調　查　報　告

壹、案　　由：114年6月傳出中華電信所發出之憑證將遭到Google撤銷信任，影響遍及政府機關網站、金融交易平臺、公共服務入口及企業內部等等，究其影響範圍為何?作為負責發放政府網站憑證之數位發展部有無善盡職責?憑證機構(CA)之發放、撤銷及內控有無疏失?等，均有深入瞭解調查之必要。

貳、調查意見：

在全球網路世界中，數位憑證扮演著確保網路連線安全與身分驗證的關鍵角色。這個複雜的信任體系主要由三個參與者組成：憑證發行機構（CA[1]）、瀏覽器供應商（Browser），以及廣大的終端用戶（End User）[2]。三者之間，瀏覽器供應商信任憑證發行機構所簽發之TLS/SSL憑證，當用戶透過瀏覽器連接到具有有效憑證的網站時，瀏覽器就可以直接放行；反之，當用戶連接到不具有有效憑證的網站時，瀏覽器將提出安全警告，而構成網際網路連線安全及信任的重要機制。

在本案事件中，擔任政府網站服務憑證發行機構的中華電信股份有限公司(下稱中華電信)卻疑似因為管理及技術問題，導致瀏覽器供應商Google Chrome不信任其中華電信政府伺服器數位憑證管理中心(GTLSCA)[3]簽發之傳輸層安全性協定/安全通訊協定(TLS/SSL)[4]憑證，

---

[1] Certificate Authority

[2] 黃彥棻(114年6月9日)。臺灣首度引爆憑證信任危機（一）：中華電信憑證失效，連自家網站的憑證都要跟別人買。IThome(https://www.ithome.com.tw/news/169438)。

[3] Government TLS Certification Authority, GTLSCA

[4] 傳輸層安全性協定，Transport Layer Security(簡稱TLS) /安全通訊協定，Secure Sockets Layer(簡稱SSL)。依據AWS網站簡介，Secure Sockets Layer（SSL）是一種通訊協定或一組規則，可在網路上的兩台裝置或應用程式之間建立安全連線。在您透過網際網路共用憑證或資料之前，重要的是要先建立信任並驗證對方身分。SSL 是您的應用程式或瀏覽器

而將中華電信ePKI[5]和HiPKI憑證設定為不信任，風險遍及政府機關網站、金融交易平臺、公共服務入口及企業內部，引發憑證信任危機。

數位發展部(下稱數發部)為因應此一事態，先於民國(下同)114年3月以強化韌性為由，要求各政府機關網站導入雙憑證機制，嗣於同年6月對外聲明[6]係「中華電信處理不當」，惟該部負責政府機關公開金鑰基礎建設(GPKI)業務並將GTLSCA委託中華電信營運，究該部有無善盡職責?憑證機構(CA)之發放、撤銷及內控有無疏失等，均有深入瞭解調查之必要。

經調閱數發部、中華電信及審計部等機關卷證資料，並於115年3月6日詢問相關主管人員，已調查完畢，茲臚列調查意見如下：

一、數發部主責政府機關公開金鑰基礎建設(GPKI)業務，並連同政府伺服器數位憑證管理中心(GTLSCA)委由中華電信營運，攸關全國政府網站及公共數位服務之信任基礎，114年5月30日卻爆發Google Chrome預告於同年8月1日起撤銷憑證信任情事，嚴重衝擊政府數位治理形象；經查，該部最早於113年3月工作會議即已掌握風險徵兆，惟該部斯時對於違反國際憑證規範(Baseline Requirements，BR)之撤銷時效，既未意識其嚴重性，也未見要求中華電信積極強化檢核及大量撤銷機制或要求團隊人力調度等作為，導致政府數位信任形象受損，各行政機關所耗費之行政成本更是難以估計。基此，中華電信於本案顯有處置不當，惟數

可能用來在任何網路上建立安全、加密的通訊管道的技術。但是，SSL 是一種較舊的技術，其中包含一些安全性漏洞。Transport Layer Security (TLS) 是 SSL 的升級版，解決了現有的 SSL 弱點。TLS 以更有效率的方式驗證身分，並繼續支援加密的通訊管道。(https://aws.amazon.com/tw/compare/the-difference-between-ssl-and-tls/)

[5] 中華電信公開金鑰基礎建設(Chunghwa Telecom ecommerce Public Key Infrastructure, ePKI)

[6] https://tw.news.yahoo.com/share/74adcc78-434f-3083-ae43-510d7e6d1bc5

發部於數位信任基礎建設之風險覺察及管理亦有未當，違失明確，應確實檢討。

(一)本案緣於2025年5月30日Google Chrome於Security Blog刊出「維持數位憑證安全-Chrome根目錄即將推出的變更」[7]公告，內容略以:「由於過去一年觀察到的令人擔憂的行為模式……，中華電信作為Chrome根目錄中CA擁有者的可靠性信心已下降。這些模式代表完整性的喪失,未達預期,侵蝕了這些CA擁有者作為Chrome預設受信任的公開憑證發行者的信任」。為此，Chrome瀏覽器預告於114年8月1日零時起不再預設信任中華電信所簽發之ePKI及HiPKI等TLS憑證，而政府網站憑證機構GTLSCA既繫屬於ePKI，其影響遍及數千個政府機關及公共服務網站。

1、一旦GTLSCA所簽發之憑證遭到瀏覽器撤銷預設信任，使用者倘以Chrome瀏覽器瀏覽前開網站，除無法進入頁面外，更將出現警告畫面，並顯示「攻擊者可能嘗試從〇(IP)竊取你的資訊(例如密碼、郵件或信用卡資訊)」等訊息，基於Chrome瀏覽器市占率高達72%[8]，幾乎壟斷瀏覽器市場，此舉對政府網站及公共服務之影響極鉅。

2、憑證失效之具體影響，數發部於114年1月20日發布新聞稿[9]之舉例略以:「民眾連線臺鐵訂票系統時將被瀏覽器(如Chrome、Edge、Safari等)判別為不可信任網站，而讓民眾誤解臺鐵訂票系統為詐騙、惡意網站，甚至瀏覽器阻擋民眾使用臺鐵

[7] https://security.googleblog.com/2025/05/sustaining-digital-certificate-security-chrome-root-store-changes.html
[8] https://www.techbang.com/posts/125755-chrome-market-share-openai-threat
[9] https://moda.gov.tw/press/press-releases/15076

訂票系統，影響民眾權益」，已敘述甚明。

3、根據中華電信查復[10]，GTLSCA於114年5月1日之有效憑證達11,409個，如未採取因應作為，所有憑證[11]均會於114年8月1日零時起失效。

4、基於前開Google Chrome公告並未具體揭露中華電信違反CA/B Forum所制定之BR具體條文，經本院請數發部及中華電信說明[12]113年3月以來GTLSCA違反BR條款情形並綜整如下表1，其中較嚴重之樣態主要可以分為兩種：

表1　GTLSCA違反BR條款情形

日期	事件編號	違反條款	說明
113/3/22	1887096	違反 Baseline Requirements 7.1.2.7.6	憑證延伸用途(Extended Key Usage, EKU)欄位標示錯誤
113/4/19	1892419	違反 Baseline Requirements 4.9.1.1第12款	憑證EKU錯誤的憑證延遲撤銷
113/5/28	1899466	違反 Baseline Requirement 7.1.2.11.5	憑證物件識別碼(Object Identifier, OID)使用886國碼錯誤
113/6/17	1903066	違反 Baseline Requirements 4.9.1.1第12款	憑證OID使用886國碼錯誤的憑證延遲撤銷
113/9/3	1916392	違反 Baseline Requirements 7.1.2.7.4	憑證含2層位置資訊的格式錯誤
114/2/6	1946414	違反CCADB規範6.4	2023稽核自評表缺交
114/2/6	1946418	違反CCADB規範6.4	2024稽核自評表缺交
114/3/27	1956910	違反 Baseline	GTLSCA未完整檢查憑證

[10] 中華電信114年8月7日信規資訊字第1140000316號函。

[11] 一個網站或服務可能同時使用多張憑證，因此憑證數量不等於受影響網站數量。

[12] 中華電信114年8月7日信規資訊字第114000316號函。

日期	事件編號	違反條款	說明
		Requirements 3.2.2.8	授權核發的CA，導致誤發憑證
資料來源：中華電信			

（1）憑證格式違規。

〈1〉113年3月22日發生EKU欄位標示錯誤情形，共影響6,450張憑證不符BR。

〈2〉113年5月28日發生使用886國碼錯誤情形，共影響12,911張憑證不符BR。

（2）未能於時效(5日)內撤銷格式錯誤之憑證。

〈1〉因EKU欄位標示錯誤所影響之6,450張憑證未能於5日內撤銷。

〈2〉因使用886國碼錯誤所影響之12,911張憑證未能於5日內撤銷。

(二)由於數發部114年1月20日發布新聞稿[13]稱：「數發部職掌之一為維護我國電子金鑰GPKI架構，並發放政府網站憑證(GTLSCA)，作為政府機關網站身分辨識及資料傳輸加密之數位基礎，此政府網站憑證適用於對象為gov.tw所轄各級政府網站，包括臺鐵訂票系統……」等語，然而該部於本案事發後又對外表示[14]：「……是中華電信在管理面與作業面的恢復機制沒處理好，……而數發部與中華電信僅為委外契約關係，並非督導關係」等語，明顯前後矛盾。數發部雖稱：「係協助各機關統一採購TLS憑證服務，並委託中華電信於其商用根憑證下建置GTLSCA，……在運作上實質獨立於GPKI範疇」云云；惟包含GTLSCA在內，數發部共有6個憑證機構委由中華電信營運[15]，且均屬政府數位公共服務之重要基礎，

[13] https://moda.gov.tw/press/press-releases/15076

[14] https://finance.ettoday.net/news/2971609

[15] 審計部114年7月31日台審部六字第1140020118號函。

影響極為鉅大，數發部之責任及作為不宜自我限縮為契約關係，應先敘明。

1、依據113年11月13日修正通過之「數位發展部處務規程」第10條第8項規定，該部數位政府司掌理「政府數位基礎建設與其運作韌性之規劃、協調及管理」。對此，該部查復[16]說明，數發部負責政府機關公開金鑰基礎建設(GPKI)業務，辦理政府憑證總管理中心(GRCA)、政府憑證管理中心(GCA)、組織及團體憑證管理中心(XCA)，並協調其他目的事業主管機關建置相關憑證機構(MOEACA、MOICA、HCA)，TLS憑證並不在其中。

2、次查政府憑證管理中心(GCA)網站對於GTLSCA則說明略以：「數位發展部為政府憑證管理中心的主管機關，中華電信數據通信分公司受數位發展部委託，負責政府憑證管理中心之維運」，此外，政府伺服器數位憑證管理中心(GTLSCA)於108年7月19日成立，係中華電信公開金鑰基礎建設(ePKI)之下屬憑證機構。

3、復據數發部與中華電信於113年11月19日生效之「113年度政府公開金鑰基礎建設服務後續擴充」契約(契約編號ZD113057)，合約內容包括營運三項CA，包括GRCA、GCA以及XCA，政府網站所需之TLS憑證採購作業亦併入該案執行，整體契約金額為新臺幣(下同)3,200萬元。經查政府憑證總管理中心(GRCA)網站[17]顯示，政府機關公開金鑰基礎建設(GPKI)係依據電子化政府推動方案(90至93年度)，為健全電子化政府基礎環境建設，

[16] 數發部114年8月7日數位政府字第1140018757號函。

[17] https://grca.nat.gov.tw/02-01.html

建立行政機關電子認證及安全制度而設立。目前除醫事憑證管理中心(HCA)之外，中華電信共接受數發部委託營運6個憑證機構[18]，包括政府憑證總管理中心(GRCA)、政府憑證管理中心(GCA)、組織及團體憑證管理中心(XCA)、自然人憑證管理中心(MOICA)、工商憑證管理中心(MOEACA)及政府伺服器數位憑證管理中心(GTLSCA)。

4、對於數發部於GTLSCA維運之職責及其邊界，該部葉寧次長於本院詢問時亦補充如下：

（1）我們能用的手段是契約手段，但作為採購政府憑證的機關，我們也會利用行政指導手段促請改善。

（2）我認同(在契約手段之外)應該有更好的控管。

(三)再查，由於憑證機構(CA)對於BR合規性事件必須上Bugzilla論壇報告並接受會員檢視，若無法完整交代事件原因並提出可杜絕錯誤之檢討措施，將使瀏覽器對於CA之信任造成進一步侵蝕，最終導致撤銷信任。而本案於113年3~6月間發生兩次大量憑證格式錯誤事件均無法於5日內撤銷，於Bugzilla論壇上已引起會員嚴重責難；惟檢視數發部與中華電信之工作會議紀錄，該部斯時對於違反BR撤銷時效既未意識其嚴重性，也未見要求中華電信積極強化檢核及大量撤銷機制，實為GTLSCA遭撤銷信任之根因，顯有缺乏風險控管意識之違失。

1、茲摘述兩次事件處置過程中，中華電信GTLSCA於Bugzilla遭受其他會員責難情形[19](中華電信提供，本院自行翻譯)：

---

[18] 114年8月7日中電信公司信規資訊字第1140000316號函。

[19] https://www.bugzilla.org/

（1）在整個錯誤中，你(指中華電信)沒有提供任何行動項目來解決事件的真正根本原因，也就是中華電信未能根據BR，履行其作為公共CA的責任。

（2）整整1個月過去了，你又宣布有意拖延撤銷期限。你已經晚了兩週才申請撤銷，而且你還打算再拖1個月，針對超過8,000張憑證。

（3）故意延遲撤銷的原因從來不是關於憑證用戶，用戶的流程、系統、使用情境、無能、資源不足或不良態度都無法阻止準時的撤銷。唯一導致延遲撤銷的原因是CA管理不善及決策錯誤，這次是中華電信決策失敗。

（4）(針對中華電信回復因用戶都是政府機關，且立即撤銷可能影響機場管制監控系統正常運作等)遭會員指出簽發憑證用於航空飛行及控制系統，已同時違反ECA CP及GTLSCA CPS(均為中華電信自訂之憑證簽發政策或規定)，而遭質疑未誠實說明。

（5）如果你無法撤銷已簽發的憑證，那你就不適合成為CA，這是成為CA的主要要求之一。

（6）針對中華電信表示需要一些時間聯繫各政府機關窗口以更新憑證，會員則表示：這完全違反了BR，這是你嚴重的疏忽，我希望你能提供保證，說明你如何調合BR義務和政府壓力。一般來說，在需要撤銷憑證的案件中，你在得知事件後有24/120小時的時間和用戶溝通，但撤銷日期不能根據用戶的要求更改。此規定並未提供例外條款。

2、據中華電信函復，數發部每月定期召開專案會議審查該公司所提交之營運報告，並視需要不定期

舉行會議，茲摘述113年3~6月工作會議內容如下，由該工作會議紀錄顯示，數發部斯時對於違反撤銷時效(5日)之嚴重性尚未充分認知。

（1）113年3月工作會議決議第3點：「有關GTLSCA之TLS憑證格式錯誤一事，請團隊協助回報Bugzilla並向本部報告後續處理計畫，待本部同意後於網站公告並以電子郵件通知憑證用戶。」

（2）113年4月工作會議決議第2點：「有關GTLSCA之TLS憑證格式錯誤一事，共影響6,450張憑證，至4月18日新憑證下載數量已達3,637張，請團隊持續追蹤並聯繫憑證用戶儘速更新，以確保網站安全性。」

（3）113年5月工作會議決議第1點：「有關GTLSCA之TLS憑證格式錯誤一事，共影響6,450張憑證，至5月13日已將受影響的憑證全數廢止、換發，請團隊持續協助追蹤Bugzilla上的提問，向本部報告，並經本部同意後再於Bugzilla上回復。」

（4）113年6月工作會議決議第4點：「有關近期TLS憑證廢止一事，至6月20日已廢止12,875張(99.7%)憑證，剩餘的憑證，請團隊提醒相關機關更新憑證，以利後續廢止作業，並於Bugzilla持續追蹤有關本案的incident report，積極回應相關提問以免影響Google同意GTLSCA-G2憑證植入Chrome之意願。」

3、至於數發部葉寧次長於本院詢問時說明無法於5日內撤銷憑證之原因略以：「安裝憑證是各機關各自處理，因此6,000多個政府網站各自安裝就來不及在5天內完成，第2次事件也雷同」，該部

王誠明司長亦補充:「以(撤銷憑證的)能量來說5天不是控制在CA，而是各機關網站管理者」云云，顯然仍未意識到CA/B Forum及其所制定的BR，對於撤銷時限沒有訂定任何例外或豁免條款，瀏覽器廠商基於資安考量也不會接受任何類似理由；爰此，如何使各機關於5日內完成憑證轉換以達成BR之合規性，完全是數發部與中華電信必須研謀解決的事項，俾符合「業務可以外包，責任不能外包」之原則。

(四)此外，數發部函復雖說明係於「114年1月18日始獲悉Chrome瀏覽器將撤銷GTLSCA信任，並立即採取對策」云云，惟瀏覽器廠商撤銷信任之決定並非單一事件造成；事實上，數發部於113年6月工作會議已認知到兩次違反憑證撤銷時效可能影響Google同意GTLSCA憑證植入Chrome之意願，至113年10月處理層級雖已提升至司長，至114年2月11日處理層級再提升至次長。由相關會議資料顯示，數發部應變舉措包括要求撤換專案經理並備妥備用憑證等，益證數發部於本案所能運用之工具及強度絕非僅止於契約關係，惟期間該部與中華電信仍未針對兩次違規之根因，包括「憑證格式檢核機制」及「大量撤銷憑證機制」研擬具體解決方案，顯示數發部及中華電信之應變處理量能仍有未洽。

1、有關數發部最早係於何時獲悉可能遭Google Chrome撤銷憑證機構信任，根據該部於本院詢問前查復，Google Chrome於114年1月18日通知中華電信憑證團隊:「因未見實質改進承諾，且發現中華電信持續未能充分理解並達成Google Chrome根憑證計畫政策與BR最低合規要求，故無法核准中華電信簽發GTLSCA憑證」等語。

2、惟查，數發部與中華電信113年6月20日召開之該月份工作會議已有決議指出略以:「有關近期TLS憑證廢止一事，……以免影響Google同意GTLSCA-G2憑證植入Chrome之意願」等語。

3、至113年10月22日，數發部召開「GTLSCA用戶憑證效期縮短為90天因應方案」會議，處理層級提升至司長，會議決議略以：

（1）有關TLS憑證效期，請中華團隊與Browsers爭取影響較小的方案，如有相關資訊請通知數發部，並於協商結果確定後，向該部說明應對之規劃，以減少對GTLSCA用戶之影響。

（2）如與Browsers協商結果為中華電信商用(CHT OVCA)憑證(下稱商用憑證)效期維持1年而GTLSCA憑證效期縮減，全國機關得透過GTLSCA申請商用TLS憑證，並請中華電信團隊維持(至多)15,000張有效之商用TLS憑證。

（3）因Browsers對TLS憑證要求日趨嚴格，且今年GPKI專案執行期間有3次因格式不符而大批量廢止TLS憑證，為維護專案品質，減少對各機關之影響，請由商用憑證團隊負責GTLSCA之維運，並建請中華電信提供更為合適之專案經理人選。

4、數發部嗣於接獲Google通知後，於114年2月11日開會研商「GTLSCA不受Chrome瀏覽器信任因應會議」，處理層級提升至次長。會議決議略以：

（1）為降低減少GTLSCA不受Chrome瀏覽器信任對政府機關之衝擊，以下兩方案將同時進行：

〈1〉方案一：爭取Google同意以HiPKI(中華電信第二代憑證)簽發GTLSCA-G1(第一代憑證)，請配合辦理以下事項：

〈2〉因應Google可能不同意方案一，請中華電信團隊提早規劃及辦理換發商用憑證事宜(如憑證之簽發、新憑證安裝說明等)，於今年3月10日前，以大量GTLSCA申請資料自動轉入商用憑證OVCA簽發機制之方式，備妥1萬5千張商用憑證供政府機關網站備用。

(2)請中華電信團隊以技術面的角度提供GTLSCA-G2未受Google信任及GTLSCA改以商用憑證簽發之說帖，以應對外界可能衍生之質疑。

(3)為提升GTLSCA團隊專業及運作量能，請中華電信資訊技術分公司儘速合併商用憑證團隊及政府憑證團隊，更換專案經理，並補充足夠人力。

(五)另查，根據前述「GTLSCA不受Chrome瀏覽器信任因應會議」會議結論，數發部隨即要求中華電信無償提供1萬5千張商用憑證備用，並同時以8,300萬元向「臺灣網路認證股份有限公司」(下稱TWCA)採購2年不限數量之商用TLS憑證簽發服務，以建立雙憑證系統；該部嗣於114年3月21日以數位政府字第11440004011號函通知各機關導入雙憑證，以確保政府網站及服務不致中斷，茲臚列辦理情形如下；而該部雖稱雙憑證政策及相關採購經費屬於既定政策，並非本次事件之衍生成本，惟所謂雙憑證機制仍需機關網站管理者逐一手動啟用，並非自動化備援，本次事件對於全國行政機關及公共服務網站管理者仍損耗難以估計之行政成本。

1、數發部補充說明，該部向TWCA採購2年不限數量之商用TLS憑證簽發服務，採購費用8,300萬元，分別由「深化政府資通訊應用建設」及「健全政府數位服務基礎環境及人力培力」支應。

2、有關該部向中華電信要求1萬5千張商用憑證備用之後續辦理情形及其價值，該部於詢問前補充說明，實際使用憑證共計7,871張，總價值約4,700萬餘元；經本院於詢問時向中華電信查證，中華電信江彬榮科長表示：「沒有對外採購，沒有額外成本所以沒有列（會計帳）」等語，故不列入本次事件之衍生成本。

3、有關雙憑證系統之備援切換方式，數發部及中華電信分別說明如下：

（1）數發部：需由機關管理單位啟用憑證，因此無法由外部協助其自動完成切換。

（2）中華電信:現有網站服務管理員僅能在設定檔上設定1張憑證，無法自動進行憑證備援切換。

(六)綜上，GTLSCA所簽發之TLS憑證係政府網站及公共服務運作所必須，數發部雖係代替所有政府機關採購憑證並包裹於GPKI委外營運契約中，並對外聲稱本次事件「數發部與中華電信僅為委外契約關係」云云；惟本案涉及層面及影響鉅大，又政府機關資訊服務委外情形極為普遍，該部作為推動數位發展及資通安全之主管機關，其責任切割方式難為其他機關表率。此外，Google Chrome決定撤銷中華電信憑證信任，並非單一事件所致，亦非短時間內決策，而係GTLSCA於113年上半年一連串違反合規性之事件所導致，包括6千餘張及1萬餘張之憑證格式錯誤，且兩次事件均未於5日時效內完成撤銷；數發部於斯時雖意識到有造成信任損害之虞，惟並未充分認知該等合規性問題之嚴重性，亦未積極研擬憑證檢核工具導入及大量撤銷機制，後續縱然逐步提升處理層級及強度，仍無法改變Chrome撤銷信任之決定，爰該部之風險管理及覺察敏感度亦有檢討空

間。

二、數發部為掌握中華電信營運GPKI及GTLSCA情形，設有相關管理措施，包括外部稽核、營運報告、工作會議及契約罰則等等，惟前述措施於本次憑證信任撤銷事件中並未發揮預防功能；經查原因包括定期稽核難以因應全自動化即時檢核、契約或營運期間未具體要求充分導入憑證檢核工具，以及未事先訂定大規模撤銷之授權層級等複合式因素；此外，GPKI及GTLSCA均未納入「國家關鍵資訊基礎設施」防護架構管理，於風險識別、系統相依性評估及持續營運等亦有相當程度影響，該部實宜秉持資通安全持續精進之精神予以通盤評估，以杜類案肇生。

(一)依據資通安全管理法第9條規定:「委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗等」；經查[20]GPKI常態性委外辦理已行之有年，數發部為掌握中華電信營運情形，並符合日趨繁複之資安及採購法遵性，近年契約內相關管理措施亦有逐年漸趨嚴謹完善的趨勢，以下摘述相關管理措施之強化及執行情形。

1、GPKI(含GTLSCA)委外營運係常態性辦理(110年時由國家發展委員會承辦)，歷年合約名稱及金額整理如下表2：

表2 GPKI近年委外合約簡表(數發部提供，本院自行整理)

年度	合約名稱(案號)	金額(元)	生效日
110	政府公開金鑰基礎建設委外服務案(110092711)	34,300,000	110年9月27日
111	政府公開金鑰基礎建設委外服務案(modaz111002)	29,387,700	111年12月16日
112	政府公開金鑰基礎建設服	37,150,000	112年9月28

[20] 數發部詢問前提供資料，未備文。

年度	合約名稱(案號)	金額(元)	生效日
	務案(ZD112032)		日
113	政府公開金鑰基礎建設服務後續擴充案(ZD113057)	32,385,000	113年11月19日
114	政府公開金鑰基礎建設服務案(ZD114026)	43,630,000	114年10月21日
數發部提供，本院自行整理			

2、根據審計部[21]查復資料，數發部為確保GPKI所屬憑證機構之運作符合GPKI憑證政策與實務作業基準，及相關法規或規範，經建立稽核制度，每年委託第三方(安侯建業聯合會計師事務所，下稱KPMG)辦理憑證機構外部稽核作業（111至113年度委辦金額分別為659萬餘元、659萬餘元及691萬餘元），其中113年10月稽核報告發現如下，顯示外部稽核確有發掘問題及評估影響程度之能力。

（1）依據WebTrust for SSL BR 5.3之8規範：CA判斷憑證出現的任何資訊不正確時，需於5天內撤銷用戶憑證。書面審查「數據營運及資安應用處簽」並勾稽「業務資通安全事件通報單」、「矯正措施處理單」後發現，113年3月19日之事故於113年5月13日完成廢止；113年5月23日之事故於113年6月28日完成廢止，均未於5日內完成廢止作業，與稽核標準要求不符。

（2）可能影響：未依據標準要求時限內完成憑證廢止作業，可能影響憑證信任鏈，導致客戶網站均無法運作。

3、另查，數發部係於113年11月19日生效之「113年度政府公開金鑰基礎建設服務後續擴充」契約新

[21] 114年8月12日審計部台審部六字第1140019478號函。

增諸多涉及違反BR之違約罰則，茲臚列如下。數發部亦因中華電信於本案違反「被外界發現TLS憑證不符最新BR標準」，而處以50萬元之違約金。

(1)「113年度政府公開金鑰基礎建設服務後續擴充」契約中，違約評估涉及GTLSCA及TLS/SSL信任之項目摘述如下表3：

表3 「113年度政府公開金鑰基礎建設服務後續擴充案」涉及CA及TLS/SSL信任之違約項目。

評估項目	評斷方式	要求基準	違約金計點
資安指標	對於所維護之憑證管理中心，未取得WebTrust for CA驗證	通過驗證	未通過計罰350點
服務水準	被外界發現TLS憑證不符最新BR標準	1次	每次計罰100點
	自行發現TLS憑證不符最新BR標準	1次	每次計罰60點
	於Bugzilla建立事件報告	依Common CA Database規定，GTLSCA發現事件時應於72小時內於Bugzilla建立初步報告(initial report)，如果完整的事件報告尚未準備好應提供初步報告(preliminary report)，並於事件發生後兩週內發布完整的事件報告。	每逾1日計罰10點
	及時回復Bugzilla上與GTLSCA的提問	依Common CA Database規定，應於一週內回覆	每逾1日計罰2點

註：每點違約金金額為伍仟元。

數發部提供，本院自行整理

（2）次據中華電信查復[22]及數發部說明[23]，因於114年3月26日被Google(外界)通知部分GTLSCA所核發之TLS憑證，CAA紀錄不符最新BR規範，依據契約第15條第3款規定，若被外界發現TLS憑證不符最新BR標準，每次計罰100點，每點違約金金額為5,000元，故處以違約金50萬元，中華電信無另提起申復或行政救濟措施。

(二)在定期稽核難以因應全自動化即時檢核部分，查近年外部稽核報告顯示，每年外部稽核作業係定期於10月份左右辦理，其中112年10月份完成之外稽報告並未指出GTLSCA有違反BR合規性之風險，直至中華電信於113年3至5月間發生合規性問題後，113年度10月完成之外部稽核報告始具體指出問題並要求中華電信提出矯正預防措施；換言之，外部稽核並未發揮事前預警之功能。對此，數發部說明：「國際瀏覽器廠商（如Google）已全面導入高度自動化的Linting（語法檢查）工具，採全時段、逐筆方式檢核，傳統外稽方式難以即時捕捉到合規風險」等語，雖屬實情；惟數發部既已挹注經費於外部稽核，仍宜設法與外部稽核及營運機構密切合作，以提升稽核效能，降低風險覺察落後之情形。

(三)此外，基於憑證格式錯誤需於極短時間(視情形於1日或5日內)內撤銷，有效的源頭管理策略是在憑證製發前以軟體工具進行複式檢核，以嚴格控制其合規性。經查本案契約或營運期間，數發部僅於契約中要求營運單位符合最新BR規範，並未具體要求營運單位充分導入憑證檢核工具。而中華電信於事件

[22] 中華電信114年8月7日信規資訊字第1140000316號函。
[23] 數發部114年5月22日數位政府決字第1144000845號函。

發生之前，係採用ZLint[24]和自行研發之檢核工具合計兩道把關程序；惟本院於114年1月14日參訪TWCA獲悉，該公司已長期運用PKIlint[25]、ZLint及一套自行研發之檢核工具，合計三道把關程序，較能有效降低憑證格式錯誤之機率。對此，中華電信說明已於事件後導入PKIlint，並於114年底再導入第4套檢核工具，應可有效降低憑證格式錯誤情形，而從源頭降低需撤銷大量憑證之風險。

(四)另查，以本案兩次合規性事件為例，需於5日內撤銷之TLS憑證高達6千及1萬餘張，且均涉及政府網站及公共服務，若未於事前定義事件規模、依規模設計撤銷授權層級並預擬動員計畫，於事件發生時將無法逕依劇本快速應變；經本院調查後，數發部及憑證機構(中華電信及TWCA)已合作完成撤銷作業設計如下，應可有效提升應變速度。

1、中華電信已訂定大量憑證撤銷之標準程序，並於114年11月進行大量憑證撤銷演練且經過WebTrust for CA的合格外部稽核認可，已確認該公司具備此管理及技術能力。

2、預防性規範與程序標準化：

（1）明確告知用戶義務：憑證申請頁面明確規範：若發生不符BR規範之情事CA具備於24小時（安全性事故）或5天（一般錯誤）內強制廢止憑證之義務，如無法立即更換，用戶應主動告知管理中心延遲原因，並配合儘速辦理憑證更換與廢止作業。

---

[24] ZLint是一個用Go編寫的X.509憑證linter，它檢查憑證是否符合標準（例如RFC 5280）和其他相關的PKI要求，例如CA/瀏覽器論壇基準要求(https://github.com/zmap/zlint)

[25] PKIlint是一個針對使用ASN.1編碼的文件的linting框架。PKIilint被設計成一個高度可擴展的工具組，可以快速創建針對各種ASN.1結構/「文件」類型的linter，以檢查是否符合各種標準和策略。(https://github.com/digicert/pkilint)

（2）憑證大規模廢止計畫與用戶配合事項：TWCA已制定憑證大規模廢止計畫，內容具備全面性作業框架，涵蓋事件應變、用戶溝通，以及憑證廢止與替換流程，確保所有作業皆符合BR和各根儲存庫(Root Program Store)的政策規範。

3、危機發生時之應變機制：

（1）主動分級通報：第一時間透過系統清查受影響機關，並發送緊急通知。

（2）建立延遲廢止申報機制：若機關評估立即更換將導致重大服務中斷，應依據BR規範程序提出「延遲廢止說明」，由憑證管理中心彙整後向國際瀏覽器供應商（如Google、Mozilla）進行合規說明，以爭取緩衝時間。

4、授權層級：

（1）策略決策層：由數發部次長決定全國大規模網站憑證換發之政策制定及跨部會溝通等工作。

（2）執行管理層：由TWCA副總經理負責核准該公司執行大規模廢止計畫、督導應變處置以及審核延遲廢止之申請案件審核進度。

（3）在中華電信部分，大量憑證撤銷通報及授權層級為該公司憑證政策管理委員會主席，現為資訊技術分公司副總經理，但若涉及憑證數量龐大或影響重大時，應再向資訊技術分公司總經理呈報，並由分公司總經理視情節輕重決定是否需向總公司請示應變方案。

(五)再查，GPKI及GTLSCA之營運並未納入國家關鍵基礎設施安全防護架構下進行管理，有其潛在風險。事實上，GPKI及相關憑證簽發與管理體系(如GTLSCA)於本案已顯露出具有支撐跨機關資通服務安全運作及公共服務之特性，且一旦失效將導致大規模數

位服務信任中斷，其失效影響性及系統相依性十分接近「國家關鍵基礎設施安全防護指導綱領」中對於國家關鍵資訊基礎設施(CII)之定義[26]，然而現行指導綱領對CII之界定，仍以「支撐實體基礎設施」為核心思維，尚未充分反應數位政府與網路服務對於憑證、身分驗證及信任體系之高度依賴，致使具橫向影響力之數位信任基礎設施，囿於定義未臻明確，而未以關鍵基礎設施之思維進行風險管理，有賴數發部與行政院國土安全辦公室進一步合作予以評估。

1、「國家關鍵基礎設施安全防護指導綱領」所揭示之目標包括「維護國家與社會重要功能持續運作，確保攸關國家安全、政府治理、公共安全、經濟與民眾信心之基礎設施與資產的安全。」以及「以全災害為安全防護考量，掌握設施相依性，辨識潛在威脅與災害影響，降低設施脆弱性，縮減設施失效影響範圍與程度，提高應變效率並加速復原」等語，均與GPKI及GTLSCA之失效影響性及系統相依性高度相關。

2、根據數發部葉寧次長及王誠明司長於本院詢問時說明如下，顯示目前GPKI及GTLSCA之營運確實尚未納入「國家關鍵基礎設施安全防護指導綱領」。

（1）王誠明司長：因為按照定義，CII要支撐系統營運的資訊系統，GPKI是認證系統，所以沒有納入。

（2）葉寧次長：(經過事件後)我們回去評估是否納

[26] 國家關鍵資訊基礎設施（Critical Information Infrastructure, CII）係指涉及核心業務運作，為支持國家關鍵基礎設施持續營運所需之重要資通系統或調度、控制系統（Supervisory Control and Data Acquisition,SCADA），亦屬國家關鍵基礎設施之重要元件（資通訊類資產），應配合對應之國家關鍵基礎設施統一納管。

入。

綜上，GPKI與TLS憑證體系係政府數位服務之信任基礎，其正常運作為身分驗證與網路通訊之必要前提，一旦失效將導致跨機關服務中斷與整體數位信任崩解；數發部對委託中華電信辦理GPKI及相關憑證中心營運雖設有諸多管理手段，且本案在雙方合作下並未造成實際損害；惟由本案調查仍可發現部分管理盲點，包括外部稽核、契約技術細節、應變授權層級及CII納管之可能性等等，基於「資通安全是持續精進的風險管理」精神，數發部宜視本案盲點為精進契機，以有效控制潛在之系統性及技術性風險。

參、處理辦法：

一、調查意見一及二，函請數位發展部確實檢討改進見復。

二、調查意見一及二，函復審計部。

三、調查意見經委員會討論通過後公布。

四、檢附派查函及相關附件，送請交通及採購委員會處理。

調查委員：賴鼎銘

葉宜津