_Is_Locked 0xDB011204)。
Q8：請問取出公開金鑰及私密金鑰？ A： 私密金鑰是無法取出來的。 HiSECURE API 並不提供取出公開金鑰或私密金鑰的方式，取代的用法為呼叫 GetKeyObjectHandle()這個函式取出金鑰的控制指標來執行密碼模組運算功能，詳細的取得控制指標(HANDLE)方式請參照各個密碼模組的操作指引。
Q9：讀取憑證內容時，是否需要驗證 PIN 碼？ A： 讀取憑證及解析憑證內容時不需要驗證 PIN 碼。
Q10：取出私密金鑰時，是否需要驗證 PIN 碼？ A： 不論使用何種方式都無法取出私密金鑰，只能取得它的控制指標，在使用私密金鑰時需要驗證 PIN 碼。
Q11：GPKI 安全保密函式庫提供哪幾種雜湊運算演算法？各種演算法雜湊後的長度是多少？ A：目前提供 MD5、SHA-1、SHA-2(包含 SHA-256、SHA-384、SHA-512)五種雜湊運算演算法，雜湊運算後的長度分別為 16(MD5)、20(SHA-1)、32(SHA-256)、48(SHA-384)、64(SHA-512)個位元組長。
Q12：送入雜湊函數的資料長度是否有限制？ A： 沒有限制。
Q13：XCA 憑證在加解密與簽驗章運算使用的金鑰對是否相同？ A：XCA 憑證採用雙金鑰對，也就是簽驗章和加解密是使用不同的金鑰對。
Q14：在使用加解密與簽章驗簽章運算時，應使用什麼金鑰？ A： 當您要做加密運算、驗證簽章時應該使用公鑰控制指標，並請注意分別採用收文者與發文者之公鑰控制指標。 若是要做解密運算、製作簽章時則應使用私鑰控制指標，並請注意分別採用收文者與發文者之私鑰控制指標。
Q15：XCA 憑證製作的簽章長度是多少？

A： XCA 憑證對應私密金鑰所製作的簽章(簽體)長度是 128 個位元組長。
Q16：GPKI 安全保密函式庫提供哪幾種加解密運算法？ A： 目前提供的加解密運算法為: 非對稱式加解密運算法有 RSA 對稱式加解密運算法有 :DES CBC、DES ECB、3DES CBC、3DES ECB、AES CBC、AES ECB 等六種。
Q17：被簽章的資料是否有長度限制？ A： GPKI 安全保密函式庫簽章前會先以 SHA_1 雜湊函式運算，再對運算結果進行簽章，所以簽章檔案沒有長度的限制。
Q18：GPKI 安全保密函式庫提供哪幾種簽驗章運算法？ A： 目前只提供 SHA_1 with RSA 演算法。