行政機關電子憑證推行小組第 10 次委員會議紀錄

壹、時間：96 年 8 月 31 日（星期五）上午 10 時 40 分

貳、地點：宜蘭蘇澳鎮中山路 1 段 220 號

參、主席：陳副主任委員俊麟（何處長全德代） 記錄：戴慧明

肆、出列席人員（如簽到冊）

伍、主席致詞（略）

陸、討論事項及決議

一、GPKI相關文件修訂審查：

（一）政府機關公開金鑰基礎建設憑證政策修正，請增加時戳時間源之說明。

（二）政府機關公開金鑰基礎建設憑證及憑證廢止清冊格式剖繪1.2.1節(12) 請修訂為「伺服器應用軟體憑證簽發對象為政府機關（構)、單位及業務主管機關認可的組織或團體的伺服應用軟體程序（Server AP)，例如Secure Web (SSL) Server、Time Stamp Server、OCSP Server及專屬應用伺服軟體等」。

二、 GPKI相關文件修訂備查報告：

（一）有關GCA CPS、MOEACA CPS、XCA CPS審查意見如下：

1.有關憑證實務作業基準6.1.5節「用戶使用1024位元或2048位元的RSA金鑰」及6.3.2.2 節「當金鑰長度為RSA 2048位元時，公開金鑰憑證之使用期限至多為10年，私密金鑰之使用期限至多為10年。」修正建議，本次不進行修正，俟未來用戶金鑰長度變更時，再配合修改。

2.有關憑證實務作業基準6.6.1節「本管理中心的系統研發遵循能力成熟度模式整合(Capability Maturity Model Integration, CMMI）的規範進行品質控管」乙節，修訂為「本管理中心的系統研發遵循主管機關認可之品質管理規範進行品質控管」。

（二）政府測試憑證管理中心憑證實務作業基準修正乙節同意備查。

三、 時戳政策討論：

（一）後續請與相關應用及主管單位(如經濟部商業司、衛生署及檔管局)研議相關需求。

（二）建議中華電信股份有限公司邀集相關產業及主管機關，研究籌設時戳服務之可行性。

（三）電子化政府相關應用系統應使用本國之標準時間源。