# 附件 1：**應用系統配合未來政府公開金鑰基礎建設（GPKI）採用 2048 位元憑證 IC 卡改版建議期程**

以下假設 GPKI 之任一 CA 將於日期 D (D day)開始簽發 2048 位元憑證 IC 卡，則往前推算 180 天(即日期 D-180)至日期 D 之間，應用系統配合改版之程序，建議如下表：

表 1：應用系統配合改版之程序

| 日期 | 完成事項 |
|---|---|
| D-180 | **應用系統開發廠商取得「新版 API 測試套件包」，並開始進行應用系統改版，使新版應用系統能夠搭配新版 API 使用。**<br>1：行政院研考會、內政部、及經濟部舉辦 API 改版說明會(註 1)，並贈送參加說明會的機關或廠商 1 份「新版 API 測試套件包」(註 2)，套件包內含 2 張測試 IC 卡、1 部讀卡機、1 張新版 API 光碟。<br>2：未參加說明會之機關或廠商，請另發函向行政院研考會、內政部、及經濟部索取「新版 API 測試套件包」。<br>(註 1) 經濟部已於 97 年 8 月 28 日辦竣，行政院研考會 97 年 10 月 22 日辦竣。<br>(註 2) 此新版 API 測試套件包相容於行政院研考會、內政部、及經濟部所主管 CA 所發新舊用戶憑證。 |
| D-90 | **以 3 個月(由 D-180 至 D-90)的時間完成新版應用系統開發及測試(舊版系統於此期間請繼續保持運作)**。 |
| D-60 | **完成新版應用系統部署及上線，同時保留舊版應用系統併行運作。** |

| 日期 | 完成事項 |
| --- | --- |
| | 1：建議於新版系統之網頁保留一個超連結供用戶使用舊版系統，當用戶無法使用新版系統（可能是因為用戶電腦同時必須使用另一個尚未改用新版 API 之應用系統，而需要舊版 SafeSign CSP/PKCS#11 或舊版 HiSecure API 舊版）時，先暫時讓用戶回去使用舊版系統(可能要請用戶重新下載及安裝 SafeSign 工具)。<br>2：由於新版 API 必須請用戶下載及安裝「HiCOS 卡片管理工具」，因此建議新版系統網頁上指引用戶至各 CA 網站下載「HiCOS 卡片管理工具」。<br>3：在日期 D-60 時，GPKI 各 CA 網站會開始提供 「HiCOS 卡片管理工具」，同時也會繼續提供 SafeSign 工具供用戶下載。 |
| D | **正式切換到新版應用系統系統，舊版應用系統予以下架。**<br>1：到達日期 D 時，也就是 GPKI 之中有一個 CA 開始簽發 2048 位元憑證 IC 卡的日子，此時所有的 PKI-enabled 應用系統皆應切換到新版，否則會影響其他已經切換到新版的應用系統。<br>2：到達日期 D 時，不管是 GPKI 之中哪一個 CA 開始簽發 2048 位元憑證 IC 卡，不論應用系統是否會使用到該 CA 所簽發出來的 2048 位元憑證 IC 卡，皆應配合切換至新版，如果不切換，則該應用系統之用戶因使用其他應用系統而安裝了新版 API 之相關動態函式庫檔案(如 DLL 檔)，則該尚未切換到新版之應用系統，將可能會受到影響，而無法在該用戶的電腦上使用。 |

| 日期 | 完成事項 |
| --- | --- |
| | 3：到達日期 D 時，GPKI 各 CA 網站會將 SafeSign 工具下架，而開始只提供 「HiCOS 卡片管理工具」。 |


註:上述 MOEACA 及 MOICA 期程為暫定，擬待經濟部商業司及內政部近期確認。