出國報告（出國類別：會議）

參加 104 年「憑證機構與瀏覽器論壇」(CA/Browser Forum)工作小組會議報告

服務機關：內政部資訊中心
姓名職稱：沈金祥 主任
派赴國家：瑞士
出國期間：104 年 6 月 21 日至 6 月 27 日
報告日期：104 年 9 月 18 日

內容摘要：

本案出國參加 104 年 6 月 23 日至 25 日於瑞士蘇黎世舉辦之「憑證機構與瀏覽器論壇」(CA/Browser Forum)工作小組會議，主要目的係在確保自然人憑證可隨國際瀏覽器規範之更新，可適用於不同瀏覽器並強化其於安全郵件應用。此外，藉予與各國瀏覽器及 CA 廠商共同交換意見瞭解未來發展方向，俾尋求自然人憑證於不同瀏覽器間之互通，並獲取相關安全郵件國際間互通之解決方式。

Mozilla 於會中對電子郵件認證於會中提出新的規範，就我國核發的自然人憑證而言，內政部憑證管理中心應該針對寫入憑證內的所有資訊確認其真偽，既然 MOICA 有要寫入電子郵件並讓用戶使用在安全電子郵件功能上，就應該要對電子郵件進行認證，以確保憑證管理中心的公信力，並為各國瀏覽器認可，可以互通。

另鑑於中國互聯網絡信息中心（CNNIC）濫發數位憑證，Google Chrome 及 Mozilla Firefox 瀏覽器更新不再承認來自 CNNIC 的根憑證與延伸驗證（Extended Validation, EV）憑證，我國各憑證管理中心(CA)發行之憑證務必遵循國際憑證政策(CP)及憑證實務作業基準(CPS)之規範，否則將影響其簽發之憑證於國際主要瀏覽器間之應用。

基於本次出席 104 年 6 月「憑證機構與瀏覽器論壇」(CA/Browser Forum)工作小組會議之經驗與體識，有關內政部憑證管理中心業務之推展及相關事項，謹綜合建議如下：

一、檢討自然人憑證要求民眾將電子郵件地址寫入憑證內有否需要，若必要時則須進行認證方屬安全。

二、我國各憑證管理中心(CA)發行之憑證務必遵循國際憑證政策(CP)及憑證實務作業基準(CPS)之規範，否則將影響其簽發之憑證於主要瀏覽器間之應用。

三、安全性 SSL(Secure Sockets Layer)憑證最大有效期間限制為 39 個月應予正視。

四、歐美各國重視電子簽章驗證，並持續強化製作與驗證之技術及推廣應用。

五、中華電信公司宜研討派員參加 CA/Browser Forum 之策略，以利會議經驗傳承，拓展國際合作機會。

六、邀請 CA/Browser 重要成員會長及立陶宛代表參加國內舉辦之相關國際研討會或參訪活動。

目次

壹、參加會議目的

本案出國參加 104 年 6 月 23 日至 25 日於瑞士蘇黎世舉辦之「憑證機構與瀏覽器論壇」(CA/Browser Forum)工作小組會議，主要目的係在確保自然人憑證可隨國際瀏覽器規範之更新，可適用於不同瀏覽器並強化其於安全郵件應用。此外，藉予與各國瀏覽器及 CA 廠商共同交換意見瞭解未來發展方向，俾尋求自然人憑證於不同瀏覽器間之互通，並獲取相關安全郵件國際間互通之解決方式。

一) 與各國瀏覽器及 CA 廠商共同交換意見瞭解未來發展方向。

「憑證機構與瀏覽器論壇」(Certificate Authority Browser Forum，又名 CA/Browser Forum)，是由憑證管理中心、瀏覽器及作業系統軟體業者自組聯盟。該聯盟 制定 X.509 v3 憑證的發放和管理行業準則，以及信任憑證鏈管理。其指導方針涵蓋於 SSL / TLS 憑證、程式簽署的憑證，以及憑證管理中心的系統和網路的安全性。內政部核發之自然人憑證即依照 X.509 之規範準則辦理，俾利自然人憑證能安全使用不同瀏覽器提供服務。

二) 尋求自然人憑證於不同瀏覽器間之互通，並獲取相關安全郵件國際間互通之解決方式。

本(104)年 4 月 23 日國家發展委員會召開行政機關電子憑證推行小組第 28 次委員會議決議，請各憑證管理中心追蹤各瀏覽器之國際規範，並配合辦理，以避免微軟 IIS 伺服器無法使用自發憑證於伺服器憑證串鏈，及無法收取郵件之 email 如何進行憑證 email 認證流程等問題。 內政部派員參加本次 CA/Browser Forum 工作會議，目的在現場瞭解各會員對未來網路瀏覽器相關稽核基準改變之意見，與中華電信公司(代表我國之該論壇會員，長期經營包含政府 PKI、ePKI 及金融 PKI 業務，也是自然人憑證維運廠商)共同表達我方意見，與各國瀏覽器及 CA 廠商共同交換意見瞭解未來發展方向，俾供內政部憑證管理中心及早準備因應，尋求自然人憑證於不同瀏覽器間互通，並獲取相關安全郵件國際間互通之解決方式。

貳、參加會議過程

一 第一天會議摘要 (6 月 23 日星期二)

1. 中國互聯網絡信息中心(China Internet Network Information Center, CNNIC)申請入會
   雖然中國互聯網絡信息中心(以下簡稱 CNNIC)完成申請的相關文件準備，但是仍有兩個問題：
   1) NNIC 並非中國核准的憑證機構(BR 要求加入的 CA 必須取得該國核准。
   2) 他們同時負責最高網域名稱的核發及 CA 憑證的核發。主席(Dean)示將會請 CNNIC 解釋以上兩點後，再下次會議確認其申請

2. 政策工作小組報告

目標：

i. 讓文件可讀性更高
ii. 讓文件格式相同於 RFC3647
iii. 讓 CA 能在 CP/CPS 中加入相關的政策規定
iv. 描述 EV 憑證的必須項目

待解問題：

i. 廢止問題
ii. 實體安全防護描述

完成事項：

在每個政策描述時，必須參考 WebTrust 及 ETSI 對相關的規範，並設法融入相關規範，避免產生政策衝突。Ben 邀請有興趣的會員參加工作小組會議。

3. 驗證工作小組會議

目標：

i. 描述驗證憑證申請流程所需項目
ii. 驗證 Domain 擁有者身分及處理 EV 的問題

目前狀況：

i. 提出新的 DV 驗證方式
ii. 驗證的方式可從 9 種減為 7 種，其他兩種移至 DV 的驗證
iii. 討論如果能把一個檔案放在網站中，是否就代表擁有該網站的控制權問題，但此方法容易受到攻擊
iv. 有興趣參與討論的會員，可加入 Kirk, Cecilia, Robin or Jeremy 的工作小組

4. 程式碼簽署工作小組

目前狀況：

目前已完成草案制定，仍有兩件事項待討論

最新狀況：

已定義文件格式，且規範金鑰必須儲存於硬體載具

5. 訊息分享工作小組

因主要分享人員未能到會，因此略過討論

6. 微軟根憑證服務(Microsoft Root Program)更新

微軟在 2015/6/2 日發佈新的相關政策，並收集相關的回應後，訂定新的根憑證服務相關規定，並要求各 CA 簽署相關規定回覆資訊。微軟目前有 79 個商用 CA 及 49 個政府 CA 在信任清單中，應用於從 windows 95 至 windows 10 的作業平台中，本次主要變更包含以下項目

i. 更新本服務的加入、持續以及剔除的相關規定及辦法
ii. 描述必須提供的稽核方法、BR 或其他對 CA 相關的規範
iii. 重新定義政府 CA 及商用 CA 的合約，以區分其用途及使用範圍。同意書必須在 90 天內簽署回覆。

在新的作業模式之下，所有的通知均以 email 進行，CA 必須主動提供新的聯絡窗口，否則將會錯過相關的通知及告警訊息。稽核報告所對應的相關準則必須由 CA 方提供，並應能對應到 WebTrust 相關的規範。政府 CA 必須在其限定的

TLD 下簽發憑證，否則就應以商用 CA 的標準進行審查。

Don 建議下屬 CA 的稽核報告必須跟 Root 稽核報告能連結，避免誤會

簽發 DV/OV/EV 的下屬 CA 必須分離，並在其政策中描述其簽發的憑證種類。Eddy 說這對 CA 來說衝擊太大，但 Jody 表示微軟願意讓各 CA 有足夠的緩衝時間來因應。微軟表示這樣不同 CA 的管理，有利於後續如果要廢止的話，有較佳的彈性。

微軟強調會執行此一方案，但也會給足夠的緩衝時間，且 CA 均應針對此方案進行相關的調整修訂。

CA 必須訂定金鑰破解等緊急應變程序，並主動通知微軟，微軟也可主動進行緊急應變程序以去除遭破解的 CA。舊的已加入信賴清單的 CA 不受影響，但是新的要加入的 CA 會依此新的方式審查

憑證內的 CN 雖然不是 BR 中的必要項目，但是微軟的規定仍要求要有 CN，因此 CA 應配合加上 CN。

二 第二天會議摘要 (6 月 24 日星期三)

1. 短效期憑證

Ben Wilson:數年前，我們試著在短時間處理 Diginotar 的 CA 被破解事件，因此提出短效期憑證的概念，甚至其效期短於廢止清冊或 OCSP 發佈頻率，因此不需要有廢止查詢相關資訊。但是 BR 規範該資訊必須存於所有憑證中，但這樣會讓短效期憑證免查詢廢止的加速功能消失。

一些廠商支持這樣的憑證修訂，但一些廠商認為應導入 CT 及 Stable OCSP 來面對憑證廢止的查詢。Ryan 認為這樣的方式對 CT 的憑證信賴鏈會產生衝擊，對 Chrome 來說並不有利。

Mozilla 表示，如果能有專屬 Sub CA 在一定的 DN 範圍內核發此類無廢止訊息的憑證，對 Mozilla 來說用戶體驗會較好，因此不反對在這種情況下發短效期憑證。

2. 展示議題建立、投票、文件修改方式

因為 BR 等文件的修訂，最終只有看到修訂後的文件，但是缺少相關討論的歷程，以致追蹤其修訂的原因變的困難，而議題投票也是類似，只有看到結果，但參與討論的過程都難以看到。因此 Ryan 與 Peter 提出 BR 的修訂方法，以文字形式進行修訂，並可以讓每個人對不同的修訂的意見可以留在上面，並可看到每個議題討論的過程，以確保整份 BR 的修定資訊是完整的。

但是有些人可能會擔心該 GIT 等工具不如原本 pdf/word 這麼方便使用，因此可能要有更方便的工具教學等方法，讓大家都能使用。

3. WebTrust 最新發展

Don 提到以下最新發展

i.WebTrust 委員會上次於 Seattle 開會，主要討論稽核員特許資格及微軟新的要求如何對應至 WebTrust 稽核流程。

ii. 稽核員特許資格：因為近日有 CA 的稽核報告上有錯誤的 WebTrust 標章 (TrustCor)的問題，因此 Don 建議 CA 應該去確認其稽核報告是含有正確的標章資訊，並且是正確的稽核報告，避免稽核員的錯誤導致 CA 變成不受

信任

iii. 因為採用新的 RFC3647 文件格式，以致於 Baseline and Network security audit guidelines 的修訂工作變的較麻煩且緩慢。此外，新的網路安全的要求不是統一格式也導致一些複雜的修訂問題。

iv. 微軟新的根憑證計畫會導致以下問題：(1)稽核員要能完整掌握整個樹狀結構以進行稽核，但稽核員可能被蒙蔽。(2)必須為 EV/DV/OV 設立不同的 CA。(3)針對不同瀏覽器廠商提出新的驗證需求，但這些需求不包含在 WebTrust 稽核，因此取得稽核報告無法讓瀏覽器廠商驗證其需求。

v.

4. 瀏覽器廠商最新訊息

Google：Chrome 和微軟 Edge 將會阻擋混合內容的網頁(阻擋 Blockable 的內容，但讓 Optionally-Blockable 的內容仍然下載)，以避免安全性疑慮。

Opera 目前基於 Chromium 進行開發，因此行為模式會接近 Chromium 計畫的行為模式，包含根憑證的認證。Presto 仍然使用我們自己的根憑證清單，該清單是來自 Mozilla 根憑證機構。Opera 會將 SHA1 的網站標示為未加密的網站，且會加入 EV 憑證的 green bar 顯示模式、以及 CT 的支援。

Mozilla：1024bit 的 root 將在 2016/1/26 的 Firefox 44 版被移除，但仍可手動加回。SHA-1 及 RC4 的警告會出現在 Firefox 37 版。預設會優先使用 HTTPS 的連線，但是一定要提供 Staple OCSP 資訊。

三 第三天會議摘要 (6/25 星期四)

1. 憑證效期展延(Extended Validation)與萬用網域憑證

目前並不允許憑證效期展延(EV)萬用網域憑證，但因為其審查嚴格，應該可以比照 DV 萬用網域憑證來核發。不過之前 Netcraft 會議中，有些網站如 fbsbx.com 就可以讓用戶產生網頁，因此可能就會被偽冒核發憑證。

Ryan 表示，因為 foo.appspot.com 不能代表 appspot.com 的擁有權力，因此 EV 憑證不允許「其他的驗證方式」也就可以避免 foo.appspot.com 的擁有者替 appspot.com 申請萬用網域憑證。Bruce 說 store.com 允許個人擁有自己的 subdomain 如 bruce.store.com，但如果 Bruce 是壞人，他仍然可以受到 store.com 的萬用網域憑證的保護，讓用戶身陷危險而不知。因此 Wayne 建議採用多重網域憑證，而非使用萬用網域憑證，以確保每個網址都是受審核且受信任的。

Opera 認為雖然一開始感覺這個點子不好，不過實際上在使用時，它並不會傷害到其他系統或用戶，因此感覺還好。

2. 憑證透明度 Certificate Transparency 新消息

Ryan 提到 Certificate Transparency 計畫的一些新消息

i.現在有 7 個組織成立 log 收容機制

ii. Chrome 43 和 44 仍會採用寬容的 Log 認定方法

iii. CT 的新政策包括 Chrome 46 版會讓 SCT 的最低數量仍然相同，但至少要有一個是來自 Google；

iv. 取得 Green bar 的條件包括：(1)憑證在 2014 的白名單中(2)憑證有 SCT 且 SCT 仍有效(需來自 Google)(3)憑證有 SCT 且其 SCT 至少有一個是來自 Google)

v. 寬容 Log 認定方法是暫時的，最終仍然會回歸原本的要求，且會 Log 所有的憑證，不是只有 EV。
vi. CT 的目標是 Log 所有的 CA 發的 SSL 憑證，因此 Google 鼓勵 Log 收容中心可以收集所有其他人發出的憑證。CA 不要僅向單一的 Log 發佈憑證，因為系統總是有可能出狀況。
vii. Google 正在進行 CT 的相關分析，以確保 SCT 有加入 Log。

3. ETSI 的報告

Iñigo Barreira 報告 ETSI 將下列文件於 2015 年 6 月發佈 TS，並在 2016 成為 EN

- 319 401 General Policy Requirements for Trust Service Providers

EN 319 411 Policy and security requirements for Trust Service Providers issuing certificates

- 319 411-1: General requirements
- 319 411-2: Requirements for trust service providers issuing EU qualified certificates

EN 319 412 Certificate Profiles

- 319 412-1: Overview and common data structures
- 319 412-2: Certificate profile for certificates issued to natural persons
- 319 412-3: Certificate profile for certificates issued to legal persons
- 319 412-4: Certificate profile for web site certificates issued to organizations
- 319 412-5: QC Statements

- 319 421 Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps
- 319 422 Time-stamping protocol and electronic time-stamp profiles

319 411-1 和 319 411-2 是 eIDAS 的一般必須項目。319 412-4 和 319 412-5 是 CAB Forum 和 CA 需遵守的標準。Iñigo 說施行的時間尚未確定，但 eIDAS 的稽核要件是每 24 個月都需自費通過可信賴稽核員的稽核。ETSI 稽核只接受依據 TS 102 042 的附錄 E 所列之稽核組織。目前包含 KPMG, TUVIT 和 LSTI。

4. 網域驗證 (Domain 驗證)

Robin 說，之前我們為了保有彈性，會留下一個例外條件，讓 CA 有自主性可以提供特別的 Domain 驗證方法，但是這往往會造成誤用和濫用，因此我們希望能正面表列所有的方法，避免灰色地帶，以增加安全性。我們並不是希望阻止我們目前已使用的方法，而是希望能夠更清楚的在 BR 中表達適用的方法。Ryan 也表示之前有 CA 利用這個巧門，定義了一些完全不合標準的方法，因此訂定這些方法有其必要性。但是這會是一個冗長的過程，需要大家同心協力定義這些方法出來。Robin 表示希望大家能夠一起參與工作小組，共同訂定相關標準。

第一到四項方法都不變，第五項是來自原本第六項，展示對該網域的控制性，但是此方法仍然有其安全性問題，包含網域主機的安全性不足，或是代管主機的安全條件限制等，對此方法都有影響。

第六項是展示其對 DNS 記錄變更的能力，以確定他是這個 Domain 的擁有者。

5. 憑證效期

因為 DV 和 OV 憑證都是可以 3 年有效，但 EV 是限制 2 年有效，因此是否要統

一效期為 2 年或 3 年，因為市場有人詢問是否能購買 3 年有效的 EV 憑證。Tim 及 Kirk 均表示，EV 憑證都需要每年驗證持有人身分，因此是 2 年或 3 年並沒有差異，安全性是相同的。但是 Ryan 表示憑證效期更長表示有更多人會去試著透過阻擋廢止清冊的方式，讓已廢止憑證有更長效期，且每年的重新驗證程序往往較為簡略，可能會因 Domain 的擁有者換人，但新 Domain 仍然有效的狀況，而略過廢止程序。以下列出各位代表人對憑證效期的看法

Type	Today	Tim	Wayne	Ryan	Eddy	NN
DV	3	1	3	2	1	2
OV	3	2	3	2	2	3
EV	2	3	3	2	3	3

6. Browser 對不同憑證的 UI 展示
   Rick Andrews 說 Firefox 對將 RC4 的網站顯示安全性不足，而 Ryan 也展示尚未 release 的 chrome 會對沒有 CT 記錄的憑證取消其 Green bar。因此針對這些不同的 UI 展現方式，google 建立一個測試網站：badssl.com，裡面提供各式憑證及使用的演算法，讓用戶能測試看看其瀏覽器會顯示什麼樣的效果。

7. 憑證效期
   Dean 說，微軟決定要求 DV/OV/EV 的 OID 必須描述，但 DV/OV 是 BR 有描述，不過 EV 卻沒有。ETSI 說其 OID 已有定義，且許多 CA 已使用。雖然微軟要求要訂定 OID，但其 Root Program 中使用的 OID 卻不是已議定好的，因此會上有討論如何訂定此 OID，而微軟表示會遵照使用會中所訂定的 OID 進行規範。

8. 討論第 36 次伊斯坦堡會議及之後的會議
   因為本次住房費用較高，因此會員建議可以提供額外的附近飯店選擇，讓會員決定要入住的飯店，且費用不要高於 USD$225。Dean 建議 E-Turgra 能提供數個不同預算的飯店選擇。
   未來 2 年辦理論壇之地主為：2016 年 2 月由 Go Daddy 於鳳凰城主辦； 2016 年 6 月由 Izenpe 於 Bibao 主辦；2016 年 9 月由微軟於西雅圖)主辦。台灣中華電信可於 2017 年 2 月或 2017 年 10 月主辦會議。

參、研討成果彙整

本次「憑證機構與瀏覽器論壇」會議雖僅參天，但每天議程緊湊，各方發言討論熱烈，為能提供相關資訊供我國內相關 PKI 憑證主管機關參考，爰將會中研討重要事項及學習成果，盧列如後：

一 「憑證機構與瀏覽器論壇」簡介 -目的、 狀態和反托拉斯法

一) 論壇目的：憑證機構與瀏覽器論壇係自願集合領先的憑證授權、互聯網瀏覽器軟體和其他應用程式的供應商。憑證機構與瀏覽器論壇成員密切合作，為網上交易提供增強安全性和創建更直觀方法，並為互聯網使用者定義安全網站的指導方針和最佳執行做法。

1 論壇活動現狀：

論壇不具公司或協會身分，只是一群憑證授權和瀏覽器業者互相協調或不定時舉行會議，討論共同關心論壇宗旨有關的議題。論壇對成員或其他人沒有監管或產業的權力。除了論壇創立的智慧財產權權利政策具有權利和責任，論壇"全體會員"或其他參與者不僅傳達法律地位和權利，也完全規範參與論壇活動的指南。

2 智慧財產權政策，反壟斷法律和法規，目標與為：

在論壇活動中論壇成員、 准成員和有關各方必須遵守當時的智慧財產權政策和所有適用的反壟斷法律和規範。

論壇活動 (包括對所有事項的提議進展、指導方針和表決) 歷史性目標，在進行或採用最終工作產品之前，論壇成員間須先尋求實質性共識，這一目標未來仍將維持下去。參加成員在論壇中既不得推廣自己的產品和服務，也不可限制或阻礙其他成員的產品和服務。

主席在所有論壇會議開始前都會宣讀反托拉斯法規 (或在其他場合，主席認為有必要時) ，宣讀內容如下:

「如你所知，這次會議包括相互競爭的公司。這次會議宗旨是討論技術標準，是有關現有和新類型的數位憑證，可以在開發和行銷上提供無競爭限制的技術標準。這次會議不打算在競爭對手間分享競爭敏感性的資訊-CA/瀏覽器論壇 v.1.22 地方法章程 (2014 年 10 月 16 日生效)，因此所有參與者都同意不討論或交換與下列相關的資訊：

(a) 定價政策、定價公式、 價格或其他銷售條件。
(b) 成本、成本結構、利潤空間。
(c) 未決定或計畫性的服務提供。
(d) 客戶、 業務或行銷計畫。
(e) 分配客戶、 領土，或任何形式的產品。」

二) 論壇全體會員和投票

1 資格：CA/瀏覽器論壇會員應當符合下列條件之一。

(1) 頒發 CA： 成員組織經營之憑證機構，需具備合格的稽核員出具 CAs 稽核、ETSI 102042 或 ETSI 101456 稽核報告為網路認證機構，並可以主動頒發證書給公開網路上提供任何主流瀏覽器存取資訊的網頁伺服器。

(2) 根 CA：成員組織經營之憑證機構，需具備合格的稽核員出具 CAs 稽核、ETSI 102042 或 ETSI 101456 稽核報告為網路認證機構，並可以主動頒發證書給下屬 CA，並陸續主動頒發證書給公開網路上提供任何主流瀏覽器存取資訊的網頁伺服器。

(3) 瀏覽器: 成員組織生產的軟體產品，提供大眾安全地使用瀏覽網頁。

2 任期: 論壇將選舉主席和副主席，每位任期兩年。當主席缺席或不能擔任時副主席可行使主席權力，任何委派給主席的職責都由副主席來執行。例如，主席缺席時，論壇會議和論壇電話會議將由副主席主持。

二 主要瀏覽器支持憑證效期展延 (或 EV)的萬用網域憑證 Wildcard EV certificates supported by major browsers)

憑證效期展延或 EV 憑證，是由控制 SSL 憑證和網域名稱的合法身份憑證授權公司設計，提供更高層次的查證。反之，最共同類型的憑證、網域驗證，只要求 CA 驗證網域名稱。瀏覽器在使用者介面上顯示特定 EV 線索以醒目顯示這個額外驗證：最值得注意的是，公司名稱顯示在網址列中，通常配有一個綠色的掛鎖或綠色的欄。

Login.live.com 在谷歌 chrome 瀏覽器憑證效期展延
EV 憑證服從附加要求遠高於基本要求以上。例如基本要求中，EV 指南是由 CA/瀏覽器論壇，瀏覽器廠商和 CAs 產業集團所制定，EV 指南中禁止 EV 憑證使用萬用網域憑證(即 www.example.com，mail.example.com 和 paypal.example.com 將都匹配為 *.example.com)，明確提起兩次這項限制"萬用網域憑證對 EV 憑證來說是不允許的 "。

然而，Verizon 公司已決定藉由發行憑證給 Accenture 來測試瀏覽器對萬用網域 EV 憑證*. cclearning.accenture.com 處理方式。Verizon 公司不是 CA/瀏覽器論壇的成員，但卻以特立獨行發行憑證給違反基本要求憑證 (包括 EV 憑證)而聞名。土耳其、瑞士是那些在 CA 瀏覽器會議中反對 EV 萬用網域憑證的國家之一。中國是贊成 EV 萬用網域憑證而不是 DV 萬用網域憑證。

儘管 EV 指南禁止發行萬用網域 EV 憑證，目前大多數主流瀏覽器並無強制實施此限制。當使用者瀏覽 EV 憑證的網站，Google Chrome、 Firefox、 IE，Opera 和 Safari (桌上型) 皆保留 EV 瀏覽器的提示。

唯一的例外是 Safari 桌上型 會與其他桌上型瀏覽器一樣正常顯示 EV 提醒； 然而，Safari 在 iOS 7 上就不顯示 EV UI。

三 重視憑證透明度 (Certificate Transparency，CT)

憑證透明度(CT) 是用來監控和稽核數位憑證的一種實驗 IETF 開放標準和開放原始碼框架。透過系統的憑證日誌、 監視器和稽核員，憑證透明度將允許網站使用者和網域擁有者辨識錯誤或惡意發行憑證，以及辨識詐欺的憑證機構 (CAs) 。

一) 背景

詐欺性憑證張揚地揭露現行數位憑證管理制度之缺陷，很明顯證明其安全和隱私之漏洞存在。2011 年荷蘭的 CA(Certificate Authority) DigiNotar 遭侵入者利用其基礎設施，成功打造 500 多個詐欺性數位憑證後，DigiNotar 申請破產。 [2] 班·勞裡和亞當·蘭利構思打造一個運用開放資源性計畫以發展作為憑證透明度和實行架構。

二) 優勢

數位憑證管理的問題之一是詐欺性憑證需要很長的時間來被瀏覽器廠商發現、舉報和撤銷。憑證透明度(Certificate Transparency, CT 以下簡稱 CT)將助益一種狀況不被發生:也就是說經由某網域將發行的憑證不可能不被網域擁

有者知悉。CT 不需要其它通信管道來驗證憑證，像是做某些匹配性技術，如線上憑證狀態協議（Online Certificate Status Protocol，OCSP）及聚合。憑證透明度也無須運用第三方的信認。

三) 憑證透明度日誌(Certificate Transparency Logs, CTLs)

CT 取決於可驗證的憑證透明度日誌。日誌追加新的憑證，以一種不斷增長型梅克爾雜湊樹[3]來展現 。要被視為正常表現，日誌必須：

1 驗證每個提交的憑證或 Pre-憑證以一個有效的簽名鏈，其領回到受信任的根 CA 之憑證。

2 拒絕發布這無效的簽名鏈憑證。

3 從最近已接受憑證回到根憑證並存儲在整個驗證鏈。

4 呈現出這驗證鏈的審核要求。

5 憑證透明度日誌可能會接受那些憑證，如尚未完全有效和已過期的憑證。

CT 監控程序

監控程序也同時扮演客戶端的日誌伺服器。監控程序檢查日誌，以確保它們正確地執行。”不一致性”是用來驗證日誌，其代表為一個不正確的日誌(譯註:意味著有人使用假憑證)，並在日誌中的資料結構（梅克爾樹）的簽名，防止日誌否認不當行為。

CT 審核程序

審核程序還扮演客戶端的日誌伺服器。CT 審核程序使用的部分有關信息的日誌，以驗證對他們有其他的部分信息的日誌。[4]

CA 實施

2013 年 9 月，DigiCert 成為第一個 CA 實施 CT。谷歌(google)目前正在執行一項前導型憑證透明度日誌(Pilot Certificate Transparency Log, PCTL)。谷歌已經宣布將於 2015 年 1 月部署至少產製 3 個 CTLs。緊接產製這些日誌部署後，谷歌 Chrome 瀏覽器將開始致力執行憑證透明度擴展驗證憑證（Extended Validation Certificates, EVs）。

在過去的幾年裡，由於 CAs(Certificate Authorities)的失誤，與有時也經由已被入侵並用於基礎設施之伺服器，經產生了許多假的 SSL 萬用憑證。這些假冒的 SSL 憑證可用於偽裝成合法的安全網站，出現待驗證及可靠存疑，愚弄人的網頁瀏覽器，因此用戶沒辦法分辨他們正在一個不安全的網站。

對於假憑證不應該掉以輕心; 甚至連谷歌也已經受到他們影響，以及其他大型企業和一些政府。於是在憑證吊銷效應下產生了許多憤怒的用戶和一些無法使用的網站。

SSL 憑證在本質上是 HTTPS 協議的基礎。如果沒有 SSL，就沒有亞馬遜(Amazon)或易趣(eBay)。這些憑證是由受信任的 CA 簽署，通過一定數量驗證後，才會應發出的每個憑證，以確保憑證需求是由網域真正擁有者提出的。

在嘗試預防類似憑證造假在未來發生，谷歌已經創造了一個獨特而強大的工具，以盡量減少從單一不良憑證的潛在損害。該技術被稱為憑證透明度（CT）以及意味著的是授權憑證提供者發布的憑證將會是透明的。

四 歐洲電信標準協會（European Telecommunications Standards Institute ,ETSI）簡介

歐洲電信標準協會（European Telecommunications Standards Institute ,ETSI）是一個獨立的，不以營利為目的，在電信行業標準化組織（設備製造商和網絡運營商），其標準運用片佈歐洲以及全球。 ETSI 產生的資訊和通信技術（Information and Communication Technologies, ICT）全球適用的標準，包括固定，移動，無線電，融合，廣播和網路技術。

ETSI 是由 CEPT 創建於 1988 年，並正式通過了歐盟委員會和歐洲自由貿易聯盟秘書處的認可。總部設在索菲亞 - 安提波利斯（法國），ETSI 正式負責資訊和在歐洲範圍內通信技術（Information and Communication Technologies, ICT）的標準化。
ETSI 每年發行 2,000 至 2,500 標準。自 1988 年成立以來，產出超過了 30,000。這些標準涵蓋全球並起動相關關鍵技術的發展，如 GSM™系統的手機，3G，4G，DECT™，TETRA 專業行動無線電系統，以及短距離設備的要求，包括 LPD 無線電，智慧卡和多標準的成功案例。

顯著卓越的 ETSI 技術委員會和工業規範團體（ISGs）包括 SmartM2M（機器對機器通信），智慧交通系統，網路功能虛擬化，網路安全，電子簽章和基礎設施等 ETSI 激發了創作，並為合作夥伴，在 3GPP 和 oneM2M 上。所有技術委員會，工作和工業規範團體是經由 ETSI 門戶訪問取得。

ETSI 技術集群[1]提供簡單，容易掌握 ETSI 概述的活動用於 ICT 的標準化上。每一個技術集群代表了全球 ICT 架構的重要組成部分，涵蓋了許多具有共同的技術範圍和視野的 ETSI 技術委員會和工作組的工作。一個單一的技術委員會的工作可能在幾個集群呈現。集群有助於方便識別之基礎上業務相關性和應用領域，而不是純粹的具體技術工作領域感興趣的區域。

在 2013 年，ETSI 的預算超過 2 千 3 佰萬歐元，其捐款來自成員，商業活動如銷售文件，插件測試和論壇舉辦[2]，契約工作和合作夥伴提供資金。
ETSI 是全球標準合作舉措的創始合夥組織。第 9 屆 ETSI 安全研討會這個一年一度的 ETSI 安全研討會已造成一個資訊安全盛會的美譽。它匯集了來自那些制定國際標準和安全專家最新討論及最近的事態發展，分享知識，識別。

五 建議修訂網域驗證 (Domain Validation)之要求

建議網域驗證修訂的 CA/瀏覽器論壇基本要求第 11.1.1 節，釐清(說明)可接受的驗證網域控制的方法：

一) 增加以下的定義：

基本網域：申請成為 FQDN 的一部分，這是一個註冊表控制或公用後置網域名加註冊表控制或公用的後置網域名（如“example.co.uk”或左邊的第一個網域名節點“example.com”）。

授權網域名：網域名（i）對於非通用型的 FQDN，建立由通過修剪零個或多個元件的 FQDN 內含憑證之需求，（ii）用於通用型的 FQDN，建立由通過修剪至少有一個或多個元件的 FQDN，及（iii）包含至少第二級 DomainBase 網域的通

用高層級網域名（gTLD），如.com，.net 或.org，或者，如果 FQDN 包含 2 字母國家代碼高層級網域名（ccTLD），那麼至少包含根據該 ccTLD 的規則允許註冊任何網域名的資訊。

隨機亂數：CA 指定給申請者的一個數值，能至少展示出 112 位元的熵值。
請求符記(Token)：CA 從公開金鑰中指定的一組方法所推導出的數值，作為發證使用。請求符記的唯一性與推導過程的不可逆轉性至少要與憑證簽章所用的加密簽章演算法一樣強健。
測試憑證：指憑證包含了特定資料，對於應用軟體廠商或公開信任 TLS 伺服器而言，將憑證解讀為廢棄不再使用，例如憑證含有的重要延期資訊，不再被任何應用軟體廠商所識別，或是根憑證所發的憑證不符合這些需求。
網域名稱註冊者授權

二) 完整網域名稱(FQDN)

憑證機構與瀏覽器論壇段落 11.1.1 基礎需求更改如下：
憑證中列出的每一個完整網域名稱，CA 應該確認憑證核發日期，申請者(或申請者的母公司，子公司或分支機構，基於此節目的皆參照為”申請者”)為網域名稱註冊者或藉由下列方式對 FQDN 有控制權:

1. 確認申請者作為網域名稱註冊者能夠與網域名稱註冊商透過可靠的通訊方式，例如使用 WHOIS 提供的資訊；或
2. 確認申請者直接與網域名稱註冊者透過可靠通訊方式獲得憑證核發授權，方式為(i)從網域名稱註冊商獲得或(ii)在註冊網域 WHOIS 記錄中列為註冊者、技術、管理聯絡人或
3. 確認憑證核發授權透過事先決定的電子郵件位址‘admin’，‘administrator’，‘webmaster’，‘hostmaster’，或‘postmaster’，跟隨著 at 符號(“@”)，接著是授權網域名稱；或
4. 仰賴於網域授權文件(i)證明通訊來自於網域名稱註冊者（包含任何私人，匿名或代理註冊服務）或網域名稱註冊商列在 WHOIS 且(ii)經過 CA 檢驗過，屬於(a)日期為憑證請求日或晚於該日期，亦或者是(b)為 CA 所使用來驗證之前核發的憑證且註冊的網域名稱 WHOIS 記錄自從之前的憑證核發後便未再修改；或
5. 申請者能證明其對 FQDN 具有控制權，藉由在符合 RFC5787 的授權網域名稱加入一個檔案其名稱或內容包含了一個隨機亂數或一個請求符記(Token)至“/.well-known/certificate”目錄。
6. 申請者能證明其對 FQDN 具有控制權，藉由在申請者對授權網域 DNS 記錄資訊作出變更，而其變更是插入隨機變數或請求符記；或
7. 申請者能證明其對 FQDN 具有控制權，藉由 CA 確認申請者能控制授權網域來自於 DNS 對 CNAME 記錄的搜尋，其請求的 FQDN 符合本節 11.1.1；或
8. 申請者能證明其對 FQDN 具有控制權，藉由 CA 確認申請者能控制 IP 位址來自 DNS 對於 A 或 AAAA 記錄的搜尋，其請求的 FQDN 符合本節 11.1.2；或
9. 申請者能證明其對 FQDN 具有實際控制權，藉由申請者請求然後安裝一個 CA 對 FQDN 核發的測試憑證，該 FQDN 被存取且經由 https 被 CA 批准。

三) 確認程序是由 email 進行追蹤且利用自動程序記錄成功的回覆，例如 email 中的超連結的條文，CA 必須查核對申請者而言，之前是不可預知且未知的值已填寫在回覆中。在此節 CA 在完成批核前，不應依賴期間超過 14 天的隨機變數，請求符記或測試憑證。

注意：FQDNs 可能列在訂閱者憑證，使用 X.509 的 subjectAltName 擴充規格的 dNSNames 或者是下屬 CA，在 X.509 名稱限制條件擴充規格的 permittedSubtrees 選項中的 dNSNames。

六 SSL 憑證有效期間 (Cert Validity Period)

SSL 憑證最大有效期間 39 個月 SSL 有效期間：在之前的會議報告中，谷歌與微軟鼓勵各個 CAs 不再使用有弱點與過時的 SHA-1 雜湊演算法並且改用更強大的 SHA-2 演算法。

從 2016 年 1 月 1 日開始，CAs 不可以再發任何使用 SHA-1 雜湊演算法的 SSL 新憑證。但直至 2017 年 1 月 1 日為止，各 CAs 仍可以繼續使用 SHA-1 來簽章憑證以確認線上憑證狀態協定(OCSP)的回應訊息。

根據 CA/Browser 論壇準則，從 2015 年 3 月 1 日開始，SSL 憑證將會限制最大效期為 39 個月。此限制會影響所有的 SSL 憑證廠牌(Symantec, Comodo, Thawte 與 GeoTrust)，包含了全部 4 或 5 年的網域批准(DV)，組織批准(OV)及其他憑證。然而，擴充批准(EV)憑證將不會被此更新所影響，因它們已被限制為 2 年的有效期間。

七 SSL 憑證的種類與功能

一) 種類

在過去幾年使用 SSL 憑證的組織數量已大大的增加。使用 SSL 的應用程式也有所增加。例如：某些組織僅因為機密性而需要使用 SSL，例如加密。某些組織希望使用 SSL 來強化它們的安全與身分識別，例如：它們想要跟顧客展示它們是經過查核的且為合法的組織。

擴充批准(EV)SSL 憑證：CA 確認申請者的正當性，並附加上一個特定的網域名稱來對組織作通盤的查核。EV SSL 憑證的核發程序非常嚴格的定義在 EV 準則中，其在 2007 年由 CA/Browser 論壇正式批准通過，在其中規定了 CA 核發憑證前所需的所有步驟，包含了：

查核該組織實體在法律面、實體面、營運面的存在事實證明。

查核該組織實體的身分識別吻合官方紀錄。

查核該組織實體有專屬的權力來使用定義在 EV SSL 憑證中的網域。

查核該組織實體對於 EV SSL 憑證的核發有適當授權。

各種工商行號皆可取得 EV SSL 憑證，包含了政府機關，及法人與非法人公司行號。準則的第二部分，EV 稽核準則，在其中規定了 CA 在核發 EV SSL 憑證前需成功的完成稽核作業。

組織批准(OV) SSL 憑證：CA 確認申請者的正當性，並附加上一個特定的網域名

稱來對組織作部分的查核。當顧客點擊安全網站標章時，額外的公司查核資訊會顯示給使用者看，如此一來，提供了強化的安全可見性，可知道是誰在負責此網站及提高相關的信任度。

網域批准(DV) SSL 憑證：CA 確認申請者使用一個特定的網域名稱的正當性。沒有公司的身分識別資訊會被作查核，且安全網站標章只會顯示加密資訊。
GlobalSign – 簡化範圍的彈性 SSL 憑證
GlobalSign 是第一家提供簡化範圍的彈性 SSL 憑證供應商－完美地符合了三個新定義的 SSL 類別：網域批准(DV)，組織批准(OV)及擴充批准(EV)。藉由 GlobalSign 其 15 年的產業經驗，提供了值得信賴的 SSL 解決方案，GlobalSign 對於近幾年出現的 SSL 三種型態提出了一個簡單的方法論。

其他 SSL 供應商較傾向使用複雜產品命名和分類方式，如此便可與使用基本功能的產品來區分。 GlobalSign 則為另一趨勢，它是採用簡單的產品命名和指定功能來提供每項產品作為選擇。這種方法意旨在幫助消除耗時和令人沮喪“何種憑證，是我需要” 的問題，而此類問題是客戶於評估 SSL 供應商解決方案時常提出的。

GlobalSign SSL 簡易分類，包括：**增強驗證企業驗證。**
增強驗證： GlobalSign 增強型 SSL 數位憑證
最新的也可能是最顯著進步就在於 SSL 技術，因為它從最初成立以來，就是遵循標準化的增強驗證準則。目前新的高安全性瀏覽器，如微軟的 Internet Explorer 7+，Opera 9.5+，火狐 3 +，谷歌 Chrome，Apple Safari 3.2+ 和 iPhone 的 Safari 3.0+皆具有 EV 憑證之增強型 SSL 數位憑證，可激活網站瀏覽器的地址欄使其變成綠色，鮮明的標示這個網站正受到最嚴密的訊息安全防護。對於追求真實性及高水準的客戶而言，增強型 SSL 數位憑證是理想的解決方案。
企業驗證： GlobalSign 企業型 SSL 數位憑證
GlobalSign 已簽發企業型驗證憑證達 15 年。對於申請企業型數位憑證的公司於簽發前皆會詳查其公司的內部事務。

二)功能
一家憑證頒發機構，頒發憑證予 E 公司時，應該確認憑證上的公鑰及名稱是否屬於 E 公司的.對於 SSL 數位憑證伺服器憑證：。
E 公司的名稱是一個主機名，就像是 www.google.com，也可能是一張”萬用卡”（*.google.com）。這是 SSL 客戶端驗證;這是有關於名稱，而不是 IP 地址。
CA 接到公鑰時才承認憑證的要求。因此“身份”的概念在這裡真的是網域名所有權的問題。CA 希望確保它所收到是真正控制網域的人之要求。有數種方式;兩個最常用方式如下：
CA 以電子郵件發送一個需求至 WHOIS 資料庫內所指定的電子郵件地址。
CA 的需求包括一些網域資料，例如 DNS 隨機主機名。
這些檢查不是非常強大（它們所依賴的是“不可能”侵入，各別的電子郵件或者 DNS，也既沒有很好的保護），所以目前較時尚且有效力的驗證，稱為增強性驗證憑證。對於 EV 憑證，CA 是應該做更多的文書工作，以確保它商談的權利主體。

追溯性，非 EV 憑證被稱為“DV”（以下簡稱“網域驗證”）。
EV 憑證網路效力將使 Web 瀏覽器更能夠識別，並能為人類用戶提供更奢華且更加環保的事實。雖然，非 EV 憑證在法律上也能工作。 EV 憑證是值得努力的，當你的用戶已被訓練能夠區別 EV 憑證其適用度較優於一般“普通”的憑證（譬如仍有著名的“鎖”標識）。，我會說，現在大多數網民還尚遠遠地沒有意識到此二者的區別，所以購買 EV 憑證是一種無用的。
(EV 憑證將會變成有用的，當他們要求成為強制性時，即當 Web 瀏覽器開始拒絕或發出警告，對於沒有被標註為“EV”認證的 SSL 伺服器。這是一個相當艱難的過渡，我並未看到它在不久的將來會發生。)
當一個壞人使用你的伺服器名稱（前提安裝一個真正成功的模仿攻擊）獲得一個看似有效的憑證，他必須執行下列操作之一
誤導 CA.誤導 CA 相較於 EV 憑證（這一點）更難。但是，即使你得到一個 EV 憑證,它不會阻止攻擊者以你的名字從輕率的 CA 獲得非 EV 憑證,EV 憑證將可保護你對抗草率的 CA，只要你的客戶進行教育訓練，，當他們看到一個看似正確但非 EV 憑證記載您的網站名稱, 便能暫停和開始懷疑。此點目前似乎很難就可實現的。
竊取你的私鑰。如果攻擊者竊取你的私鑰，那麼他就可以使用它與您的憑證（這是公開的），安裝於假冒的服務器。 EV 或非 EV 是這裡無關緊要;重要的是，你應該保護你的私鑰好。如果您的服務器被侵入，通知 CA，以便它可以撤銷你的憑證，並發給您另一個新的密鑰。
人類用戶仍被誤導進入瀏覽器，無視危險及可怕的警告,僅管無效的憑證已顯示。你真的無法抵禦的，除了通過教育訓練用戶。Web 瀏覽器顯示的警告隨著時間的推移趨向增加警示（和危險）。
誤導人類用戶去連接到攻擊者所擁有的一個完全有效憑證的網域，它看起來就像是預期中的服務器名稱的名稱。例如 www.gogle.com 或 www.google.business.com，而不是 www.google.com（虛構的例子）。再一次說明，只有對用戶教育訓練方能真正對抗
大多數釣魚攻擊是基於最後兩個方法之一，因此這意味著你不應該過分擔心於，在 DV/ EV 二分法。對於安全性很重要的一點是用戶教育訓練。

八 中華電信公司為我國於 CA/Browser Forum 之重要會員，將於 2017 年舉辦 CA/Browser Forum

中華電信公司為 CA/Browser Forum 會員，負責我公開金鑰基礎建設(ePKI)與各大作業系統及瀏覽器根憑證計畫(Root Certificate Program)之聯繫窗口，負責相關系統之研發工作，掌握 SHA-1 憑證淘汰決策，而於去年底完成 PublicCA 可簽發 SHA 256 SSL 憑證機制。本次參與 CA/Browser Forum 會議將有助於中華電信掌握憑證與瀏覽器最新技術應用趨勢，有利於協助維運我各政府憑證；掌握國際 SSL 憑證及程式碼簽章憑證最新規範、憑證機構同業、瀏覽器大廠與稽核業者之動態，促進電子交易之發展。此外，中華電信憑證總管理中心於年底新簽發的第 2 代 RSA 4096 bits w/SHA 256 自簽憑證，進行維運行政院國家發展委員會政府憑證總管理中心採第 2 代 RSA 金鑰長度 4096 bit，及以 SHA 256 自簽憑證申請植入各大作業、瀏覽器與軟體平台之 CA 信賴清單。
本次 CA/Browser Forum 經討論決議，未來 2 年辦理論壇之地主為：2016 年 2 月由 Go Daddy 於鳳凰城主辦； 2016 年 6 月由 Izenpe 於 Bibao 主辦；2016 年 9 月由微

軟於西雅圖)主辦。台灣中華電信可於 2017 年 2 月或 2017 年 10 月主辦會議。惟據聞該公司每次參加本會議，僅派乙人出席，且歷次都屬不同人員，此對於掌握會議議題，國際會議經驗傳承，海外專業人派連結，及相關國際合作皆未能有積極作為及成果，殊為可惜。有鑑於其他會員公司，若非指派二人參加，則指定同一人代表參加，或可供中華電信公司作為今後派員參加此論壇之借鏡，俾利 2017 年主辦，台灣之第一次 CA/Browser Forum。

九 Mozilla 提出電子郵件認證的新規範

Mozilla 於會中對電子郵件認證於會中提出新的規範(如附件一)，主要是因為他們有提供 thunderbird 電子郵件的服務。 因此，對植入他們信賴清單中的 ROOT CA 憑證之下屬 CA 關於電子郵件的認證會特別要求。

就我國核發的自然人憑證而言，內政部憑證管理中心本來就應該針對寫入憑證內的所有資訊確認其真偽，既然 MOICA 有要寫入電子郵件並讓用戶使用在安全電子郵件功能上，就應該要對電子郵件進行認證，以確保憑證管理中心是有公信力的，而不是隨便進行審查的。

十 歐美國家重視電子簽章之驗證，並持續強化驗證技術及推廣應用

電子簽章本質上是相當於一個手寫簽字，以電子形式的訊息連接到其它電子設備對接資訊（發票，支付票據，契約等等），以此為驗證的方法。

電子簽章不僅是手寫簽名的“圖片”。它是一個使用加密轉換資訊，以允許資訊接收者收取訊息，並驗證所接收的資訊的來源和完整性。除了這個數位簽名的電子簽章也經由數位憑證，智慧卡或生物特徵方法使用戶認證。越來越多的電子簽章被賦予同等於手寫方式的合法性。

歐盟委員會 e 標記指令（1999/93 / EC），在這個方向邁出的一步，以及 2000 年 6 月，美國政府的 e-標誌法案。

2008 年 11 月 28 日，歐盟委員會採用了一項“行動計劃，e 簽名和 e 標識，以方便在單一市場提供跨境公共服務”（COM（2008）798）。

2009 年 12 月 22 日，歐盟委員會發布了關於電子簽章（M/460），用於定義一個合理的標準化架構。

肆、心得及建議

基於本次出席 104 年 6 月「憑證機構與瀏覽器論壇」(CA/Browser Forum)工作小組會議之經驗與體識，有關內政部憑證管理中心業務之推展及相關事項包括：

Mozilla 於會中對電子郵件認證於會中提出新的規範，就我國核發的自然人憑證而言，內政部憑證管理中心應該針對寫入憑證內的所有資訊確認其真偽，既然 MOICA 有要寫入電子郵件並讓用戶使用在安全電子郵件功能上，就應該要對電子郵件進行認證，以確保憑證管理中心的公信力，並為各國瀏覽器認可，可以互通。

另鑑於中國互聯網絡信息中心（CNNIC）濫發數位憑證，Google Chrome 及 Mozilla Firefox 瀏覽器更新不再承認來自 CNNIC 的根憑證與延伸驗證（Extended Validation, EV）憑證，我國各憑證管理中心(CA)發行之憑證務必遵循國際憑證政

策(CP)及憑證實務作業基準(CPS)之規範，否則將影響其簽發之憑證於國際主要瀏覽器間之應用。

其他各相關事項，謹綜合建議如下：

一、檢討自然人憑證要求民眾將電子郵件地址寫入憑證內有否需要，若必要時則須進行認證方屬安全

為便利憑證管理中心與憑證持有人之聯絡，目前民眾申辦自然人憑證時，均須填寫電子郵件地址， 因電子郵件地址長且不易記憶，要求民眾填寫電子郵件地址常引起抱怨，且民眾填寫後又無從及時檢驗其正確性，逕自寫入憑證內能否發揮原有設計功能仍叫民眾存疑。故應檢討自然人憑證要求民眾將電子郵件地址寫入憑證內事有適宜。

若將電子郵件地址寫入憑證內有其必要性，以確保其功能之周延性，則依 Mozilla 於會中提出對電子郵件認證新的規範，憑證管理中心未來就應該針對寫入憑證內的所有資訊確認其真偽。換言之，既然自然人憑證要求民眾寫入電子郵件，並讓用戶使用在安全電子郵件功能上，就應該要對電子郵件進行認證，以確保憑證管理中心的公信力。

二、我國各憑證管理中心(CA)發行之憑證務必遵循國際憑證政策(CP)及憑證實務作業基準(CPS)之規範，否則將影響其簽發之憑證於主要瀏覽器間之應用

Google 於今(104)年 3 月發現埃及的資安業者 MCS 透過中國 CNNIC 所發行的中間憑證（intermediate certificate）假冒了 Google 網域，可能讓使用者誤以為所造訪的是 Google 網站，衍生中間人攻擊的風險。Googl 抨擊中國互聯網絡信息中心（CNNIC）濫發數位憑證之後，Google 採取進一步的行動，在 4 月宣布，下一版的 Chrome 瀏覽器更新不再承認來自 CNNIC 的根憑證與延伸驗證（Extended Validation, EV）憑證。

繼 Google 宣布之後，Mozilla 也表示，經過調查與討論後，他們也決定不再讓 Mozilla 的 Firefox 信賴 CNNIC 自今年 4 月 1 日之後所頒發的任何憑證， 因 Mozilla 認為，MCS 並無開發憑證實務作業基準，未被允許執行金鑰產生程式，在合約之外缺乏其他任何形式的控制，而 MCS 也坦承 CNNIC 並未指導他們如何安全的儲存或管理此一不受限制的中繼憑證。

依中國互聯網絡信息中心（CNNIC）之前例，我國各憑證管理中心(CA)發行之憑證務必遵循國際憑證政策(CP)及憑證實務作業基準(CPS)之規範，否則將影響其簽發之憑證於主要瀏覽器間之應用。

三、安全性 SSL(Secure Sockets Layer) 憑證最大有效期間限制為 39 個月應予正視

在之前的會議報告中，谷歌與微軟鼓勵各個 CAs 不再使用有弱點與過時的 SHA-1 雜湊演算法並且改用更強大的 SHA-2 演算法。

從 2016 年 1 月 1 日開始，CAs 不可以再發任何使用 SHA-1 雜湊演算法的 SSL 新憑證。但直至 2017 年 1 月 1 日為止，各 CAs 仍可以繼續使用 SHA-1 來簽章憑證以確認線上憑證狀態協定(OCSP)的回應訊息。

根據 CA/Browser 論壇準則，從 2015 年 3 月 1 日開始，SSL 憑證將會限制最大效期為 39 個月。此限制會影響所有的 SSL 憑證廠牌(Symantec, Comodo, Thawte 與 GeoTrust)，包含了全部 4 或 5 年的網域憑證 (DV)，組織憑證 (OV)及其他憑證。然而，效期延伸(EV)憑證將不會被此更新所影響，因它們已被限制為 2 年的有

效期間。我國於訂定憑證政策(Certificate Policy)時，應重視此一國際趨勢。

四、歐美各國重視電子簽章驗證，並持續強化製作與驗證之技術及推廣應用

電子簽章本質上是相當於一個手寫簽字，以電子形式的訊息連接到其它電子設備對接資訊（發票，支付票據，契約等等），以此為驗證的方法。

電子簽章不僅是手寫簽名的“圖片”。它是一個使用加密轉換資訊，以允許資訊接收者收取訊息，並驗證所接收的資訊的來源和完整性。除了這個數位簽名的電子簽章也經由數位憑證，智慧卡或生物特徵方法使用戶認證。越來越多的電子簽章被賦予同等於手寫方式的合法性。

歐盟委員會 e 標記指令（1999/93 / EC），在這個方向邁出的一步，以及 2000 年 6 月，美國政府的 e-標誌法案。

2008 年 11 月 28 日，歐盟委員會採用了一項“行動計劃，e 簽名和 e 標識，以方便在單一市場提供跨境公共服務”（COM（2008）798）。

2009 年 12 月 22 日，歐盟委員會發布了關於電子簽章（M/460），用於定義一個合理的標準化架構。

五、中華電信公司宜研討派員參加 CA/Browser Forum 之策略，以利會議經驗傳承，拓展國際合作機會

中華電信公司為 CA/Browser Forum 會員，負責我公開金鑰基礎建設(ePKI)與各大作業系統及瀏覽器根憑證計畫(Root Certificate Program)之聯繫窗口，負責相關系統之研發工作，掌握 SHA-1 憑證淘汰決策，而於去年底完成 PublicCA 可簽發 SHA 256 SSL 憑證機制。其參與 CA/Browser Forum 會議將有助於中華電信掌握憑證與瀏覽器最新技術應用趨勢，有利於協助維運我各政府憑證。

本次 CA/Browser Forum 經討論決議，位來 2 年辦理論壇之地主為：2016 年 2 月由 Go Daddy 於鳳凰城主辦； 2016 年 6 月由 Izenpe 於 Bibao 主辦；2016 年 9 月由微軟於西雅圖)主辦。台灣中華電信可於 2017 年 2 月或 2017 年 10 月主辦會議。惟據聞該公司每次參加本會議，僅派乙人出席，且歷次都屬不同人員，此對於掌握會議議題，國際會議經驗傳承，海外專業人派連結，及相關國際合作皆未能有積極作為及成果，殊為可惜。有鑑於其他會員公司，若非指派二人參加，則指定同一人代表參加，或可供中華電信公司作為今後派員參加此論壇之借鏡，俾利 2017 年主辦，台灣之第一次 CA/Browser Forum。

六、邀請 CA/Browser 重要成員會長及立陶宛代表參加國內舉辦之相關國際研討會或參訪活動

CA/Browser 重要成員，如正副會長(會長 Mr. Dean Coclin，副會長 Mr. Kirk Hall and 前會長 Mr. Ben Wilson)，皆對我國友好且具 CA Brower 及資訊安全之專業知能，其實務經驗豐富且為國際業界所尊重之學者專家。而立陶宛代表 Mr. Moudrick Dadashov 專經 PKI 技術與應用，且為該國際建立 eID 制度之主要工作成員之一。上述專家若宜適當時機邀請渠等至國內演講或參與研討會，如參加 105 年自然人憑證國際研討會，非但對我推展 PKI 於電子化政府業務，及刻正規劃辦理中之晶片身分證上有實質之助益，同時可進一步拓展我國與國際業界之交流合

作。。

伍、附件

附件一「憑證機構與瀏覽器論壇」(CA/Browser Forum)工作小組會議議程

工作小組會議
2015/06/23(星期二)

時間	分區	描述	主持人
9:00-9:30		報到及早餐	
9:30-9:35		歡迎致辭	Dean&Connie
9:35-9:40		反壟斷聲明及會議記錄安排	Dean
9:40-10:30	1	憑證政策工作小組報告	Ben
10:30-10:45		休息	
10:45-12:00	1	憑證政策工作小組報告	Ben
12:00-13:00		午餐	
13:00-14:00	2	憑證驗證工作小組報告	Jeremy
14:00-14:10		休息	
14:10-14:40	2	憑證驗證工作小組報告	Jeremy
14:40-15:20	3	程式簽署工作小組報告	Dean/Jeremy
15:20-15:30		下午茶	
15:30-17:10	4	資訊分享工作小組報告	Ben
17:10		散會	
		晚餐自行處理	

CAB Forum 大會第一日
2015/06/24

時間	分區	描述	主持人
8:30-9:15		報到及早餐	
9:00-9:10		前次會議及事項重點報告	Dean&Connie
9:10-9:15		反壟斷聲明及會議記錄安排	Dean
9:15-10:45	1	萬用憑證及憑證效期討論	Jemery
10:45-11:00		休息	
11:00-11:45	1	短效期憑證討論	Jemery
11:45-12:05		工作小組報告	
12:05-13:00		午餐	
13:00-13:30	2	工作小組報告	
13:30-14:30		歐盟合格 SSL 憑證報告	Slavik Gorniak, ENISA, eIDAS (Invited)
14:30-14:45		休息	
14:45-15:30		WebTrust 更新討論	
15:30-16:30		Browser 新聞(Apple, Google, Microsoft, Mozilla, 360, Opera)	

16:30-17:00		Browser 新聞	
17:00		散會	
		SwissSign 安排晚餐	

CAB Forum 大會第二日
2015/06/25

時間	分區	描述	主持人
8:30-9:00		報到及早餐	
9:00-10:00		待定	
10:00-10:30		憑證透通性更新討論	Dean
10:30-10:45		休息	
10:45-11:30		ETSI 簡報	Iñigo Barreira and Arno Fiedler
11:30-12:10		條例更新	Dean
12:10-13:00		午餐	
13:00-14:00	17	網域名稱驗證	Jemery
14:00-14:30	18	EV 萬用憑證及效期討論	Jemery
14:30-15:00	19	待定	
15:00-15:20		下午茶	
15:20-16:30		DV/OV/EV 憑證用法及對應 OID	Dean, Jemery
16:30-16:40		下次會議討論	
16:40-17:00		檢視完成事項及工作事項	
17:00		散會	
		晚餐自行處理	

Working Group Meetings
Tuesday, 23 June 2015

Time	Start	Stop	Slot	Description	Discussion
0:15	9:00	9:15		**Check-in**, badging, get situated in room @ Hotel	
0:15	9:00	9:30		**Breakfast** - Continental	
0:05	9:30	9:35		**Welcome**, Prelim Matters, Logistics, etc.	Dean, Connie
0:05	9:35	9:40		**Antitrust Statement, Assign Minute-Taking**	Dean
0:50	9:40	10:30	1	**Policy revision** Working Group	Ben
0:15	10:30	10:45		**Break**	

1:30	10:30	12:00	1	**Policy revision** Working Group (cont.)	Ben
1:00	12:00	13:00		**Lunch Service** - Working Lunch	
1:00	13:00	14:00	2	**Validation** Working Group	Jeremy
0:10	14:00	14:10		**Break**	
0:20	14:10	14:40	2	**Validation** Working Group	Jeremy
0:40	14:40	15:20	3	**Code Signing** Working Group	Dean/Jeremy
0:10	15:20	15:30		**Coffee/Beverage Service Break**	
1:40	15:30	17:10	4	**Information Sharing** Working Group	Ben
0:00	17:10			**Adjourn** for the Day	
2:30	19:00	21:30		**Casual Dinner** - @ - **On your own or informal group**	

Day 1 Wednesday, 24 June 2015

Time	Start	Stop	Slot	Description	Discussion Leader / Notes
0:30	8:30	9:00		**Check-in**, badging, get situated in room @ Hotel	
				Instructions	
0:45	8:30	9:15			**Breakfast** -
0:05	9:00	9:05		**Recap of Prelim Matters** and Logistics	Dean, Connie
0:15	9:05	9:15		**Antitrust Statement & Assign Note Takers**	Dean Coclin
1:30	9:15	10:45	5	**Wildcard and Cert duration**	Jeremy
0:15	10:45	11:00			**Break**
0:15	11:00	11:45	6	**Short Lived certificates**	Jeremy
0:20	11:45	12:05	7	**Working Group reports**	
0:55	12:05	13:00			**Lunch**
0:30	13:00	13:30	8	**Working Group reports cont.**	
1:00	13:30	14:30	9	**Presentation on EU Qualified SSL Certificates**	Slavik Gorniak, ENISA, eIDAS

0:15	14:30	14:45			Break
0:45	14:45	15:30	10	**WebTrust** Update	Review current status of Web
1:00	15:30	16:30	11	**Browser News**	Apple, Google,
0:30	16:30	17:00	12	**Browser News (cont)**	
	17:00				**Adjourn** for the day
3:00	18:00	21:00			**Dinner** hosted by

Day 3 Thursday, 25 June 2015

Time	Start	Stop	Slot	Description	Discussion Leader / Notes
0:45	8:15	9:00		**Check-in** badging, get situated in room @ Hotel,	
0:45	8:15	9:00			**Breakfast** - Continental
1:00	9:00	10:00	13	***Open Slot***	
0:10	10:00	10:30	14	**Certificate Transparency Update:** Current log status, Future plans, etc	
0:10	10:30	10:45			**Break**
0:45	10:45	11:30	15	**ETSI** Presentation	Iñigo Barreira and Arno Fiedler will review status of ETSI's trust service provider
0:40	11:30	12:10	16	**Bylaw Updates**	Kirk/Dean
0:30	12:10	13:00		**Lunch**	
1:00	13:00	14:00	17	**Domain Validation**	Jeremy
0:30	14:00	14:30	18	**EV Wildcards and Validity Periods**	Jeremy
0:40	14:20	15:00	19	***Open Slot***	
0:20	15:00	15:20			**Coffee/Beverage Break**
1:10	15:20	16:30	20	**DV/OV/EV Certificates, Appropriate use and OIDs**	Dean, Jeremy

0:10	16:30	16:40	21	Discuss **F2F Meeting 36** in Istanbul Oct 5 and Future **F2F Meeting volunteers**	
0:20	16:40	17:00	22	**Review** accomplishments / list of tasks	
	17:00				**Adjourn**
2:30	18:00	20:30			**Dinner** - on your own

四) Mozilla 建議電子郵件認證的規範

電子郵件認證 Mozilla 的規範
Mozilla 的要求在他們的 CA: Recommended Practices 1.7 節中有提到，如下說明
https://wiki.mozilla.org/CA:Recommended_Practices

Verifying Email Address Control
We rely on public documentation and audits of those documented processes to ascertain that the requirements of section 7 of the Mozilla CA Certificate Policy are met.
Section 7 of the Mozilla CA Certificate Inclusion Policy states: “for a certificate to be used for digitally signing and/or encrypting email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate”
The CA's public documentation needs to provide sufficient information describing how the email address is verified to be owned/controlled by the certificate subscriber. For instance, if a challenge-response type of procedure is used, then there needs to be a brief description of the process. If public resources are used, then there should be a description of which public resources are used, what data is retrieved from public resources, and how that data is used to verify that the certificate subscriber owns/controls the email address.
The recommended way to satisfy this requirement is to perform a challenge-response type of procedure in which the CA sends email to the email address to be included in the certificate, and the applicant must respond in a way that demonstrates that they have control over that email address. For instance, the CA may send an email to the address to be included in the certificate, containing secret unpredictable information, giving the applicant a limited time to use the information within.
It is not sufficient for the CP/CPS to just say that an email is sent to the customer. The CP/CPS needs to be clear that the RA sends email to the email address to be included in the certificate. The CP/CPS needs to be clear that the email shall contain some non-predictable information that the subscriber must then use or respond with to confirm that the owner of the email address actually received the email and responded.

Mozilla 會針對電子郵件認證提出此項規範，主要也是因為他們有提供 thunderbird 電子郵件的服務，因此對植入他們信賴清單中的 ROOT CA 憑證之下屬 CA 關於電子郵件的認證會特別要求。

再者，憑證管理中心本來就應該針對寫入憑證內的所有資訊確認其真偽，既然 MOICA 有要寫入電子郵件並讓用戶使用在安全電子郵件功能上，就應該要對電子郵件進行認證，以確保憑證管理中心是有公信力的，而不是隨便進行審查的

五) 公開信賴憑證管理之憑證政策基礎(Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates)

https://cabforum.org/wp-content/uploads/CAB-Forum-BR-1.3.0.pdf

CA/Browser Forum. Version 1.3.0 April 16, 2015 cabforum.org

TABLE OF CONTENTS

六) 「憑證機構與瀏覽器論壇」章程 (2015)

BYLAWS OF THE CA/BROWSER FORUM
Adopted effective as of 16 October 2014

1. CA/BROWSER FORUM – PURPOSE, STATUS, AND ANTITRUST LAWS

1.1 Purpose of the Forum:

The Certification Authority Browser Forum (CA/Browser Forum) is a voluntary gathering of leading certification authorities (CAs) and vendors of Internet browser software and other applications.

Members of the CA/Browser Forum have worked closely together in defining the guidelines and means of implementation for best practices as a way of providing a heightened security for Internet transactions and creating a more intuitive method of displaying secure sites to Internet users.

1.2 Status of the Forum and Forum Activities

The Forum has no corporate or association status, but is simply a group of CAs and browsers which communicates or meets from time to time to discuss matters of common interest relevant to the Forum's purpose. The Forum has no regulatory or industry powers over its members or others. Other than those rights and responsibilities found in the Forum's Intellectual Property Rights Policy (IPR), Forum "membership" or other participation status does not convey any legal status or rights, but is intended simply as a guide to the levels of participation in Forum activities.

1.3 Intellectual Property Rights Policy; Antitrust Laws and Regulations; Goal; Conduct

Forum Members, Associate Members, and Interested Parties must comply with the then-current IPR policy and all applicable antitrust laws and regulations during their Forum activities.

The historic goal of Forum activities (including development of proposed requirements and guidelines and voting on all matters) has been to seek substantial consensus among Forum Members before proceeding or adopting final work product, and this goal will remain for the future. Members shall not use their participation in the Forum either to promote their own products and offerings or to restrict or impede the products and offerings of other Members.

The Chair will read an antitrust compliance statement at the start of all Forum Meetings (and on other occasions, as the Chair deems necessary) in substantially the following form:

"As you know, this meeting includes companies that compete against one another. This meeting is intended to discuss technical standards related to the provision of existing and new types of digital certificates without restricting competition in

developing and marketing such certificates. This meeting is not intended to share competitively-sensitive information among competitors, and therefore all participants agree not to discuss or exchange information related to:

(a) Pricing policies, pricing formulas, prices or other terms of sale;

(b) Costs, cost structures, profit margins,

(c) Pending or planned service offerings,

(d) Customers, business, or marketing plans; or

(e) The allocation of customers, territories, or products in any way."

2. FORUM MEMBERSHIP AND VOTING

2.1 Qualifying for Forum Membership

(a) CA/Browser Forum members shall meet at least one of the following criteria.

(1) Issuing CA: The member organization operates a certification authority that has a current and successful WebTrust for CAs audit, or ETSI 102042 or ETSI 101456 audit report prepared by a properly-qualified auditor, and that actively issues certificates to Web servers that are openly accessible from the Internet using any one of the mainstream browsers.

(2) Root CA: The member organization operates a certification authority that has a current and successful WebTrust for CAs, or ETSI 102042 or ETSI 101456 audit report prepared by a properly-qualified auditor, and that actively issues certificates to subordinate CAs that, in turn, actively issue certificates to Web servers that are openly accessible from the Internet using any one of the mainstream browsers.

(3) Browser: The member organization produces a software product intended for use by the general public for browsing the Web securely.

(b) Applicants should supply the following information:

(1) Confirmation that the applicant satisfies at least one of the membership criteria (and if it satisfies more than one, indication of the single category under which the applicant wishes to apply).

(2) URL of the current qualifying performance audit report.

(3) The organization name, as you wish it to appear on the Forum Web site and in official Forum documents.

(4) URL of the applicant's main Web site.

(5) Names and email addresses of employees who will participate in the Forum mail list.

(6) Emergency contact information for security issues related to certificate trust.

(c) An Applicant shall become a Member once the Forum has determined by vote that the Applicant meets all of the requirements of subsection (a). A vote of Members shall be held as soon as the Applicant indicates that it has presented all information required under subsection (b) and has responded to all follow-up questions from the Forum and the Member has complied with the requirements of Section 5.5.

2.2 Ballots Among Forum Members

Ballots will be conducted in accordance with the following rules.

(a) Only votes by Members shall be accepted.

(b) Only one vote per Member company shall be accepted; representatives of corporate affiliates shall not vote.

(c) A representative of any Member can call for a proposed ballot to be published for review and comment by the membership. Any proposed ballot needs two endorsements by other Members in order to proceed. The review period then shall take place for at least seven calendar-days before votes are cast.

(d) The CA/Browser Forum shall provide seven calendar-days for voting, with the deadline clearly communicated via the members' electronic mailing list. All voting will take place online via the members' electronic mailing list.

(e) Only votes that indicate a clear 'yes' or 'no' response to the ballot question shall be considered (i.e. votes to abstain and votes that do not indicate a clear 'yes' or 'no' response will not figure in the calculation of item 6, below).

(f) Members fall into two categories: CAs (comprising issuing CAs and root CAs, as defined in the membership criteria) and product suppliers (as defined in the membership criteria). In order for the motion to be adopted by the Forum, two-thirds or more of the votes cast by the Members in the CA category must be in favor of the motion, and at least 50% plus one of the votes cast by the members in the browser

category must be in favor of the motion At least one CA Member and one browser Member must vote in favor of a ballot for the ballot to be adopted.

(g) A ballot result will be considered valid only when more than half of the number of currently active members has participated. The number of currently active members is the average number of member organizations that have participated in the previous three meetings (both teleconferences and face-to-face meetings).

(h) The CA/Browser Forum will tabulate and announce the results within one calendar-day of the close of the voting period.

3. OTHER FORUM PARTICIPATION

3.1 Associate Members

The Forum may enter into associate member relationships with other organizations when the CA/Browser Forum determines that maintaining such a relationship will be of benefit to the work of the Forum. In the past, entities qualifying as Associate Members have included the AICPA/CICA WebTrust Task Force, the European Telecommunications Standards Institute, Paypal, the Internet Corporation for Assigned Names and Numbers, tScheme, the U.S. Federal PKI, and CAs applying for membership but awaiting full qualification under Section 2.1.
Participation as an Associate Member is by invitation only. In order to become an Associate Member, an organization must sign a mutual letter of intent, understanding, or other agreement and the Forum's IPR Agreement, unless this latter requirement is waived in writing by the Forum based on overriding policies of the Associate Member's own organization IPR rules. Associate Members may attend face-to-face meetings, communicate with Forum Members on member lists, and access Forum wiki content. Associate Members are not entitled to vote except on special straw polls of the Forum (e.g. when selecting meeting dates, locations, etc.)

3.2 Interested Parties

Any person or entity that wishes to participate in the Forum as an Interested Party may do so by providing their name, affiliation (optional), and contact information, and by agreeing to the IPR Agreement attached as Exhibit A (indicating agreement by manual signing or digitally signing the agreement).

Interested Parties may participate in Forum activities in the following ways:

(a) By becoming involved in Working Groups,

(b) By posting to the Public Mail List, and

(c) By participating in those portions of Forum Teleconferences and Forum Meetings to which they are invited by the Forum Chair relating to their areas of special expertise or the subject of their Working Group participation.

Interested Parties are required to comply with the provisions of the IPR Agreement and these Bylaws. Interested Parties may lose their status as Interested Parties by vote of the Members, in the Members' sole discretion.

3.3 Other Parties

The public may follow the Forum's activities by reading all postings on the Public Mail List and the Public Web Site. Questions or comments to the Forum may be sent to Questions Mail List.

4. OFFICERS AND FINANCES

4.1 Officers

(a) Term of office: The Forum will elect a Chair and Vice Chair, each to serve for a two-year term. The Vice Chair has the authority of the Chair in the event of any absence or unavailability of the Chair, and in such circumstances, any duty delegated to the Chair herein may be performed by the Vice Chair. For example, the Vice Chair will preside at Forum Meetings and Forum Teleconferences in the Chair's absence. The offices of Chair and Vice Chair may only be filled by Forum Member representatives.

No person may serve as Chair for more than a two-year period or be elected to Vice Chair upon expiration or termination of the person's service as Chair, but a person is eligible to be elected as Chair again after having vacated the position as Chair for at least two years.

(b) Manner of conducting nominations: At least sixty (60) days prior to the expiration of the current Chair's term or upon his/her early termination as Chair, the Chair or Vice Chair will announce through the management mailing list that nominations are open for the office of Chair and the Vice Chair will automatically be nominated as the next Chair, but Forum Members may nominate themselves or others to be additional candidates as Chair. A Vice Chair may decline the nomination to the office of Chair and/or indicate an intent to seek nomination for re-election to the office of Vice Chair. The nomination period for Chair will last for at least one week but no longer than four weeks. Upon the close of the nominations for Chair, the nomination period for the office of Vice Chair shall immediately open. The nomination period for Vice Chair will last for at least one week but no longer than four weeks.

(c) Manner of holding officer elections: If a single individual is nominated for a position, the Forum will hold a ballot to confirm appointment of the nominee. For the confirmation ballot, each Forum Member is entitled to a single vote regardless of the number of participating Forum Member representatives or whether the Forum Member is categorized as a CA or product supplier. If multiple votes are received from a Forum Member's representatives, the last vote submitted during the voting period is considered the Forum Member's vote. The single nominee is considered confirmed if a majority of the Forum members who vote are in favor of the appointment, regardless of the number of votes cast and irrespective of whether 2/3 of the CAs or 1/2 of the product suppliers approve appointment of the nominee.

If more than one candidate is nominated for Chair or Vice Chair, the Forum will announce an election ballot to determine which candidate will fill the position. Within two weeks after the close of the nomination period, the Chair or Vice Chair will establish an election committee and announce the election ballot on the management mailing list along with the ballot start date, ballot end date, and a description of the voting process. The Chair or Vice Chair will appoint the election committee by selecting at least two volunteers who have a reputation for independence, preferably individuals without voting rights in the Forum and that participate as Interested Parties. The election committee is responsible solely for tallying Forum Member votes in connection with the election ballot. The description must include the email address(es) where members will send their vote, which should be the email addresses of the election committee.

For election ballots, each Forum Member is entitled to a single vote regardless of the number of participating Forum Member representatives or whether the Forum Member is categorized as a CA or product supplier. If multiple votes are received from a Forum Member's representatives, the last vote submitted during the voting period is considered the Forum Member's vote. Within

two weeks after the election ballot closes, the election committee will compile the votes, ensure that only one vote is counted per Forum Member, confirm the results with other members of the election committee, and publish the ballot results by sending an email to the public mailing list. The election committee will not include any votes submitted before or after the voting period when compiling the votes. The ballot results email will contain only the following information:
a short description of the ballot purpose, the total number of votes submitted during the ballot period, and the name of the nominee receiving the most votes. The election committee may include other language as necessary to accurately describe the ballot and any concerns the election committee had with the ballot, provided that such language does not disclose how individual Forum Members voted. The election committee will treat the votes of individual Forum Members as confidential information. The nominee receiving the most votes is appointed to the applicable position, regardless of the number of votes cast and irrespective of whether 2/3 of the

CAs or ½ of the product suppliers voted for the nominee. If the election ballot results in a tie among the candidates receiving the most votes, the Chair or Vice Chair will call for another election ballot that includes only the two tying candidates.

(d) Duties: The Chair and Vice Chair shall exercise their functions in a fair and neutral manner, allowing all Members equal treatment for their comments and proposals, and shall not favor one side over another in any matter (except that the Chair and Vice Chair may indicate their own position during discussion and voting on the matter). The Chair and Vice Chair shall have no personal liability for any activities of the Forum or its Members or Interested Parties.

The Chair or the Vice Chair may sign correspondence, applications, forms, Letters of Intent, and Memoranda of Understanding relating to projects with standards bodies, industry groups, and other third parties, but shall have no personal liability therefor.

4.2 Finances

Because the Forum has no corporate status, it will not maintain funds or banking accounts. The costs of operating Forum websites or mailing lists will be covered by voluntary contribution from Forum Members (who may seek voluntary contributions from other Members to help defray
such costs). Forum Members may propose other group activities which they propose to sponsor (e.g., research projects, etc.) which require funding and may seek voluntary contributions from other Members for such activities.

Forum Meetings may be held from time to time upon the voluntary sponsorship of one or more Forum members. The sponsor of a Forum Meeting may suggest a fixed cost per meeting participant as reimbursement to the sponsor to cover (a) the cost of meeting rooms and refreshments, and (b) the cost of any meeting dinner or other group activity. Sponsors will be encouraged to announce any suggested per-participant fixed cost reimbursement amount in advance of the Forum Meeting for participant planning purposes, and will provide a statement or invoice to each participant upon request after the Forum Meeting for submission to the participant's accounting department. All per-participant reimbursements shall be paid directly to the sponsor.

Interested Parties will not be required to pay anything for their participation in Forum activities, but must cover their own expenses for participation in any Working Group meetings.

5. FORUM ACTIVITIES

5.1 Member Mail List and Member Web Site

The Forum shall maintain a Member Mail List and Member Web Site that are not accessible by the public. The following matters may be posted to the Member Mail List and Member Web Site:

(a) Draft minutes of Forum meetings (both virtual and in-person, and including any sub- groups or committees) will be posted to the Member Mail List to allow Members to make sure they are being correctly reported.

Minutes will be considered Final when approved at a subsequent Forum Meeting or Forum Teleconference, or after 2 weeks have elapsed since publication of the draft if no Forum Meeting or Forum Teleconference is imminent. Final minutes will then be posted to the Public Mail List and Public Web Site. The Chair will, upon request, make redactions of any part of the public copy of the minutes identified as private or sensitive by either the information discloser or a member mentioned or affiliated with the subject of the information.

(b) Messages formally announcing ballots or ballot outcomes, including vote and quorum counts, will be posted to the Public Mail List. However, ballots and the listing of final votes by each Member will only be posted to the Member Mail List and Member Web Site.

(c) Nominations for officer positions, Forum Meeting and Forum Teleconference scheduling issues, and discussion of Forum financial issues.

(d) Security incidents if, in the opinion of the Members, discussion on the Public Mail List could reasonably be detrimental to the implementation of security measures by Members.

(e) Proposed responses to questions sent to the Questions Mail List.

(f) Matters which, in the opinion of the Members, require confidentiality.

Members have discretion about which mailing list they use, but are strongly encouraged to use the Public Mail List for matters other than those listed above.

Members are strongly discouraged from posting the text of Member Mail List messages to the Public Mail List without the permission of the author or commenter.

5.2 Public Mail List and Public Web Site

The Chair shall appoint a List Manager who shall maintain a Public Mail List. Forum Members and Interested Parties may post to the Public Mail List in compliance with these Bylaws.
Anyone else is allowed to subscribe to and receive messages posted to the Public Mail

List, which may be crawled and indexed by Internet search engines.

The Chair shall appoint a Webmaster. The Webmaster shall post instructions on the Public Web Site for subscribing to the Public Mail List.

The following materials shall be posted to the Public Mail List or Public Web Site:

(a) Draft and final agendas for Working Group meetings, Forum Meetings and Forum Teleconferences (including any sub-groups or committees).
(b) Final minutes of Forum Meetings and Forum Teleconferences (including minutes of any sub-groups or committees), and minutes of all Working Group teleconferences and meetings.
(c) Messages formally proposing a Forum ballot (including ballots to establish, modify, or terminate Working Groups) and announcing ballot outcomes, including vote and quorum counts but not identifying individual votes by name of Member.
(d) Initial and final drafts of Forum requirements, guidelines, and recommendations after the drafter has had an opportunity to receive and respond to initial Member comments.
(e) Initial and final drafts of Working Group requirements, guidelines, and recommendations after the drafter has had an opportunity to receive and respond to initial Working Group member comments.

5.3 Working Groups

Members may propose by ballot the appointment of Working Groups open to participation by Members and Interested Parties. The ballot shall outline the scope of the Working Group's activities, including deliverables, any limitations, and Working Group expiration date. Upon approval of the Working Group, the Chair will call for a show of interest in participation by Members, and shall appoint a Working Group Chair from among the interested Members.

Upon creation of a Working Group, the Forum will post an invitation to all Interested Parties to participate, and will solicit others with expertise and interest in the Working Group subject matter to become Interested Parties and participate in the Working Group. With the approval of the Chair, Working Groups may establish separate list-servs, wikis, and web pages for their communications, but all such separate list-servs must be managed in the same fashion as the Public Mail List. Working Groups may meet by teleconference or face-to-face meetings upon approval by the Chair and the Working Group Chair, but the Forum shall not be responsible for the expenses of any such teleconferences or meetings.

Working Groups may draft recommendations to be forwarded to the Forum for its consideration, but no recommendations will be considered the product of the Working Group unless approved by two-thirds of all Working Group members who vote on the

recommendations. All substantial initial and final drafts of the Working Group product will be posted on the Public Mail List.

The Forum shall review the final recommendations from a Working Groups and may approve and implement some or all of the recommendations as appropriate in the Forum's judgment following the Forum's regular voting rules. The Forum shall retain the right to amend a Working Group recommendation before approval, but in most cases should first return the proposed amended recommendation to the Working Group for its review and response before voting.

The Forum shall not be required to submit any matter to a Working Group, but may itself draft requirements and guidelines without a Working Group in its discretion.

5.4 Forum Teleconferences and Forum Meetings

From time to time the Forum will hold Forum Teleconferences and Forum Meetings among the Members and Associate Members, who may participate in person or (where feasible) by teleconference. Interested Parties and others may be invited by the Chair, in the Chair's discretion, to participate in those portions of Forum Teleconferences and Forum Meetings that are relevant to their expertise or their participation in Working Groups.

5.5 IPR policies

As a requirement for membership, Members must execute and return to the Chair the IPR Agreement attached as Exhibit A.

As a requirement for participation as an Associate Member or Interested Party, Associate Members and Interested Parties must execute and return to the Chair the IPR Agreement attached as Exhibit A.

5.6 Project Lifecycle

In general, Forum projects will follow the model Project Lifecycle attached as Exhibit B. However, the Members may modify this model as appropriate by their subsequent actions.

6. MISCELLANEOUS

6.1 Posting and Amendment of the Bylaws

The current Bylaws shall be posted to the Public Web Site. These Bylaws may be amended by subsequent ballot of the Members.

6.2 Procedure for Dealing with Questions and Comments

The Forum procedure for dealing with questions and comments sent to the Questions Mail List shall be as follows. The Chair shall appoint a Questions List Coordinator. The responsibilities of the Questions List Coordinator are:

(a) If practical, within 24 hours send an acknowledgment to the questioner indicating that the question or comment has been received and that a response will provided as soon as is practical.
(b) Coordinate discussion using the Member Mail List until consensus has been achieved.
(c) Post the proposed response to the Member Mail List indicating that Members have 24 hours to object.
(d) If no objections are received before the deadline expires, then send the response to the questioner.
(e) If consensus cannot be achieved, or one or more objections are received, then the matter should be dealt with in the next Forum Meeting or Forum Teleconference.

DEFINITIONS

Forum Meetings: Face-to-face meetings of Members as scheduled from time to time.

Forum Teleconferences: Teleconference meetings of Members as scheduled from time to time.

Member: A Member of the Forum or a representative of the Member (depending on context).

Member Mail List: The email list-serv maintained by the Forum for communications by and among Forum Members. The Member Mail List is not available to Interested Parties or Other Parties.

Member Web Site: The password-protected web site available only to Members (currently called the CA/Browser Forum Wiki).

Public Mail List: The public email list-serv currently located at public@cabforum.org maintained by the Forum for communications by and among Members and Interested Parties. The Public Mail List may be read by Other Parties, but Other Parties may not post to the Public Mail List.

Public Web Site: The web site available only to Members, Interested Parties, and

Other Parties (currently located at cabforum.org). A Forum Member will be appointed as Webmaster and will control all postings to the Public Web Site.

Questions Mail List: The email list-serv currently located at questions@cabforum.org maintained by the Forum for communications from the public to the Forum.

Exhibit A

CAB Forum IPR Policy Agreement
This CAB Forum IPR Policy Agreement (the "Agreement") constitutes a binding contract amongst all participants who make Contributions during the process of developing a Draft Guideline for the purpose of incorporating such material into a Draft Guideline or a Final Guideline of the CA / Browser Forum.

In consideration of the mutual promises herein, Participant agrees on his/her/its behalf, and on behalf of any Affiliates, to abide by the terms of the Intellectual Property Rights Policy of the CAB Forum (the "IPR Policy") v.1.0, incorporated herein by reference. Participant acknowledges that some of its obligations under the IPR Policy may survive the termination of this Agreement, as more fully described in the IPR Policy.

The party signing this Agreement intends that it shall take effect as an instrument under seal. If such party is not a natural person, the individual signing this Agreement for the Participant represents and warrants that he or she has the authority to enter into this Agreement on behalf of the Participant.

The Participant represents and warrants that either: (a) it has the authority to enter into this Agreement on behalf of all of its Affiliates; or (b) it has no Affiliates; or (c) each of its Affiliates has executed and delivered to the CAB Forum a countersignature to this Agreement, indicating that it consents to this Agreement, and agrees to enforce this Agreement's terms as to any of such Affiliate's Intellectual Property, including such terms as may properly be changed by the CAB Forum by notice to the Participant under this Agreement.

PARTICIPANT

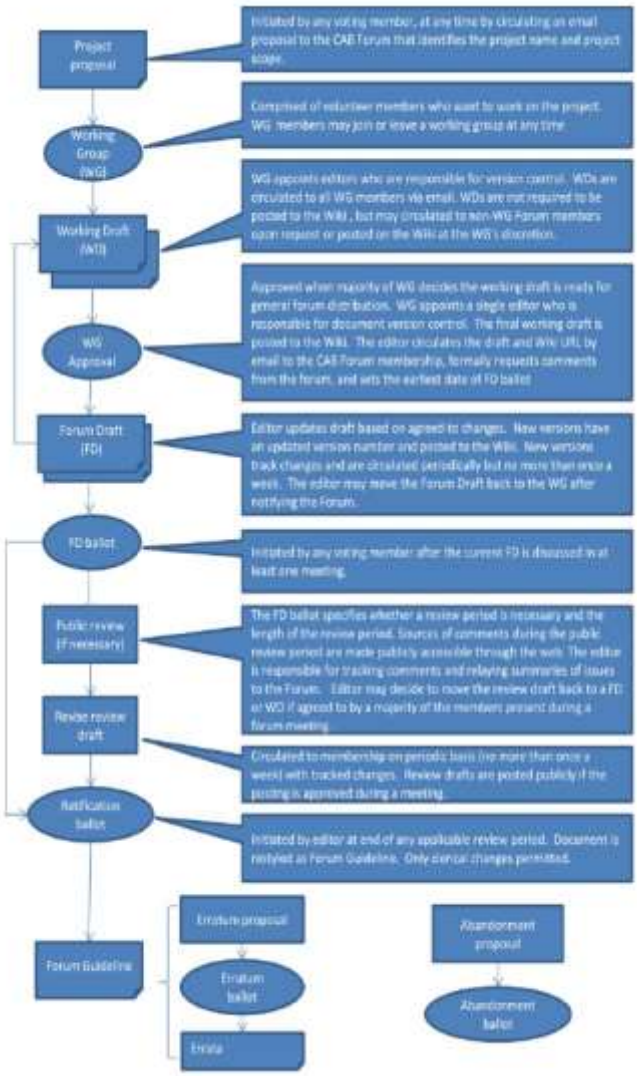
By:
(Signature)

Print Name

Title:

Participant Organization Name (if entity)

Exhibit B - Project Lifecycle



附件三 會議活動照片

會議場地：瑞士蘇黎世 Atrium Hotel Blume

會議會場圖 之一

會議會場圖 之二

與 CA/Brower Forum 會長 Mr. Dean Coclin 合照

與 CA/Brower Forum 副會長 Mr. Kirk Hall 合照

地主國 瑞士會員代表致歡迎詞