【19】中華民國　　【12】專利公報　（B）

【11】證書號數：I941301
【45】公告日： 中華民國 115 (2026) 年 10 月 01 日
【51】Int. Cl.：　*H04L9/28　(2006.01)*　*G06F21/60　(2013.01)*
G06N10/00　(2022.01)

發明　　全 9 頁

【54】名　稱：申請與產製後量子密碼學多用途憑證的系統及其方法
【21】申請案號：114125517　　【22】申請日： 中華民國 114 (2025) 年 07 月 04 日
【72】發 明 人： 陳志華 (TW) CHEN, CHI-HUA；童韋豪 (TW) TUNG, WEI-HAO；林邦曄 (TW) LIN, BON-YEH；繆嘉新 (TW) MIOU, CHAR-SHIN
【71】申 請 人： 中華電信股份有限公司　CHUNGHWA TELECOM CO., LTD.
桃園市楊梅區電研路 99 號
【74】代 理 人： 卓俊傑；劉亞君
【56】參考文獻：

CN	118972049A	US	10630476B1
US	2020/0280436A1	US	2021/0377049A1
US	2022/0209944A1		

審查人員：賴奕儒

【57】申請專利範圍

1. 一種申請與產製後量子密碼學多用途憑證的系統，包括：
終端設備；以及
憑證中心，通訊連接至該終端設備，其中
該終端設備產製後量子密碼學多用途憑證申請請求，並且該終端設備傳送該後量子密碼學多用途憑證申請請求至該憑證中心，其中該後量子密碼學多用途憑證申請請求至少包括主題資訊、簽章值、該終端設備的數位簽章演算法公鑰以及該終端設備的金鑰封裝機制公鑰；
該憑證中心根據該後量子密碼學多用途憑證申請請求產製多用途憑證，其中該多用途憑證至少包括數位簽章演算法識別碼、憑證序號、該主題資訊、憑證效期、主題公鑰資訊、擴展資訊以及該簽章值。
2. 如請求項 1 所述的系統，其中
該憑證中心取得該後量子密碼學多用途憑證申請請求中的該主題資訊，並且取得該終端設備的該數位簽章演算法公鑰以及該終端設備的該金鑰封裝機制公鑰；
該憑證中心根據該數位簽章演算法識別碼，運用該憑證中心的私鑰對該多用途憑證的待簽章內容執行數位簽章演算法來產製該簽章值；
該擴展資訊至少包括金鑰用途，該金鑰用途至少包括數位簽章；
該主題公鑰資訊至少包括該數位簽章演算法公鑰；
該多用途憑證至少包括該金鑰封裝機制公鑰。
3. 如請求項 2 所述的系統，其中
該主題公鑰資訊更包括該金鑰封裝機制公鑰；該金鑰用途更包括資料加密。
4. 如請求項 2 所述的系統，其中
該擴展資訊更包括主題可選公鑰資訊；
該主題可選公鑰資訊至少包括該金鑰封裝機制公鑰；
該金鑰用途更包括資料加密。

5. 如請求項 2 所述的系統，其中
該擴展資訊更包括 Delta 憑證；
該 Delta 憑證中的該主題公鑰資訊至少包括該金鑰封裝機制公鑰；
該 Delta 憑證中的該金鑰用途至少包括資料加密。

6. 如請求項 5 所述的系統，其中
該 Delta 憑證包括該數位簽章演算法識別碼以及該簽章值；
該憑證中心根據該 Delta 憑證中的該數位簽章演算法識別碼，運用該憑證中心的該私鑰對該多用途憑證的該待簽章內容執行該數位簽章演算法來產製該 Delta 憑證中的該簽章值。

7. 如請求項 2 所述的系統，其中
該數位簽章演算法公鑰是 ML-DSA（Module-Lattice-Based Digital Signature Algorithm）公鑰、SLH-DSA（Stateless Hash-Based Digital Signature Algorithm）公鑰以及 Falcon 公鑰中的其中之一。

8. 如請求項 2 所述的系統，其中
該金鑰封裝機制公鑰是 ML-KEM（Module-Lattice-Based Key-Encapsulation Mechanism）公鑰。

9. 如請求項 1 所述的系統，其中
該憑證中心產製後量子密碼學多用途憑證回應。

10. 如請求項 9 所述的系統，其中
該後量子密碼學多用途憑證回應包括金鑰封裝資訊、金鑰包裹以及該多用途憑證的密文；
該憑證中心產製第一對稱式金鑰以及第二對稱式金鑰；
該憑證中心運用該終端設備的該金鑰封裝機制公鑰加密該第一對稱式金鑰而得到該金鑰封裝資訊；
該憑證中心運用該第一對稱式金鑰加密該第二對稱式金鑰而得到該金鑰包裹；
該憑證中心運用該第二對稱式金鑰加密該多用途憑證而得到該多用途憑證的該密文。

11. 如請求項 10 所述的系統，其中
該終端設備產製後量子密碼學多用途憑證確認；
該後量子密碼學多用途憑證確認包括該後量子密碼學多用途憑證申請請求的雜湊值以及該多用途憑證的該雜湊值；
該終端設備運用雜湊函數計算該後量子密碼學多用途憑證申請請求而得到該後量子密碼學多用途憑證申請請求的該雜湊值；
在該終端設備收到該後量子密碼學多用途憑證回應後，該終端設備運用該終端設備的金鑰封裝機制私鑰解密該金鑰封裝資訊以取得該第一對稱式金鑰；
該終端設備運用該第一對稱式金鑰解密該金鑰包裹以取得該第二對稱式金鑰；
該終端設備運用該第二對稱式金鑰解密該多用途憑證的該密文以取得該多用途憑證；
該終端設備運用該雜湊函數計算該多用途憑證而得到該多用途憑證的該雜湊值；
藉此，達到該金鑰封裝機制私鑰的所有權證明（Proof Of Possession，PoP）。

12. 如請求項 9 所述的系統，其中
該後量子密碼學多用途憑證回應包括金鑰封裝資訊、金鑰包裹以及憑證壓縮檔的密文；
該憑證中心產製數位簽章用憑證以及金鑰封裝用憑證，並且該憑證中心壓縮該數位簽章用憑證以及該金鑰封裝用憑證以取得該憑證壓縮檔；
該憑證中心產製第一對稱式金鑰以及第二對稱式金鑰；

該憑證中心運用該終端設備的該金鑰封裝機制公鑰加密該第一對稱式金鑰而得到該金鑰封裝資訊；

該憑證中心運用該第一對稱式金鑰加密該第二對稱式金鑰而得到該金鑰包裹；

該憑證中心運用該第二對稱式金鑰加密該憑證壓縮檔而得到該憑證壓縮檔的該密文。

13. 如請求項 12 所述的系統，其中

該終端設備產製後量子密碼學多用途憑證確認；

該後量子密碼學多用途憑證確認包括該後量子密碼學多用途憑證申請請求的雜湊值以及該金鑰封裝用憑證的該雜湊值；

該終端設備運用雜湊函數計算該後量子密碼學多用途憑證申請請求而得到該後量子密碼學多用途憑證申請請求的該雜湊值；

在該終端設備收到該後量子密碼學多用途憑證回應後，該終端設備運用該終端設備的金鑰封裝機制私鑰解密該金鑰封裝資訊以取得該第一對稱式金鑰；

該終端設備運用該第一對稱式金鑰解密該金鑰包裹以取得該第二對稱式金鑰；

該終端設備運用該第二對稱式金鑰解密該憑證壓縮檔的該密文以取得該憑證壓縮檔；

該終端設備解壓縮該憑證壓縮檔以取得該數位簽章用憑證以及該金鑰封裝用憑證；

該終端設備運用該雜湊函數計算該金鑰封裝用憑證而得到該金鑰封裝用憑證的該雜湊值；

藉此，達到該金鑰封裝機制私鑰的所有權證明（Proof Of Possession，PoP）。

14. 一種申請與產製後量子密碼學多用途憑證的方法，適於包括終端設備以及憑證中心的系統，其中該方法包括以下步驟：

該終端設備產製後量子密碼學多用途憑證申請請求，並且該終端設備傳送該後量子密碼學多用途憑證申請請求至該憑證中心，其中該後量子密碼學多用途憑證申請請求至少包括主題資訊、簽章值、該終端設備的數位簽章演算法公鑰以及該終端設備的金鑰封裝機制公鑰；以及

該憑證中心根據該後量子密碼學多用途憑證申請請求產製多用途憑證，其中該多用途憑證至少包括數位簽章演算法識別碼、憑證序號、該主題資訊、憑證效期、主題公鑰資訊、擴展資訊以及該簽章值。

圖式簡單說明

圖 1 是根據本發明的一實施例繪示的申請與產製後量子密碼學多用途憑證的系統的示意圖。

圖 2 是根據本發明的一實施例繪示的申請與產製後量子密碼學多用途憑證的方法的流程圖。

圖 3A 是圖 1 所示的系統的一個實施範例。

圖 3B 是圖 3A 的步驟 S21 的進一步說明。

圖 3C 是圖 3A 的步驟 S23-1 的進一步說明。

圖 4A 是圖 1 所示的系統的另一實施範例。

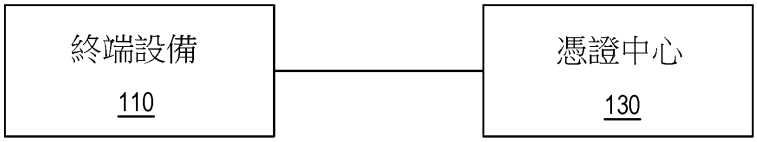
圖 4B 是圖 4A 的步驟 S21 的進一步說明。

圖 4C 是圖 4A 的步驟 S23-2 的進一步說明。

圖 5 是根據本發明的一實施例繪示的多用途憑證的示意圖。

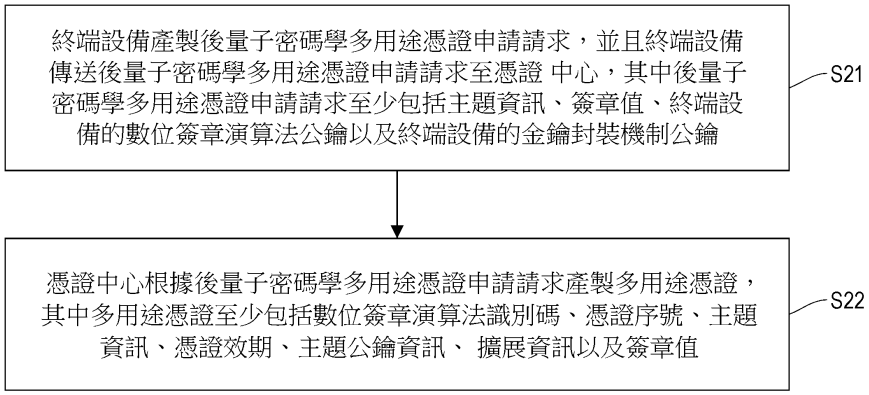
圖 6 是根據本發明的另一實施例繪示的多用途憑證的示意圖。

圖 7 是根據本發明的再一實施例繪示的多用途憑證的示意圖。

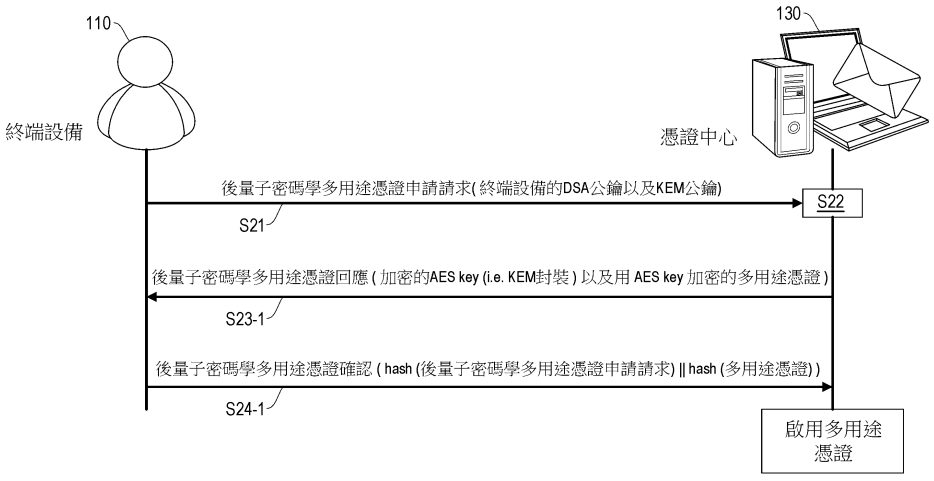

終端設備
110
憑證中心
130

100

【圖1】


終端設備產製後量子密碼學多用途憑證申請請求，並且終端設備傳送後量子密碼學多用途憑證申請請求至憑證 中心，其中後量子密碼學多用途憑證申請請求至少包括主題資訊、簽章值、終端設備的數位簽章演算法公鑰以及終端設備的金鑰封裝機制公鑰
S21
憑證中心根據後量子密碼學多用途憑證申請請求產製多用途憑證，其中多用途憑證至少包括數位簽章演算法識別碼、憑證序號、主題資訊、憑證效期、主題公鑰資訊、 擴展資訊以及簽章值
S22

【圖2】


110
終端設備
130
憑證中心
後量子密碼學多用途憑證申請請求(終端設備的DSA公鑰以及KEM公鑰)
S21
S22
後量子密碼學多用途憑證回應 (加密的AES key (i.e. KEM封裝) 以及用 AES key 加密的多用途憑證)
S23-1
後量子密碼學多用途憑證確認 (hash (後量子密碼學多用途憑證申請請求) || hash (多用途憑證))
S24-1
啟用多用途憑證

【圖3A】

後量子密碼學多用途憑證申請請求 **(PKCS#10)**
Subject: cn= 終端設備
SPKI: alg: ML-DSA-65 key: ...}
Extensions:
KEM-SPKI: {alg: ML-KEM-768 key: ...}
Sig: {ML-DSA-65}

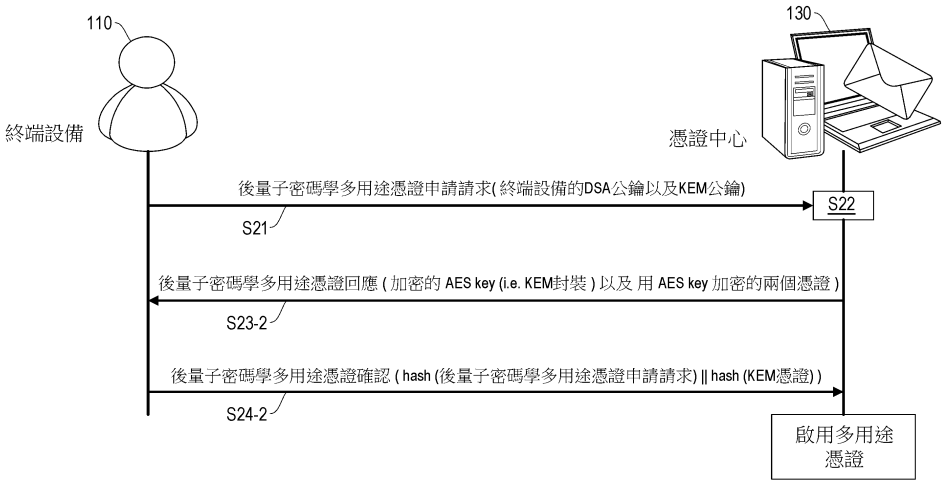
S21

【圖3B】

EnvelopedData(PKCS#7)
RecipientInfos: KEMRecipientInfo: { rid: ... **kem: ML-KEM-768** **kemct: ML-KEM Encapsulation** kdf: KMAC256-KDF wrap: aes256-wrap encryptedKey: ...}
EncryptedContentInfo: { ContentEncryptionAlgorithmIdentifier: AES-256-CBC EncryptedContent: 加密後的多用途憑證}

S23-1

【圖3C】



【圖4A】

後量子密碼學多用途憑證申請請求 (PKCS#10)
Subject: cn= 終端設備
SPKI: alg: ML-DSA-65 key: …}
Extensions:
KEM-SPKI: {alg: ML-KEM-768 key: …}
Sig: {ML-DSA-65}

S21

【圖4B】

EnvelopedData(PKCS#7)
RecipientInfos: KEMRecipientInfo: { rid: ... **kem: ML-KEM-768** **kemct: ML-KEM Encapsulation** kdf: KMAC256-KDF wrap: aes256-wrap encryptedKey: ...}
EncryptedContentInfo: { ContentEncryptionAlgorithmIdentifier: AES-256-CBC EncryptedContent: 加密後的兩個憑證 }

S23-2

【圖4C】

多用途憑證 **(X.509)**
Subject: cn= 終端設備

SPKI: {
alg: ML-DSA-65||ML-KEM-768
key: {
ML-DSA-65 key ||
ML-KEM-768 key
}
}

Extensions:
Key Usage: { digitalSignature dataEncipherment }
Sig: {ML-DSA-87}

【圖5】

多用途憑證 (X.509)
Subject: cn= 終端設備

SPKI: {
alg: ML-DSA-65
key: …
}

Extensions:
Key Usage: { digitalSignature dataEncipherment}
KEM-SPKI: {**alg: ML-KEM-768** **key: …**}
Sig: {ML-DSA-87}

【圖6】

多用途憑證 **(X.509)**
Subject: cn= 終端設備

SPKI: {
alg: ML-DSA-65
key: ...}
}

Extensions:
Key Usage: {digitalSignature}
DeltaCertificateDescriptor:
SPKI: {**alg: ML-KEM-768** **key: ...**}
Key Usage: {dataEncipherment}
Sig: {ML-DSA-87}
Sig: {ML-DSA-87}

【圖7】