檢查項目1:	
系統應由安全管道取得	引Root CA的自簽憑證(Self-Signed Certificate),並妥
善安全保存於系統中	
建議做法:	
由 GRCA 網站 https://g	grca.nat.gov.tw/的儲存庫中下載 GRCA2自簽憑證,
· 龙檢查其憑證指紋應為	5 b091aa913847f313d727bcefc8179f086f3a8c0f,オ可
放入應用系統中。	•
	×
一般詳細資料憑證路徑	
顯示(<u>S</u>): <全部>	\sim
48 44	A
欄位 高 右 か 期 列	值 7
	Government Root Certifica
国際公開会論	RSA (4096 Bits)
□□ 公開金鑰參數	05 00
〒主體金鑰識別碼	d5671de09c7a2c9ccbc59
	Subject Type=CA, Path Le
📊 金鑰使用方法	Certificate Signing, Off-lin
	b091aa913847f313d727b 🗸 🗸
b091aa913847f313d727bcefc8179f0	086f3a8cOf 編輯內齊(E) 複製到檔案(C) 確定
驗證結果:□是□否	

檢查項目2:

系統應設定所信賴的憑證保證等級,並檢查憑證之憑證政策(Certificate Policies)欄位所記載的 Policy OID 是否符合憑證保證等級的要求,對於不符保證等級之憑證應拒絕存取(例如正式上線系統應對測試等級的憑證加以拒絕)

建議做法:

由 GTestCA 網站 <u>https://gtestca.nat.gov.tw/</u> 申請測試憑證,並嘗試以該憑證 登入系統,正式系統應拒絕測試憑證登入。

系統應檢查 CA 本身憑證確 Issuer Name (DN)是否與 Roo	為 Root CA 所簽發的憑證 (至少需檢查憑證的 at CA 白然馬路納 Subject Name(DN) 扣符,并
Issuer Name (DN)是否與 Roo	at CA 白ダ馬茲始 Subject Name(DN)扣符,并
以RootCA自簽憑證所記載	的 Public Key 檢驗 CA 太身馮諮的答音)
建議做法:檢視 GRCA2自名	答馮證,並確認其 DN 與答音值正確。
一般 詳細資料 憑證路徑	
顯示(S): <全部> ~	
榴位	^
通数转着 Government Root Cer 回有效期自 2012年9月28日下午 0	P4:58:51
回有效期到 2037年12月31日下午 回主體 Government Root Cer	11:59:59 rtification Autho
国 公開金論 RSA (4096 Bits) 国 公開全論参款 05 00	
■ 主體金銷識別碼 d5671de09c7a2c9ccb	bc598e71d0726 🗸
O = Government Root Certification Authority	
C = 1 VV	
編輯內容(E)	複製到檔案(C)
	確定
■ 憑證	×
一般 詳細資料 憑證路徑	
憑證路徑(P)	
Government Root Certification Authority	
	檢視想證(⊻)
憑證狀態(<u>S</u>):	
這個憑證沒有問題。	
	確定
rk 196 /1 III - II	

檢查項目4:

系統應檢查 CA 本身憑證確實為合法的 CA 憑證(Basic Constraints 欄位標示為 CA 憑證),且憑證之金鑰用途(KeyUsage)欄位允許 keyCerSign 及 cRLSign 的用途

建議做法:

以第二代政府憑證管理中心為例,檢視 GCA2憑證,並確認其金鑰使用方法是 Certificate Signing, Off-line CRL Signing 及基本限制是 Subject Type=CA

● 課細資料 憑證路	RE .	×	
顯示(<u>S</u>): <全部>	~		
欄位 授權單位金鑰識別元 主體金鑰識別碼 CRL發佈點 授權資訊存取 透證原則 金鑰使用方法 基本限制 透證指紋	值 KeylD=d5671de09c7a2c9ccbc598e7 d11867c357fe129a916b5f5f31ea3ec [1]CRL Distribution Point: Distribution [1]Authority Info Access: Access Meth [1]Certificate Policy:Policy Identifier= Certificate Signing, Off-line CRL Signi Subject Type=CA, Path Length Constr 44b9ede7b3f9ed56ff53b7e91e4031f	^	
Subject Type=CA Path Length Constraint=	0		
	編輯內容(E) 複製到檔案(G)	
		定	
N + + 1 - 17 - 17	-		

檢查項目5:

系統應檢查 CA 本身憑證是否在效期內(例如檢查系統時間是否仍落在憑證 所記載的 validity 時間範圍內)

注意:憑證是以世界標準時間(UTC,或稱格林威治時間)來記載 Validity 時間範圍,因此系統不應拿本地時間(Local Time)直接與憑證 Validity 時間範圍相比較

建議做法:

以第二代政府憑證管理中心為例,檢視 GCA2憑證,並確認其憑證效期 (windows 檢視憑證會自動轉換成本地時間)。

憑證		×
-般 詳細資料 憑	證路徑	
顯示(<u>S</u>): <全部>	~	
螺位	信	^
IR III III 笑音读答注	sha256PSA	
Len 数字 周井 本 国 笑音雄法 定管注	sha256	
四 数千和 庆 周 并 仏 同 答 辭 者	Government Root Certification Authority TW	
	2013年1月31日上午 11:22:34	
同 有效期到	2033年1月31日上午 11:22:34	
□ 主體	政府憑證管理中心, 行政院, TW	
📴 公開金鑰	RSA (2048 Bits)	
📴 公開金鑰參數	05 00	~
	編輯內容(E) 複製到檔案(C)	
	確定	
證結果:	□是□否	

檢	查項目6:	
系	統應檢查 CA 本身憑證是否已被	廢止(例如定期下載 Root CA 簽發的憑證
機	構廢止清冊(CARL)檢查憑證廢」	L狀態)
建	議做法:	
以	第二代政府憑證管理中心(GCA2	2)為例,應定期下載
htt	p://grca.nat.gov.tw/repository/CRL	<u>_2/CA.crl</u> 於系統中,並確認 GCA2之憑
證	序號未列於撤銷憑證清單中。	
憑	證撤銷清單	×
	an 物料注册	
	一般 取列肩半	
	撤銷憑證(<u>R</u>):	
	序號	撤銷日期
	2b57edb68ed771bd182b043ab8cbce20	2014年4月23日上午
1	001/42/908000/2000103023001902/000	201344月23日 工干
	撤銷項目(E)	
	欄位佔	
	值()):	
	1	
		確定
卧	浴仕里・□₽□不	
闷双	山沁不・□尺□古	

檢查項目7:
系統應檢查 CARL 是否確實是 Root CA 所簽發(至少需檢查 CARL 的 Issuer
Name (DN)是否與Root CA 自答憑證的 Subject Name(DN)相符,並以Root
CA 白ダ馮塔所記載的 Public Kay 捡脸 (ARI 的发音)
CA日 奴忍亞川 記載的 I ublic KCy 微微 CARL 的 效 早)
建議做法・
檢視下載的 CARL 憑證廢止清單。
- 憑證撤銷清單 × ×
一般 撤銷清單
────────────────────────────────────
個位 值 100000000000000000000000000000000000
□ 资發者 Government Root Certificatio
□ <u>有效日期</u> 2020年9月9日下午 11:30:00
□下次更新 2020年9月11日 上午 12:00:00
圖 医章瓣法病管注 sha256RSA
IIII 2012年和決演界法 SNA200 □ 1000000000000000000000000000000000000
国 CRL 軟目 78682452
圖 憑證指紋 a0fbe05456cae5c6191f55dd
值(<u>A</u>):
確定
「皺諠結末・□ 定 □ 含

檢查項目8: 系統應檢查是否為最新的 CARL(當天公布的 CARL) 注意:CARL 的更新時間是以世界標準時間來記載,因此系統不應拿本地 時間直接與 CARL 的更新時間相比較 建議做法:

檢視下載的 CARL 憑證廢止清單中的有效日期與下次更新,現在時間應落於兩者之間,windows 會自動轉成當地時間。

欄位	值	
版本號	V2	
☐ 簽發者	Government Root Certificatio	
🗒 有效日期	2020年9月9日 下午 11:30:00	
🖾 下次更新	2020年9月11日 上午 12:00:00	
🗒 簽草演算法	sha256RSA	
🛅 簽章雜湊演算法	sha256	
3 授權單位金鑰識別	KeylD=d5671de09c7a2c9ccb	
 G CRL 數目	78682452	
🔄 憑證指紋	a0fbe05456cae5c6191f55dd	
		確定

檢查項目9:

系統應檢查用戶的憑證為合法 CA 所簽發(至少需檢查用戶憑證的 Issuer Name (DN)是否與 CA 憑證的 Subject Name(DN)相符,並以 CA 憑證所記載的 Public Key 檢驗用戶憑證的簽章)

建議做法:

請應用系統提供通過驗證之憑證,並檢視該憑證資料是否能通過憑證的路 徑檢查如下圖。

た担連語への
Ia ÷

檢查項目10:

系統應檢查用戶憑證金鑰用途(KeyUsage)欄位所記載的金鑰用途符合使用 目的(簽章/驗簽,或加密/解密)

建議做法:

請應用系統提供通過驗證之憑證,並檢視該憑證詳細內容是使用符合使用 目的之金鑰用途。

▶ [1] 憑證		\times	▶ 万法 (1997) 📈 📈 📈 🕹
一般 詳細資料 憑證路徑			一般 詳細資料 憑證路徑
顯示(<u>S</u>): <全部>	~		顧示(S): <全部> ~
權位 ③ 主體全論識別碼 ④ 授權資訊存取 ③ 悲體別名 ④ 主體引名 ④ 工程 歸屬壁性 ④ CRL 發佈點 ◎ CRL 發佈點 ◎ 描述 ● CRL 發佈點 ● 250 ●	值 00e466fea424d894383f8a [1]Authority Info Access: A [1]Certificate Policy:Policy I RFC822 Name-gca@gca 30 4c 30 16 06 07 60 86 76 [1]CRL Distribution Point: Digital Signature (80) 22a6fc7633f6764ba1931a 课题內密(E) 複製到檔案(C) 確定		構位 值 个 ④ 主體金鑰觀別碼 e9d8d1ea1e8d693aed7b ④ 授權資訊存取 [1]Authority Info Access: A ④ 憑題原則 [1]Certificate Policy:Policy I ④ 主體月錄屬性 30 4c 30 16 06 07 60 86 76 ④ CRL 酸佈點 [1]CRL Distribution Point: 會 金鵬使用方法 Key Encipherment, Data E 同 漢證指紋 7362d3fe1eab10849d758. ¥ Key Encipherment, Data Encipherment (30)
簽章用憑證	加解密)	用?	憑證
驗證結果:□	是□否		

檢查項目11:

系統應檢查用戶的憑證是否在效期內(例如檢查系統時間是否仍落在憑證 所記載的 validity 時間範圍內)

注意:憑證是以世界標準時間來記載,因此系統不應拿本地時間直接與憑證 Validity 時間範圍相比較

建議做法:

請應用系統調整系統時間至某張可通過驗證之憑證生效時間之前與後,再 嘗試登入系統,系統應拒絕該憑證之登入。以下圖憑證為例,應調整時間 至2015/12/9之前做一次測試,再調整時間至2021/12/10之後再做一次測 試。

示(<u>S</u>): <全部>	\checkmark	
欄位	值	~
🗐 版本號	V3	
」 序號	60c1fae82779a1a8b35674fb	
🖷 簽章演算法	sha256RSA	
🗒 簽章雜湊演算法	sha256	
🎬 簽發者	政府憑證管理中心, 行政院, TW	
🛱 有效期自	2015年12月9日 上午 11:36:08	
🎬 有效期到	2021年12月9日 上午 11:36:08	
四 主語	海路测试出入 政应海路等租出	
1]Certificate Policy: Policy Identifier=2.16.8	386.101.0.3.3	
1]Certificate Policy: Policy Identifier=2.16.8	386.101.0.3.3 編輯內容(E) 複製到檔案	 (C)

檢查項目12:

系統應檢查用戶的憑證是否已被廢止(例如定期下載 CA 簽發的憑證廢止清 冊(CRL)檢查憑證廢止狀態,或透過 OCSP 來檢查憑證廢止狀態)

建議做法:

方法一:系統採取 CRL 進行憑證廢止檢查

至憑證官方網站停用一張原本通過系統驗證之憑證。

隔1日再以該張憑證進行登入/簽章,系統應拒絕該憑證登入/簽章。

至憑證官方網站復用該張憑證。

隔1日再以該張憑證進行登入/簽章,系統應接受該憑證登入/簽章。

方法二:系統採取 OCSP 進行憑證廢止檢查

1. 至憑證官方網站停用一張原本通過系統驗證之憑證。

2. 以該張憑證進行登入/簽章,系統應拒絕該憑證登入/簽章。

3. 至憑證官方網站復用該張憑證。

4. 再以該張憑證進行登入/簽章,系統應接受該憑證登入/簽章。

檢查項目13:

系統應檢查 CRL 是合法 CA 所簽發(至少需檢查 CRL 的 Issuer Name (DN) 是否與 CA 本身憑證的 Subject Name(DN)相符,並以 CA 本身憑證所記載 的 Public Key 檢驗 CRL 的簽章),如果使用 OCSP 查詢,則本項不適用 建議做法:

檢視下載的 CRL 憑證廢止清單,其簽發者應與 CA 憑證 Subject Name 相符。

<u> </u>		
欄位	值	
□ 版本號	V2	-
🛱 簽發者	政府憑證管理中心, 行政院, TW	
🗐 有效日期	2020年9月10日 上午 11:15:02	
🛅 下次更新	2020年9月11日下午 12:00:00	
🛅 簽章演算法	sha256RSA	
🛅 簽章雜湊演算法	sha256	
🗊 授權單位金鑰識別	KeylD=d11867c357fe129a91	
🗊 CRL 數目	78682485	
🔄 憑證指紋	2ab6c3f209febb27ac2c8e796	
		Train and a

檢查項目14:

系統應檢查是否為最新公佈的 CRL(當天公布的 CRL),如果使用 OCSP 查 詢,則本項不適用

注意:CRL的更新時間是以世界標準時間來記載,因此系統不應拿本地時間直接與CRL的更新時間相比較

建議做法:

檢視應用系統下載的 CRL 憑證廢止清單中的有效日期與下次更新,現在時間應落於兩者之間, windows 會自動轉成當地時間。

欄位	值		
□ 版本號	V2		
资	政府憑證管理中心, 行政院, TW	-	
	2020年9月10日 上午 11:15:02		
□下次更新	2020年9月11日下午12:00:00		
靈草演算法 夏	sha256RSA		
📋 簽草雜湊演算法	sha256		
資 授權單位金鑰識別…	KeyID=d11867c357fe129a91		
CRL 數目	78682485		
🗐 憑證指紋	2ab6c3f209febb27ac2c8e796		
՝ 吉(Δ)·			
直(<u>A</u>):			

檢查項目15:

系統應要求用戶對傳送的訊息加簽電子簽章以驗證用戶身分

建議做法:

請應用系統提供可通過驗證的封包,並嘗試修改封包資訊的其中任何一個 字元後,請應用系統再次驗證該封包,應用系統應回應該封包簽章不正 確,並拒絕登入/簽章。

檢查項目16:

系統應具備防止用戶加簽之訊息遭到非法重送(Replay)之功能(例如在加簽 訊息中加入 Challenge-Response 或 Nonce 機制)

建議做法:

請應用系統提供可通過驗證的封包,並請應用系統再次嘗試驗證該封包, 應用系統應回應該封包簽章為重送封包,並拒絕登入/簽章。

檢查項目17:

系統傳送用戶隱私資料時應以強度128 bits 以上的安全通道進行保護(例如 使用 SSL 安全通道或是對傳送的訊息以數位信封加密),若系統未涉及傳 送用戶隱私資料時,則本項不適用

建議做法:

使用第三方 TLS 檢驗,如 <u>https://www.ssllabs.com/ssltest/</u>並輸入應用系統網站,進行 TLS 安全強度檢驗。

驗證結果:□是□否□不適用

檢查項目18:

系統應定期校時,以保持系統時間之正確性(例如定期透過 NTP 自動校時) 建議做法:

檢查系統 NTP 自動校時設定,或是手動變更時間後,確認 NTP 能將時間 校正回正確時間。

檢查項目19~21:

政府憑證附卡授權機制相關驗證(服務已停止)

建議做法:

憑證應用系統無須檢查此項目。

驗證結果:■不適用