中華電信憑證管理中心(PublicCA)

如何確認安裝的憑證效期與簽章演算法

目錄

Internet Explorer	2
Chrome	5
Firefox	9

Internet Explorer

開啟 IE 瀏覽器,以 https 連線至您的網頁(以下以連接中華電信通用憑 - 、 證管理中心網站為範例)

	M		
InPrivate https://public	cca. hinet.net /index.htm	♀ ● C Ø ♥ ● ○ ○ 中華電信通用憑證管理中心 ×	<u>₽</u> ★ ₩
檔案(F) 編輯(E) 檢視(V) 我的最愛((A) 工具(D) 說明(H)		
			<u>^</u>
山華電信涌田馮諮符刊	申由八 1 4512 1.00m		
	SSL憑證服務 HiPKI網路認	瓷套件包 電子識別瓷 安全聯網及保密器服務 儲存庫 問與	塔 English 首頁
	WELCOME to Put	alic CA L	
通用憑證管理中心	WELCOME CO FUN		
 SSL 憑證服務 		通用憑證管理中心(Public Certification Authority,	,PublicCA) 是中
 HiPKI 網路認證套件包 		華電信公開金鑰基礎建設(ecommerce Public Key Intra 的第一層下屬馮證機構(Level 1 Subordinate CA),由中	structure, ePKI) 華電信負書建署與維
		運。提供SSL憑證、電子識別證、證券下單憑證、企業專屬憑	證、應用軟體憑證及
■ 电丁諏別證		RA系統建置等PKI服務,適用於電子商務網路交易、電子化は 易所委的身分認證及資料加解密。通用馮讚管理中心也是唯一	∑府網路申辦或金融交 -本+根馮證機構在台
 安全聯網及保密器服務 		灣,為國內第一家自行開發憑證相關服務、完全掌握核心技術	f與資安管理的憑證機
 儲存庫 	REGARD PROVIDENT	構。	
	【公告消息】		
	• 2016/03/24		
	賀!! 保險經紀人同業公	≧會通過ISO 27001驗證,特別推出「SSL憑證+網站	
	<u>偵防隊」優惠方專案</u> 。		
	• 2016/03/01		~
	<u>即日起凡甲購HINETS</u>	SL <u>憑證可享8折假患,考答戶讀時可享/折假患~機管</u>	
			100% -

ニヽ

點選網址列的安全鎖鎖頭→檢視憑證

- InPrivate @ https://publicca.	hinet.net/index.htm p	✓ ▲ C Ø 中華電信通用憑證管理中心 ×	- □ × ↑ ★ \$
檔案(E) 編輯(E) 檢視(⊻) 我的最愛(A)	■ え 網站識別		^
	Chunghwa Telecom ePKI Root CA 已將此網站識別為:		
	publicca.hinet.net		
	伺服器的這個連線經過加密。 我是否應信任此網站?	子識別訖 安全聯網及保密器服務 儲存庫	問與答 English 首頁
通用憑證管理中心	检視憑證		
 SSL 憑證服務 	通用湯	5證管理中心(Public Certification Authori	ty,PublicCA),是中
■ HiPKI 網路認證套件包	華電信 的第一	፤公開金鑰基礎建設(ecommerce Public Key Ir -層下屬漲證機構(Level 1 Subordinate CA)」 - 周小のに海路、東ス浩明路、路米で開進路、久栄生	nfrastructure, ePKI) 由中華電信負責建置與維
■ 電子識別證	RAA	a供SSL漆题、电子飘动题、超多下半漆题、正来等 統建置等PKI服務,適用於電子商務網路交易、電子	·圖憑證 應用軟體憑證及 F化政府網路申辦或金融交
■ 安全聯網及保密器服務	日本 湯、清	身的身分認證及資料加解密。通用憑證管理中心也是 ⊪國內第一家自行開發憑證相關服務、完全掌握核心	。唯一本土根馮證機構在台 技術與資安管理的馮證機
 儲存庫 	A B B B B B B B B B B B B B B B B B B B		
	【公告消息】		
	• 2016/03/24		
	賀!! 保險經紀人同業公會通過]	<u>[SO 27001驗證,特別推出「SSL憑證+網站</u>	
	<u>偵防隊」優惠方專案</u> 。		
	• 2016/03/01		~
	<u>即口起八中將HINET SSL法證</u>	<u>山亭5尓で度患,名者尸類時可享/尓復悪~懱首</u>	
			€ 100% -

三、 跳出憑證後,請確認憑證效期尚未到期與簽章演算法為 sha256。

憑證	X			
一般詳細資料	憑證路徑			
· · · · · · · · · · · · · · · · · · ·	l			
• 確保遠端電	電腦的識別 1			
發給:	publicca.hinet.net			
资發者:	Public Certification Authority - G2			
有效期自	2015/ 2/ 25 39 2018/ 2/ 25			
	簽發者聲明(S)			
深入了解 <u>憑證</u>				

若簽章演算法顯示為 shal,建議更新為 sha256 憑證。

憑證	×
一般詳細資料憑證路徑	
顯示(2): <全部>	•
欄位	值
圖版本	₩3
南京 報	5h ed h2 a9 ca 10 ff 55 71 f2 1
竇發章演算法	sha256RSA
<u>夏</u> 冀卓雜決演算法	\$18250
□ ● 资發者	Public Certification Authority
	2015年2月25日上午 09:45:13
「「「」有效期到	2018年2月25日上午 09:45:13 🝷
-1-056D04	
SN8250K3A	
	26時の変化 補制列援安化
│ 深入了解 <u>憑證詳細資料</u>	
	確定

Chrome

一、 開啟 Chrome 瀏覽器,以 https 連線至您的網頁(以下以連接中華電信通用憑證管理中心網站為範例)

😓 🗋 中華電信通用憑證管理中// >	
← → C 🔒 https://publicc	a.hinet.net/index.htm 🔂 🖬
中華電信通用憑證管理 PKI資訊安全產品 снт ғ s	中心 PKI SERVICE SL壶ż服務 HiPKI網路認遠套件包 電子講別波 安全時朔及保密器服務 儲存庫 問與答 English 首頁
	WELCOME to Public CA !
通用憑證管理中心	通用過密等導由心(Public Certification Authority PublicCA),号中
 SSL 憑證服務 	華電信公開金鑰基礎建設(ecommerce Public Key Infrastructure, ePKI)
■ HiPKI網路認證套件包	的第一層下屬憑證機構(Level 1 Subordinate CA),由中華電信負責建置與維 運。提供SSL憑證、電子識別證、證券下單憑證、企業專屬憑證、應用軟體憑證及
■ 電子識別證	RA系統建置等PKI服務,適用於電子商務網路交易、電子化政府網路申辦或金融交易所需的身分認證及資料加解密。通用憑證管理中心也是唯一本土根憑證機構在台
■ 安全聯網及保密器服務	澤, 马國內第一家目行開發憑證相關服務、完全掌握核心技術與資安管理的憑證機 構。
■ 儲存庫	【公告消息】
	 2016/03/24< <p>智!! 保險經紀人國業公會通過ISO 27001驗診,特別推出「SSL憑證+網站 值防院 優惠方真窯。 </p> 2016/03/01
	<u>即日起凡申購HiNet SSL憑誇可享8折優惠, 考客戶續購可享7折優惠~機會</u> <u>難得, 欲購從速</u> 。 - 2016/02/22
Certification Authorities Certification Authorities	• 2010/02/23 公告經濟部核定中壁電信憑證總管理中心憑證實務作業基準第1.3版及中壁電 信通用憑證管理中心憑證實務作業基準第1.6版。
	• 2016/01/30

二、 點選網址列的安全鎖鎖頭→詳細資訊→View certificate

🚔 🗋 🕫	e電信通用憑證管理中。 ×		×
← → C	角 https://publicca.hinet.net/index.htm	🔂	Ξ
中華電	publicca.hinet.net X 您與這個網站建立了私人連線 <mark>: 詳細質記</mark>		^
PKI資語	Cookie 參 <u>有1個 Cookie 來自這個網站</u> , 有 0 個 Cookie 來自其他網站	電子識別證 安全聯網及保密器服務 儲存庫 問與答 English 首頁	
	權限		
通用	⑩ 位置: 預設詢問▼	CA !	1
 SSL3 	□】 攝影機: 預設詢問▼	「振遊管理中心(Public Certification Authority ,PublicCA), 是中	- 11
 HiPki 	 ◎ 麥克風: 損設詞問▼ ○ 通知: 預約物問▼ 	「一層下層温證機構(Level 1 Subordinate CA),由中華電信負責建置與編	- 11
 ■ 電子譜 	(提供SSL總證、電子識別證、證券下單總證、並某專屬總證、應用軟體總證及 終統建置等PKI服務,通用於電子商務網路交易、電子化政府網路申辦或金融交	
■ 安全勝	 ② JavaScript: 預設允許 ▼	+需的身分認證及資料加解密。通用您證管理中心也是唯一本土根您證機構在自為國內第一家自行開發憑證相關服務、完全掌握核心技術與資安管理的憑證機	
 ▲ 儲存儲 	➡️ 弾出式視窗: 預設封鎖 ▼		
	➡ 自動下載: 預設詢問 ▼		
	▶ 外掛程式: 預設封鎖 ▼	₿ <u>ISO 27001驗謲,特別推出「SSL憑診+網站</u>	
	Ⅲ) MIDI 裝置完整控制: 預設詢問 ▼		
	網站設定	<u>诊可草8折優惠, 老客戶續購可草7折優惠~機會</u>	
	<u>難得,欲購從速。</u>	-	
	· 2010/02/23 公告經濟部核定 <u>中華電信憑</u> 語	<u> 窗總管理中心憑證實務作業基準第1.3版及中華重</u>	
Certificat Authorit	ion Certification 信通用憑診管理中心憑證實 les Authorities	<u> </u>	
4	• 2016/01/30		+

😓 🗋 中華電信通用憑證管理。			3	x
← → C 🔒 https://pub	licca.hinet.net/index.htm	☆ (Ξ
中華電信通用憑證 PKI資訊安全產品 сн	音理中心 IT PKI SERVICE SSI基验服務 HiPKU網路認證套件包 電子識別證 安全聯網及保密器服務 儲存庫 問與答 English	首3	1mm/	*
 通用憑證管理中心 SSL憑證服務 HiPKI網路認證套件包 電子識別證 	WELCOME to Public CA ! 通用憑證管理中心(Public Certification Authority, PublicCA) 華電信公開金鑰基礎建設(ecommerce Public Key Infrastructure, 的第一層下屬憑證機構(Level 1 Subordinate CA),由中華電信負責題 這。提供SSL憑證、電子識別證、證券下單憑證、企業專屬憑證、應用就 福A系統證置等PKI服務,通用於電子商務關股當、電子一成功關點申謝。 ALS 2015年20日 第二 時代 第二 時代),是中 ePKI 置與約 體憑證 調 構本在	中1) 隹 皮 交 ⇔	+
🕞 💼 🛛 Elements Console S	Sources Network Timeline Profiles Resources Security Audits		:	×
Cverview Main Origin Reload to view details	Security Overview			

三. 跳出憑證後,請確認憑證效期尚未到期與簽章演算法為 sha256。 若簽章演算法顯示為 sha1,建議更新為 sha256 憑證。

X	责證	Ì		The local date	×	
ſ	-	般	詳細資料	慧證路 徑		
			憑證資訊			
		這個	國憑證的使用	目的如下:		
			• 確保速端電	腦的識別		
			發給:	publicca.hinet.net		
			簽發者:	Public Certification Author	ity - G2	
			有效期自	2015/ 2/ 25 30] 20	18/ 2/ 25	
					簽發者聲明(2)	
	3	深入了	解 <u>憑證</u>			
					確定	

憑證	×
一般 詳細資料 憑證路徑	
顯示(3): <全部>	•
欄位	值
日本	₩3 =
日 日本 (1) (1) 日本 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	5h ed h2 a9 ca 111 ff 55 71 f2 1
 □ 號章 雜決演算法 □ 簽發者 □ 有效期自 □ 有效期到 	sha250 Public Certification Authority 2015年2月25日 上午 09:45:13 2018年2月25日 上午 09:45:13 ▼
深入了解 <u>憑證詳細資料</u>	編輯內容(E) 複製到檔案(C)
	確定

Firefox

一、 開啟 Firefox 瀏覽器,以 https 連線至您的網頁(以下以連接中華電信 通用憑證管理中心網站為範例)



二、 點選網址列的鎖頭→「>」→更多資訊



三、 跳出頁面資訊視窗後,點選檢視憑證

🕹 頁面資訊 - htt	tps://publicca.hin	et.net/inde	x.htm		. D X	
〕 一般		● 安全				
網站身分						
網站: 擁有者:	publicca.hinet.n 這個網站沒有提供	et 、擁有者資訊				
驗證機構:	Chunghwa Teleo	om Co., Ltd	i .	檢	視憑證 (⊻)	
- 隱私及歷史記	錄					
我以前瀏覽過	這個網站嗎?		否			
此網站有在我	的電腦中儲存資訊	l (Cookie) 🎚	馬? 否	檢視	Cookie (<u>K</u>)	
我有在此網站	5儲存任何密碼嗎?		否	檢視已;	存密碼 (<u>W</u>)	
技術細節 連線已加密 (技術細節 連線已加密(TLS ECDHE RSA WITH AES 128 CBC SHA、128 位元金鑰、TLS 1.2)					
您正在瀏覽的	您正在瀏覽的網頁在傳送前有經過加密。					
加密功能會講 人看到內容。	加密功能會讓未授權的使用者很難偷聽兩台電腦間傳輸的資訊,所以此頁面在網路上傳輸時很難會有 人看到內容。					
				[說明	

四、 點選「詳細資訊」→您的網站憑證

憑證檢視器:"publicca.hinet.net" ▲	٢
一般 (C) 詳細資訊 (D)	
publicca.hinet.net	
海路總位 (5)	
4 publicca hinet net	
● 通證 =	
· 序號 	
△有效	
欄位值 (⊻)	
■	
	ו
開閉 (<u>C</u>)	J

五、 請確認憑證效期尚未到期與簽章演算法為 sha256。 若簽章演算法顯示為 sha1,建議可更新為 sha256 憑證。

馮	語檢視器:"publicca hinet net"	X
	一般 (G) 詳細資訊 (D)	
	馮證屬級 (H)	
	publicca binet net	
	馮證欄位 (F)	
	⊿publicca.hinet.net	*
	4週間	
	版本	=
	序號	
	憑證簽章演算法	
	證號首	
	2 有效	
	一不早於	-
	欄位值 ()	
	PKCS #1 SHA-256 加 RSA 加密	
	匯出 (公)	
		關閉 (C)
<u> </u>		
洒	證檢視器:"publicca.hinet.net"	×
憑	證檢視器:"publicca.hinet.net"	X
慿	證檢視器:"publicca.hinet.net"	×
慿	證檢視器:"publicca.hinet.net" 一般 (G) 詳細資訊 (D) 憑證層級 (H)	×
憑	聽檢視器:"publicca.hinet.net" 一般 (G) 詳細資訊 (D) 憑證層級 (H) publicca.hinet.net	
一 [證檢視器:"publicca.hinet.net" 一般 (G) 詳細資訊 (D) 憑證層級 (H) publicca.hinet.net	
一	證檢視器:"publicca.hinet.net" 一般 (G) 詳細資訊 (D) 透證層級 (H) publicca.hinet.net	
慿	證檢視器:"publicca.hinet.net" 一般 (G) 詳細資訊 (D) 憑證層級 (H) publicca.hinet.net	
慿	證檢視器:"publicca.hinet.net" 一般 (G) 詳細資訊 (D) 憑證層級 (H) publicca.hinet.net 憑證欄位 (E)	
慿	證檢視器:"publicca.hinet.net" 一般 (⑤ 詳細資訊 (ⅅ) 基證層級 (H) publicca.hinet.net 憑證欄位 (Đ) 序號	
慿	證檢視器:"publicca.hinet.net" 一般 (G) 詳細資訊 (D) 憑證層級 (H) publicca.hinet.net 憑證欄位 (C) 序號 	
慿	□證檢視器:"publicca.hinet.net" 一般 ④ 詳細資訊 ① 憑證層級 (H) publicca.hinet.net 憑證欄位 (E) 愿證欄位 (E) 原號 憑證蓋章庫算法 簽發者	
慿	證檢視器:"publicca.hinet.net" 一般 (G) 詳細資訊 (D) 憲證層級 (H) publicca.hinet.net	
慿	□證檢視器:"publicca.hinet.net" 一般(G) 詳細資訊(D) 應證層級(H) publicca.hinet.net 應證欄位(E) 原號 憑證鉴章演算法 簽發者 a 有效 不里於	
慿	aaa a a a a a a a a a a a a a a a a a	
慿	證檢視器:"publicca.hinet.net" 一般(G) 詳細資訊(D) 應證層級(H) publicca.hinet.net 憑證欄位(D) 原號 憑證簽章演算法 瓷號者 名效 不里於 不完於	
慿	證檢視器:"publicca.hinet.net" 一般(G) 詳細資訊(D) 應證層級(H) publicca.hinet.net 應證欄位(C) 序號 愿證蓋章演算法 臺段者	
匮 []	 融檢視器:"publicca.hinet.net" 一般(G) 詳細資訊(D) 憑證層級(H) publicca.hinet.net 憑證欄位(f) 序號 憑證簽章演算法 查發者 有效 不里於 不曉於 主題 憑證主題公論資訊 欄位值(D) 	
慿	證檢視器:"publicca.hinet.net" 一般(④) 詳細資訊(D) 遼證層級(H) publicca.hinet.net 慶證欄位(E) 愿證欄位(E) 愿證欄位(E) 愿證書童演算法 憂發者 本理於 不晚於 主題 不晚於 里證 忽證主證公論資訊 御位値(O) 2018年2月25日上午(09:45:13) (2018年2月25日上午(01:45:13 GMT)	
慿	證檢視器:"publicca.hinet.net" 一般(④) 詳細資訊(D) 應證層級(H) publicca.hinet.net 應證欄位(E) 序號 憑證整章演算法 臺發者 4月效 不完於 主題 《憑證主證公論資訊 欄位值(O) 2018年2月25日上午 09:45:13 (2018年2月25日上午 01:45:13 GMT)	
慿	建設得器:"publicca.hinet.net" 一般(G) 詳細資訊(D) 源證電級(H) publicca.hinet.net 源證欄位(C) 原號 源證金章演算法 臺發者	
慿	證檢視器:"publicca.hinet.net" 一般(G) 詳細資訊(D) 應證層級(H) publicca.hinet.net 應證欄位(C) 序號 應證證章演算法 查發者 考效 不完於 主題 少憑證主證公論資訊 欄位值(O) 2018年2月25日 上午 09:45:13 (2018年2月25日 上午 01:45:13 GMT)	
慿	證檢視器:"publicca.hinet.net" 一般(G) 詳細資訊(D) 應證層級(H) publicca.hinet.net 應證欄位(C) 序號 應證蓋章演算法 查錄者 a有效 不晚於 主體 ●應證主體公論資訊 欄位值(O) 2018年2月25日上午 09:45:13 (2018年2月25日上午 09:45:13 GMT)	
凄	證檢視器:"publicca.hinet.net" 一般(④) 詳細資訊(D) 海證看級(H) publicca.hinet.net 應證 應證 原號 憑證查章演算法 臺發者 47效 不是於 主題 《憑證主體公論資訊 欄位值(O) 2018年2月25日 上午 09:45:13 (2018年2月25日 上午 01:45:13 GMT)	
凄	建設機視器:"publicca.hinet.net" 一般(④) 詳細資訊(D) 夢認細胞位(D) publicca.hinet.net 夢説 憑證整章演算法 臺設者	
凄	建設視器:"publicca.hinet.net" 一般(④) 詳細資訊(型) 源證眉級(H) publicca.hinet.net 源證欄位(D) 原號 源證查庫算法 臺發者 <	
· · · · · · · · · · · · · · · · · · ·	證檢視器:"publicca.hinet.net" 一般(④) 詳細資訊(型) 應證層級(H) publicca.hinet.net 應證欄位(C) 序號 應證證查演算法 查發書 有效 不完於 主題 少憑證主證公論資訊 欄位值(少) 2018年2月25日上午 09:45:13 (2018年2月25日上午 01:45:13 GMT) (匯出 公)	

您另可善用網站之查詢憑證資訊功能,檢視您所申請的 SSL 憑證資訊。

https://ra.publicca.hinet.net/SSLQueryCert/SSLQueryCert.htm

有關國際間對於金鑰長度與演算法的規定,可參見問與答 https://publicca.hinet.net/SSL-08-06.htm