

ICS 33.200

中華民國國家標準

C N S

電力系統管理及關聯資訊交換－資料及通訊安全－第 9 部：電力系統設備之網宇安全金鑰管理

Power systems management and associated
information exchange – data and communications
security – part 9: cyber security key management
for power system equipment

草-制 1130168

中華民國 年 月 日制定公布

Date of Promulgation: - -

目 錄

節 次	頁 次
前言	4
1. 適用範圍	6
2. 引用標準	7
3. 用語定義及縮寫	8
3.1 用語及定義	8
3.2 縮寫	13
4. 適用於電力系統之安全概念	16
4.1 一般	16
4.2 安全目標	16
4.3 密碼演算法及概念	18
5. 金鑰建立及管理技術	19
5.1 一般	19
5.2 金鑰管理生命週期	19
5.3 密碼金鑰使用	23
5.4 金鑰管理系統安全政策	24
5.5 電力系統運作之金鑰管理設計原則	24
5.6 對稱金鑰之建立	25
5.7 公開金鑰基礎建設(PKI)及權限管理基礎建設(PMI)所支援之信任	30
5.8 公開金鑰憑證之憑證管理	35
5.9 公開金鑰憑證之撤銷	46
5.10 經由非 PKI 核發之(自我簽署)憑證信任	52
5.11 授權及驗核清單	52
6. 金鑰管理(規定)	54
6.1 一般	54
6.2 安全事件之處理	54

6.3	要求之密碼材料	54
6.4	隨機數產生	55
6.5	物件識別符	55
7.	非對稱金鑰管理(規定).....	56
7.1	一般	56
7.2	憑證組件	56
7.3	憑證產生及安裝	59
7.4	憑證組件及憑證查證	65
7.5	憑證撤銷	80
7.6	憑證逾期及更新	81
7.7	時鐘同步及準確度	82
7.8	授權及驗核清單	82
8.	群組式金鑰管理(規定).....	87
8.1	GDOI 要求事項	87
8.2	網際網路金鑰交換第 1 版(IKEv1)	87
8.3	階段 1 IKEv1 主模式交換型式 2	89
8.4	階段 1/2 ISAKMP 資訊交換型式 5	94
8.5	階段 2 GDOI GROUPKEY-PULL 交換型式 32	97
8.6	階段 2 GROUPKEY-PUSH 交換型式 33	115
8.7	運作考量事項	117
9.	協定實作符合性聲明(PICS).....	121
9.1	一般	121
9.2	記法	121
9.3	一般金鑰管理要求事項之符合性	121
9.4	非對稱金鑰管理要求事項之符合性	122
9.5	群組式金鑰管理之要求事項	123
9.6	支援之 GDOI 酬載 OID.....	123

附錄 A (參考) 與本系列標準其他各部及其他 IEC 標準之關係	125
附錄 B (參考) 密碼演算法及機制	127
B.1 信任及信任錨	127
B.2 密碼演算法	127
B.3 公開金鑰演算法	129
B.4 對稱金鑰演算法	138
B.5 雜湊演算法	140
B.6 完整性核對值(ICV)演算法	141
B.7 具相關聯資料鑑別加密(AEAD)演算法	143
B.8 Diffie-Hellman 金鑰協議	145
B.9 金鑰衍生	149
B.10 密碼演算法之移轉	150
B.11 後量子運算密碼學	150
B.12 隨機數產生(RNG).....	151
附錄 C (參考) 憑證登錄及更新流程圖	154
C.1 憑證登錄	154
C.2 憑證更新	155
附錄 D (參考) 對映本系列標準第 14 部之安全事件	156
D.1 一般	156
D.2 信符傳送及登錄之安全事件日誌紀錄	156
D.3 用於公開金鑰憑證查證之安全事件日誌紀錄	157
D.4 用於屬性憑證查證之安全事件日誌紀錄	160
D.5 憑證撤銷狀態之安全事件紀錄	162
D.6 用於具 GDOI 之群組式金鑰管理的安全事件日誌紀錄	162
參考資料	164
名詞對照	170
相對應國際標準	174

(共 139 頁)

(共 XX 頁)

前言

本標準係依據 2023 年發行之第 2.0 版 IEC 62351-9，不變更技術內容，制定成為中華民國國家標準者。

本標準係依標準法之規定，經國家標準審查委員會審定，由主管機關公布之中華民國國家標準。

依標準法第四條之規定，國家標準採自願性方式實施。但經各該目的事業主管機關引用全部或部分內容為法規者，從其規定。

本標準並未建議所有安全事項，使用本標準前應適當建立相關維護安全及健康作業，並且遵守相關法規之規定。

本標準之部分內容，可能涉及專利權、商標權與著作權，主管機關及標準專責機關不負責任何或所有此類專利權、商標權與著作權之鑑別。

1. 適用範圍

本標準規定密碼金鑰管理，主要聚焦於長期金鑰之管理，其通常係非對稱金鑰對，諸如公開金鑰憑證及對應的私密金鑰。因憑證建立基底，故本標準建立供用許多 CNS 62351 服務用之基礎(亦參照附錄 A)。本標準亦考量對稱金鑰管理，但僅限於如本系列標準第 6 部中所套用之群組式通訊的會期金鑰。本標準之目標係藉由規定或限制將使用的金鑰管理選項，以定義達成金鑰管理互運性之要求事項及技術。

備考：本系列標準過去編號為 CNS 15874，未來皆使用 CNS 62351 之編號，以便與 IEC 62351 系列標準調和。

本標準假設組織(或組織群組)已定義安全政策，以選擇將利用之金鑰及密碼演算法的型式，其可能須與其他標準或法規要求事項保持一致。因此，本標準僅規定此等選定之金鑰及密碼基礎建設的管理技術。本標準假設讀者對密碼學及金鑰管理原理有著基本瞭解。

通訊協定全景中成對之對稱(會期)金鑰的管理要求事項，規定於利用或規定成對通訊之本系列各部標準中，諸如：

- 第 3 部，藉由建立 TLS 選項之剖繪供 TLS 用。
- 第 4 部，供應用層端對端安全用。
- 第 5 部，用於 IEC 60870-5-101/104 及 IEEE 1815 (DNP3)之應用層安全機制。

電力系統通訊協定全景中對稱群組金鑰管理之要求事項，供利用群組安全以保護 GOOSE 及 SV 通訊用，規定於本系列標準第 6 部中。本系列標準第 9 部利用 GDOI 作為已以 IETF 所規定之群組式金鑰管理協定，管理群組安全參數，並增強此協定以載送通用物件導向變電所事件(generic object-oriented substation event, GOOSE)、取樣值(sampled value, SV)及精密時間協定(precision time protocol, PTP)之安全參數。

本標準亦定義特定狀況之安全事件，其可識別可能要求錯誤處理之事宜。然而，組織回應此等錯誤情況之運作超出本標準範圍，而預期將由組織的安全政策定義。

未來，隨著公開金鑰密碼學因量子電腦之發展而受威脅，本標準亦將於一定程度上

考量後量子密碼學。注意，目前尚未提供特定措施。

2. 引用標準

下列標準因本標準所引用，成為本標準之一部分。有加註年分者，適用該年分之版次，不適用於其後之修訂版(包括補充增修)。無加註年分者，適用該最新版(包括補充增修)。

CNS 62351-2	電力系統管理及關聯資訊交換 - 資料及通訊安全 - 第 2 部： 詞彙
CNS 62351-4	電力系統管理及關聯資訊交換 - 資料及通訊安全 - 第 4 部： 包括 MMS 及衍生之剖繪
CNS 62351-5	電力系統管理及關聯資訊交換 - 資料及通訊安全 - 第 5 部： IEC 60870-5 及其衍生協定之安全
CNS 62351-6	電力系統管理及結合資訊交換 - 資料及通訊安全 - 第 6 部： CNS 61850 系列標準之安全性
IEC 62351-3:2023	Power systems management and associated information exchange – Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP
IEC 62351-14 ⁽¹⁾	Power systems management and associated information exchange – Data and communications security – Part 14: Cyber security event logging
註 ⁽¹⁾ 起草中。	
ISO/IEC 9594-8:2020	Rec. ITU-T X.509 (2019), Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks
ISO/IEC 9594-11:2020	Rec. ITU-T X.510 (2020), Information technology – Open systems interconnection – The Directory: Protocol specifications for secure operations
ISO/IEC 9834-1:2012	Rec. ITU-T X.660 (2011), Information technology – Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree
IETF RFC 5272	Certificate Management over CMS (CMC)

IETF RFC 5755	An Internet Attribute Certificate Profile for Authorization
IETF RFC 5934	Trust Anchor Management Protocol (TAMP)
IETF RFC 6407	The Group Domain of Interpretation
IETF RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
IETF RFC 7030	Enrolment over Secure Transport
IETF RFC 8052	Group Domain of Interpretation (GDOI) Protocol Support for IEC 62351 Security
IETF RFC 8263	Group Domain of Interpretation (GDOI) GROUPKEY-PUSH Acknowledgement Message
IETF RFC 8894	Simple Certificate Enrolment Protocol

3. 用語定義及縮寫

3.1 用語及定義

下列用語及定義適用於本標準。

3.1.1 非對稱金鑰 (asymmetric key)

2 個相關金鑰 (公開金鑰及私密金鑰)，用以執行互補運作 (complementary operation)，諸如加密與解密或簽章產生與簽章查證 (verification)。

3.1.2 授權及驗核清單 (authorization and validation list, AVL)

經簽署之清單，包含對 AVL 個體之資訊，關於可能的通訊個體，以及對與此等個體通訊的可能限制。

[來源：ISO/IEC 9594-8:2020 之 3.5.9]

3.1.3 授權及驗核清單個體 (authorization and validation list entity)，AVL 個體

當扮演依賴方時，依指定之授權者所核發之 AVL 的個體。

[來源：ISO/IEC 9594-8:2020 之 3.5.10]

3.1.4 授權者 (authorizer)

受作為 AVL 個體運作之 1 或多個個體信任的個體，以建立、維護及簽署授權及驗核清單。

[來源：ISO/IEC 9594-8:2020 之 3.5.11]

3.1.5 憑證路徑 (certification path)

1 或多個公開金鑰憑證之有序清單，起始於由信任錨所簽署的公開金鑰憑證，而

結束於待驗核之終端個體公開金鑰憑證。

備考：所有中間公開金鑰憑證(若有)係 CA 憑證，其中前一公開金鑰憑證之主體係後隨公開金鑰憑證的核發者。

[來源：ISO/IEC 9594-8:2020 之 3.5.21]

3.1.6 憑證請求(certification request)

當要求新公開金鑰憑證或公開金鑰憑證之更新(renewal)時發出的請求。

[來源：IETF RFC 2986]

3.1.7 控制權(controllership)

對裝置或系統之合法所有權(legal ownership)、實體控制與邏輯控制的交集，其中裝置或系統之所有權與控制間的任何契約協議之性質於全景中並不重要。

3.1.8 密碼繫結(cryptographic binding)

CKMS 使用 1 或多種加密技術，以於金鑰與所選定詮釋資料元件間，建立受信任關聯關係。

[來源：NIST SP 800-130]

3.1.9 資料集(dataset)

資料之彙集。

3.1.10 裝置(device)

實作特定功能之組件，其可扮演客戶端(例：TLS 客戶端)或伺服器(例：GDOI 之金鑰配送中心)。

3.1.11 數位簽章(digital signature)

資料密碼式轉換之結果，當正確實作時，提供用以查證來源鑑別性、資料完整性，以及簽署者(signatory)不可否認性的機制。

[來源：FIPS 186]

3.1.12 終端個體(end entity)

已指派終端個體公開金鑰憑證之個體，其中私密金鑰無法用以簽署其他公開金鑰憑證，但可用於其他目的之簽署。

3.1.13 個體(entity)

涵蓋人類使用者、自動化系統、軟體應用程式、通訊節點、場域裝置及其他型式資產之通用用語。

3.1.14 特徵(fingerprint)

用以鑑別公開金鑰或其他資料之雜湊結果(“金鑰特徵”)。

[來源：IETF RFC 4949]

3.1.15 群組控制器/金鑰伺服器(group controller/key server, GCKS)

定義群組政策並針對該政策配送金鑰之裝置。

[來源：IETF RFC 3740]

3.1.16 解譯之群組領域(group domain of interpretation, GDOI)

管理群組安全關聯關係之領域，其係由IPsec及可能的其他資料安全協定使用。

備考：此等安全關聯關係保護 1 或多個金鑰加密金鑰(key-encrypting key, KEK)、

訊務加密金鑰(traffic-encrypting key, TEK) 或由群組成員共享之資料。

GDOI 使用群組控制器之概念，其係用以支援群組成員間安全關聯關係的建立。

[來源：IETF RFC 6407]

3.1.17 群組成員(group member, GM)

安全群組之經授權成員，發送及/或接收與該群組相關的IP封包。

3.1.18 雜湊函數(hash function)

將任意大小之資料對映至稱為摘要(digest)的固定大小資料之(數學)函數。

3.1.19 雜湊訊息鑑別碼(hash message authentication code, HMAC)

用於以對稱金鑰鑑別及資料完整性之密碼式代碼。

[來源：IETF RFC 2104]

3.1.20 金鑰配送中心(key distribution centre, KDC)

於本標準全景中提供網路服務之中心，於成功鑑別後對同級之預定義組提供臨時(對稱)會期金鑰(session key)。

備考：此亦稱為群組控制器/金鑰伺服器(group controller/key server, GCKS) (參

照 GDOI)。

3.1.21 金鑰管理系統(key management system)

用以管理(例：產生、配送、儲存、備份、歸檔、復原、使用、撤銷及銷毀)密碼金鑰及其詮釋資料之系統。

3.1.22 訊息鑑別碼(message authentication code, MAC)

對資料之密碼式核對和，其使用對稱金鑰偵測資料的非蓄意及蓄意修改。

[資料來源：SP 800-63；FIPS 201]

3.1.23 物件識別符(object identifier)

由國際物件識別符樹之根至節點的基元整數值之有序清單，其明確識別該節點。

[來源：ISO/IEC 9834-1:2012之3.5.11]

3.1.24 線上憑證狀態協定(online certificate status protocol, OCSP)

使應用程式能判定所識別憑證之(撤銷)狀態的協定。

備考：OCSP可用以滿足提供較CRL更及時之撤銷資訊的某些運作要求事項，並可能用以獲得額外狀態資訊。OCSP 客戶端對 OCSP 回應者發出狀態請求，並暫停接受相關憑證，直至回應者提供回應。

[來源：IETF RFC 6960]

3.1.25 運作者(operator)

通常負責受控制設備之正確運作的特定型式使用者。

3.1.26 預先共享金鑰(pre-shared key, PSK)

2 個個體(諸如軟體應用程式或裝置)間預先共享之秘密，使得能鑑別其自身或建立安全連接。

3.1.27 私密金鑰(private key)

(於公開金鑰密碼系統中)僅由該個體知悉之個體金鑰對中的金鑰。

[來源：ISO/IEC 9594-8:2020之3.5.50]

3.1.28 公開金鑰憑證(public-key certificate)

個體之公開金鑰連同某些其他資訊，藉由以核發該憑證的 CA 之私密金鑰進行數位簽章，變得不可偽造。

備考：公開金鑰憑證通常稱為 X.509 憑證或數位憑證。然而，此等用語並不明確，因其可能指亦由 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019) 所定義之屬性憑證。

[來源：修改自 ISO/IEC 9594-8:2020 之 3.5.58。]

3.1.29 公開金鑰密碼標準(public-key cryptography standards, PKCS)

RSA 實驗室與全球安全系統開發人員合作制定之規格，旨在加速公開金鑰加密技術的部署。

[資料來源：www.rsa.com]

3.1.30 隨機數產生(random number generation, RNG)

用以產生一系列不可預測之數字的過程。

備考：若整個母體中之各值具相同受選擇機率，則各個別值稱為隨機。

[來源：NIST SP 800-57]

3.1.31 註冊機構(registration authority, RA)

與將由憑證機構(certification authority, CA)核發之公開金鑰憑證的主體之識別及鑑別相關之憑證機構責任的該等層面。

備考1. RA 可為獨立個體或憑證機構之整合部分。

備考2. 此定義與 Rec. ITU-T X.660 | ISO/IEC 9834-1 中所定義之範圍不同。

[來源：ISO/IEC 9594-8:2020 之 3.5.61]

3.1.32 依賴方(relying party)

依賴公開金鑰憑證中之資料做出決定的個體。

[來源：ISO/IEC 9594-8:2020 之 3.5.62]

3.1.33 安全關聯(security association, SA)

於2或多個個體間建立之關係，以使其能保護其交換的資料。

[資料來源：NIST IR 7298 Rev.1]

3.1.34 安全強度(security strength)

安全技術之能力，使潛在攻擊者繞過或破壞成為不可行。

備考：此通常以安全位元數目衡量。

[來源：NIST SP 800-130]

3.1.35 會期金鑰(session key)

於對稱加密之全景中，臨時或使用時間相對短的金鑰。

[來源：IETF RFC 2828]

3.1.36 對稱金鑰(symmetric key)

密碼金鑰，用以執行密碼運算及其逆運算（例：加密及解密），或用以建立訊息鑑別碼及查證該碼。

[來源：NIST SP 800-63]

3.1.37 信任(trust)

對資訊之可靠度及真實性，或對個體於特定環境下採取適切行動的能力及傾向之堅定信念。

3.1.38 信任錨(trust anchor)

受依賴方信任，並用以驗核憑證路徑中之公開金鑰憑證的個體。

[來源：ISO/IEC 9594-8:2020之3.5.72]

3.1.39 信任錨資訊(trust anchor information)

至少包括：信任錨之區別名稱、相關聯的公開金鑰、演算法識別符、公開金鑰參數(若適用)，以及關於其使用之所有限制事項(constraint)，包括效期。

備考：信任錨資訊可提供作為自我簽署CA憑證或作為正常CA憑證[亦即跨域憑證(cross-certificate)]。

[來源：ISO/IEC 9594-8:2020之3.5.73]

3.1.40 信任錨儲存處(trust anchor store)

於1或多個信任錨用之依賴方處的信任錨點資訊彙集。

[來源：ISO/IEC 9594-8：2020之3.5.74]

3.2 縮寫

額外縮寫於 CNS 62351-2 中提供。

AA	屬性機構(attribute authority)
AEAD	具相關聯資料之經鑑別加密(authenticated encryption with associated data)
ASN.1	抽象語法記法(一)(abstract syntax notation one)
AVL	授權及驗核清單(authorization and validation list)
AVMP	授權及驗核管理協定(authorization and validation management protocol)
BRSKI	遠端安全金鑰基礎建設之啟動(bootstrapping of remote secure key infrastructure)
CA	憑證機構(certification authority)
CASP	憑證機構訂用協定(certification authority subscription protocol)
CIA	機密性、完整性及可用性(confidentiality, integrity, and availability)
CMC	經由 CMS 之憑證管理(certificate management over CMS)
CMS	密碼訊息語法(cryptographic message syntax)
CPS	憑證實務聲明(certificate practice statement)
CSR	憑證簽署請求(certificate signing request) · 亦於憑證請求之全景提及。
DER	區別編碼規則(distinguished encoding rule)
DOI	關注之領域(domain of interest)
DSA	數位簽章演算法(digital signature algorithm)
ECDSA	橢圓曲線數位簽章演算法(elliptic curve digital signature algorithm)
EdDSA	Edwards 曲線數位簽章演算法(Edwards-curve digital signature algorithm)
EST	經由安全傳送登錄(enrolment over secure transport)
FQDN	完整網域名稱(fully qualified domain name)
GCKS	群組控制者/金鑰伺服器(group controller/key server)
GA	群組相關聯之政策(group associated policy)

GCM	Galois 計數器 模式(Galois counter mode)
GDOI	解譯之群組領域(group domain of interpretation)
GKDC	群組 KDC (group KDC)
GM	群組成員(group member)
GMAC	Galois 訊息鑑別碼(Galois message authentication code)
GOOSE	通用物件導向變電所事件(generic object-oriented substation event)
HMAC	雜湊式訊息鑑別碼(hash-based message authentication code)
HTTP	超文字傳送協定(hypertext transfer protocol)
ICV	整合性核對值(integrity check value)
IDevID	初始裝置識別符(initial device identifier) · IEEE 802.1AR。
IED	智慧電子裝置(intelligent electronic device)
ID	識別資訊(identity)
IKE	網際網路金鑰交換(Internet key exchange)
ISAKMP	網際網路安全關聯及金鑰管理協定(Internet security association and key management protocol)
KD	金鑰下載(key download)
KDC	金鑰配送(key distribution centre) · 又稱 GKDC。
KDF	金鑰衍生函數(key derivation function)
KEK	金鑰加密金鑰(key encryption key)
LDevID	本地顯著裝置識別符(locally significant device identifier) · IEEE 802.1AR。
MUD	製造者使用說明(manufacturer usage description) · RFC 8520。
OCSP	線上憑證狀態協定(online certificate status protocol)
OTP	單次通行碼(one time password)
PDU	協定資料單元(protocol data unit)
PEM	增強隱私之電子郵件(privacy-enhanced electronic mail)
PKCS	公開金鑰加密標準(public-key cryptography standard)

PKI	公開金鑰基礎建設(public-key infrastructure)
RA	註冊機構(registration authority)
RNG	隨機數產生(random number generation)
RSA	Rivest Shamir Adleman，公開金鑰密碼系統。
SA	安全關聯(security association)
SCEP	簡單憑證登錄協定(simple certificate enrolment protocol)
SPI	安全參數值(security parameter index)
SV	取樣值(sampled value)
TAMP	信任錨管理協定(trust anchor management protocol)
TEK	訊務加密金鑰(traffic encryption key)

4. 適用於電力系統之安全概念

4.1 一般

本節旨在簡介適用於電力系統之密碼概念。其提供關於電力系統中安全目標之概觀、可利用哪些密碼演算法符合此等安全目標，以及如何將其套用於不同的部署環境。此外，本節與附錄 B 一起提供關於所使用之密碼演算法，以及不同環境中可能邊界條件的某些背景資訊。本標準之規定性部分將規定其應用。亦闡明安全事件之一般處理。

4.2 安全目標

4.2.1 機密性

需機密性以防止敏感資料遭存取，尤其當其係於傳輸時。

電力系統實作中資料機密性之密碼式目標，通常係藉由使用對稱金鑰加密技術加密訊息完成。訊息可能於應用層處、於其下通訊通道或於二者加密。如前所述，此訊息之機密性係取決於維護對稱金鑰機密性的發送者及接收者。此外，非對稱加密通常係用以交換或協商於規定時間長度內有效之對稱會期金鑰，從而降低與保持特定會期金鑰秘密相關聯的風險。

為限制對稱金鑰遭破解時之損害，建議於連接或關聯上所使用的對稱金鑰係屬唯

一。此能藉由使用 B.8 中所述之臨時金鑰協商達成。針對傳送層安全(transport layer security, TLS)，此能藉由選擇適切密碼套組(cipher suite)完成(依本系列標準第 3 部之概述)。

4.2.2 資料完整性

資料完整性考量偵測於傳輸期間或靜止時未經授權的資料變更。其使完整性核對值之查證者能偵測出相關資料的任何完整性違反。

有 2 種方法用於偵測資料完整性違反。2 種方法皆使用密碼式雜湊函數，偵測所接收之資料中的任何變更。依 B.5 中之討論，雜湊函數對整個某些輸入資料產生固定長度之摘要。即使待雜湊之資料僅發生微小變化，此摘要將不可預測的變更。用於偵測完整性違反之 2 種方法為：

- (a) 使用 B.3.6 中所討論之數位簽章。
- (b) 使用完整性核對值(integrity check value, ICV)，如 B.6 中所討論。

經鑑別加密係屬進一步變異，其於單一運作中提供資料機密性及資料完整性。其描述於 B.7 中。

4.2.3 鑑別

當個體接收源自其他個體之資料時，安全的鑑別該資料的發送者係屬關鍵。本標準識別與 4.2.2 中所提及資料完整性相同之 2 種鑑別方法：

- (a) 使用數位簽章，經查證之數位簽章具相當的確定性，證明發送者擁有與用以查證數位簽章的公開金鑰對應之私密金鑰。此將於 B.3.6 中進一步討論。
- (b) 使用完整性核對值(ICV)，其中經查證之 ICV 於一定程度上證明發送者擁有相同於接收者之對稱金鑰。用以產生 ICV 之對稱金鑰係作為鑑別過程一部分所建立，因此與該鑑別繫結。ICV 係於 B.6 中進一步討論。

4.2.4 不可否認性

不可否認性係指將動作(例：命令或訊息)無可辯駁的繫結至核發個體之能力。其可將發送者繫結至發送特定訊息之動作，或將接收者繫結至接收特定訊息的動作。

CNS 13888 系列標準規定不同程度之不可否認性，並規定 2 種如何建立不可否認性的不同方式：

- (a) CNS 13888-2 規定使用對稱金鑰加密之程序。此等技術要求受信任第三方的參與。
- (b) ISO/IEC 13888-3 規定使用非對稱金鑰加密之程序。

4.3 密碼演算法及概念

本標準之適用範圍為電力系統應用之金鑰管理，包括 PKI 式非對稱建鑰資料管理，以及群組式對稱金鑰管理。金鑰管理係適用於本系列標準各部，其利用密碼金鑰材料以保護電力系統自動化協定中所交換之資訊。

附錄 B 詳述不同型式加密演算法及相關概念之解釋，諸如信任、信任錨、安全等級、隨機數產生，以及從 1 種密碼演算法到另一(通常更強)密碼演算法的移轉。後者對因應量子計算之先進變得更加重要，此特別危及非對稱密碼演算法。

除對密碼演算法進行一般性簡介外，於一定延伸考量下列型式之演算法：

- 包含 RSA、ECDSA 及 EdDSA 演算法之非對稱演算法，包括不同型式非對稱演算法的一般說明、金鑰產生及安全考量事項(considerations)。
- 不同運作模式下之對稱金鑰演算法。僅考量依先進加密標準(advance encryption standard, AES)的演算法。所考量之運作模式係加密區塊鏈接(cipher block chaining)(AES-CBC)，以及同時依計數器機制的模式(AES-CTR)。其係同時針對 128 及 256 位元金鑰大小所定義。
- 雜湊演算法。所考量演算法係所謂安全雜湊演算法(secure hash algorithm) (SHA)，且僅考量 SHA-256 及 SHA-512。該說明包括使用雜湊演算法之區域清單。
- 建立完整性核對值(ICV)之演算法。有 2 種型式之 ICV 演算法與本標準相關。第 1 種型式為金鑰雜湊訊息鑑別碼(keyed-hash message authentication code, HMAC)演算法，其規定對稱金鑰及雜湊演算法之使用。包括 2 種 HMAC 演算法，其一係依 SHA-256，另一種則依 SHA-512。其他型式之 ICV 演算法係 AES - Galois 訊息鑑別碼(AES-GMAC)。
- 具關聯資料之鑑別加密(authenticated encryption with associated data, AEAD)演

算法(諸如 AES-GCM 或 AES-CCM)係屬密碼演算法，除規定加密/解密外，亦針對加密資料及某些相關聯資料提供完整性功能。包括 2 種型式之 AEAD 演算法。二者皆基於 AES 加密，但使用不同技術產生 ICV 部分。二者皆提供 128 位元及 256 位元之 AES 金鑰大小。

- 使用 Diffie Hellman 之金鑰協議依非共享私密金鑰計算共享金鑰。針對金鑰管理，立即產生對稱金鑰至關重要，而 Diffie-Hellman 方法係針對此目的之常用技術。使用 2 種不同型式之數學(質數域及橢圓曲線)提供 2 種型式的 Diffie-Hellman 方案。二者皆以支援移植至更安全者之方式定義

因此等演算法及概念套用於電力系統中，故附錄 B 提供概觀、背景資訊及對更多資訊之參考處。此附錄旨在作為簡介材料，以更佳理解此等演算法於本標準後續規定性節次中之應用。

5. 金鑰建立及管理技術

5.1 一般

本節提供針對對稱及非對稱建鑰資料管理、連接之概念及必要的基礎建設，提供關於技術的概觀。針對對稱建鑰資料，焦點係置於群組式金鑰之管理。本節針對後續各節之規定性說明建構背景。

5.2 金鑰管理生命週期

5.2.1 裝置生命週期中之金鑰管理

金鑰管理係裝置生命週期之一部分，通常依循圖 1 中所示的流程。

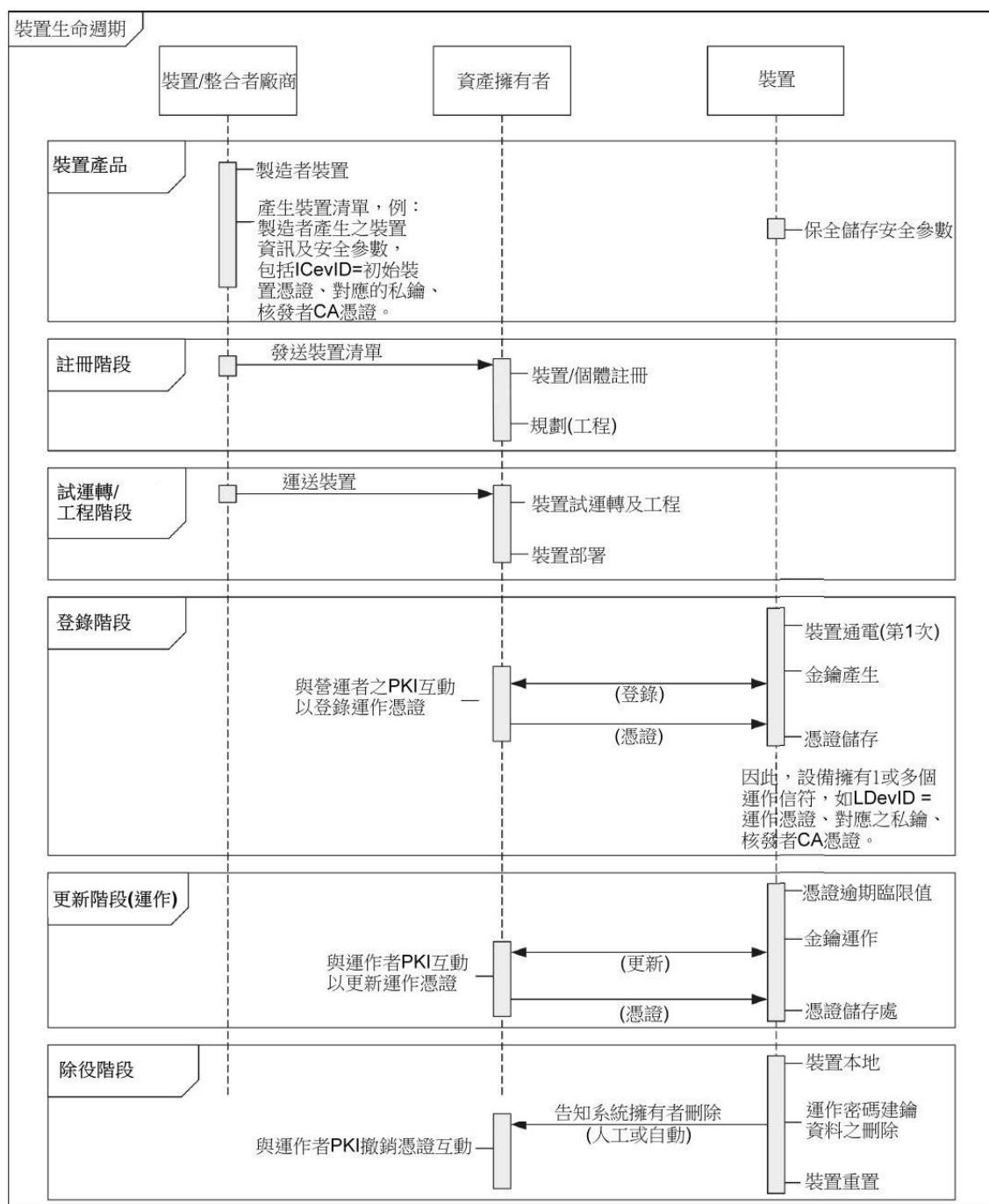


圖 1 個體生命週期中之金鑰管理概觀

製造者能藉由提供識別資訊之安全清單，用以支援個體的金鑰管理生命週期，諸如製造者唯一識別符、單次通行碼(one-time-password)、源自製造者CA之憑證或用於其各裝置及系統的製造者個體憑證。IEEE 802.1AR 將信符(credential)之此等初始集合定義為IDevID(初始裝置識別符)，由初始憑證、對應之私密金鑰及直至信任錨的憑證鏈組成。

每次所有權甚至狀態變更(例：倉儲相對於部署)時，宜登錄新憑證，提供使用中之產品識別資訊的受信任鏈。當此等個體最終被設計並部署時，其製造者憑證(若可用)可能用以於運作中登錄個體，從而獲得 1 或多個運作憑證(LDevID、本地裝置識別符)，此使其能鑑別並開始其資訊交換。於此等運作憑證即將逾期前，宜更新其以避免憑證查證錯誤。

此外，待考量者為裝置除役，其宜與任何運作密碼信符之刪除一起進行，以確保一旦裝置停止運作，此等資訊將不遭濫用。需注意，通常不刪除 IDevID (若可用)。

鼓勵製造者將用以安全的擦除裝置上任何運作信符(憑證、信任錨資料庫等)，並復原預設初始信符集之過程，簡化為簡單過程；或若必定複雜，則至少清楚的登載。此將有助於良好服務結束清理，且於適切情況下，確保任何工場/工作台測試信符於部署前已刪除。作為生命週期一部分，系統擁有者參與除役過程(參照 5.2.2)。

5.2.2 密碼金鑰之生命週期

一般而言，密碼金鑰及憑證特定的依循生命週期。其係建立、配送、安裝、適用、更新及銷毀，以滿足金鑰管理安全政策之要求事項。例：圖 2 描繪 PKI 式系統中金鑰之典型生命週期。ISO/IEC 11770 (參照 [6] ⁽²⁾)及 NIST SP 800-130 [11]中更詳細的討論一般金鑰生命週期管理。此處以抽象層級描述通常受管理之憑證的生命週期。有關憑證管理之更多細節，參照 5.8。

註⁽²⁾ 方括符中之數字參引參考資料。

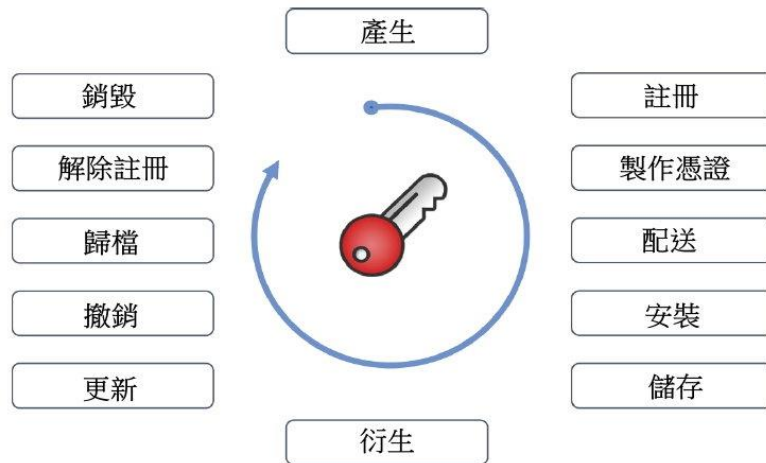


圖 2 密碼金鑰生命週期

以下簡述密碼金鑰生命週期中各個可能之階段。非對稱金鑰要求所有階段，而對稱金鑰則不要求註冊、製作憑證、解除註冊及撤銷：

- 產生(generation)：若個體具適切能力，則可由自身建立密碼金鑰。或者，金鑰可於外部建立並安裝於標的個體上。若個體無法支援產生金鑰的關鍵組件之一，則須確保高度隨機性的隨機數產生器(RNG) (參照 B.12)，通常使用後一種作法。若須歸檔金鑰(例：供所儲存資料用之加密金鑰)，則可能仍需外部建立金鑰。當憑證即將逾期時，個體需申請憑證更新。
- 註冊(registration)：若使用憑證及 PKI 過程，則透過註冊機構(RA)註冊即可建立個體之“識別資訊”。此係藉由於個體本地或集中產生金鑰對所完成。該個體提供憑證請求予 RA，然後 RA 與憑證機構(CA)一起進一步處理。
- 製作憑證(certification)：RA 註冊個體後，CA 將簽署之憑證數位化的提供予個體，從而將其公開金鑰與該個體持有之私密金鑰連結。依金鑰產生，此能為信任中心中金鑰產生之一部分，或可使用於鑑別請求中所發送的資訊完成。。
- 配送(distribution)：金鑰配送包含以安全方式將金鑰及金鑰管理資訊傳送予經授權個體之過程。私密金鑰雖理想的於端末裝置中產生，因此無須配送，但若係外部產生，則須使用保全方式配送。公開金鑰憑證中之公開金鑰可使用非保全方式配送，因端末裝置可藉由查證憑證簽章直接查證其真確性。
- 安裝(installation)：金鑰可於製造及/或工程過程期間安裝於個體中(預先共享共

享金鑰)，亦可稍後經由線上程式安裝。後一過程可能要求與安全伺服器通訊，使用分離之通訊通道進行帶外通訊，或作為服務通訊的一部分帶內通訊。

- 儲存(storage)：建議將私密金鑰/對稱金鑰安全的儲存於個體中。安全之金鑰儲存體宜遵循 FIPS 140-3 [70]或 ISO/IEC 19790 [71]。
- 衍生(derivation)：用作會期金鑰或其他短期金鑰之密碼金鑰，可自儲存於個體中的私密金鑰或對稱金鑰衍生。
- 更新(update)：金鑰需定期更新。加密金鑰具專屬生命期，例：核發予使用者之公開金鑰憑證的有效期可能為 2 年，而核發予伺服器之公開金鑰憑證有效期可能為 1 年或更短，預先共享金鑰的有效期為數週或數月，會期金鑰之效期為數小時及/或數千個封包。密碼金鑰之生命期建議，參照 NIST SP 800-57 Part 1[73]及德國 BSI TR 02102-1 [58]。
- 撤銷(revocation)：當憑證不再被授權使用時，可發生憑證撤銷。若裝置遭取消服務或變更其角色，或私密金鑰遭破解或懷疑遭破解，則可能發生該情況。
- 歸檔(Archiving)：解密長期儲存之資料所需的對稱金鑰，宜歸檔於安全機密儲存體中，以啟用資料復原(以容許稍後存取儲存的加密資料)。此外，為支援進一步簽章查證，公開金鑰憑證亦宜歸檔，儘管無需安全機密儲存體。
- 解除註冊(de-Registration)：此程序通常由註冊機構提供，用以刪除個體與專屬金鑰之關聯。其通常用於金鑰銷毀階段。
- 銷毀(destruction)：當密碼金鑰遭銷毀時，其須無法復原或使用。此發生於密碼金鑰生命週期結束時。

5.3 密碼金鑰使用

密碼金鑰係用於不同目的及產品生命週期之不同階段，且套用為：

- 公開金鑰憑證及對應之私密金鑰：用以識別、鑑別並授權個體。此外，其經常用於會期金鑰之協商或建立。
- 預先共享金鑰(例：用於即時通訊)：用作個體間之共享秘密，以確保其間的資料交換(完整性、機密性)。此於未支援 PKI 之環境中可能有用。此外，此方案可於 PKI 登錄期間使用，容許個體相對於憑證機構(certification authority, CA)

自我鑑別，例：於處理製作憑證請求時。需注意，預先共享金鑰之安全與其複雜度有關。密碼複雜度規則通常由組織安全政策所賦予。

- 會期金鑰(成對或群組式)：用以於通訊訊息上有效加密或完整性核對。
- 會談參數(專屬密碼演算法)：用以支援會談(金鑰、生命期等)。
- 加密存取符記：主要用於將資源授權/存取傳送/提供予個體。
- 其他相關個體或組織信符。

5.4 金鑰管理系統安全政策

密碼金鑰需受保護。因此，每一組織(或預期交換資料之組織群組)，宜針對其金鑰管理系統制定安全政策，其建立並規定保護組織使用的所有密碼金鑰及其相關詮釋資料之機密性、完整性、可用性，以及來源鑑別的所有要求事項。此等保護要求事項宜涵蓋金鑰之整個生命週期，包括當其係最初提供、運作、儲存及運輸時。金鑰管理安全政策亦宜包括於整個組織系統中使用之所有加密機制及協定的選擇。金鑰管理系統亦需安全管理支援，以確保遵循安全政策並維護程序。此支援之規格超出本標準適用圍，但可參照諸如 ISO/IEC 11770 ([6])或 NIST SP 800-130 ([11])或 IEC 62443- 4-2 [74]。

5.5 電力系統運作之金鑰管理設計原則

密碼金鑰係用以保護不同系統個體間之通訊，諸如使用者、系統、軟體應用、通訊節點及可能的大量設備及裝置，其通常位於遠端且不受信任的站點，且越來越多地由不同組織所擁有/營運。

宜管理此等密碼金鑰，使得能有效且安全地將其提供予要求安全資料交換之個體。此金鑰管理需考量許多議題，自個體之能力至此等個體的不同型式位置，至提供及撤銷金鑰的時序，至個體之不同所有權，至可能的不同監理管轄區，以及保護金鑰管理過程自身免遭攻擊。

例如，許多較小裝置於運算能力及儲存容量受限制，而通訊網路之可用頻寬亦可能受限制。因此，於系統強大及通訊頻寬高之傳統企業資訊技術屬系統環境中使用的某些金鑰管理技術，較不適合電力系統自動化及通訊環境。

作為另一示例，於預期交換運作資料之組織群組中，某些組織可能不具於無第三

方支援的情況下管理密碼金鑰之專業知識或人員。因此，此等現實情況宜納入金鑰管理過程之設計。

為因應此等限制事項，本標準規定可用於不同要求事項及限制事項之不同金鑰管理技術。具體而言，其規定如何管理本系列標準其他部中所規定之各加密功能的金鑰。金鑰管理設計原則之指引來源包括：

- 參考資料[6]：ISO/IEC 11770-1:2010 Information technology – Security techniques – Key management – Part 1: Framework。
- 參考資料[8]：ISO/IEC 11770-3:2008 Information technology – Security techniques – Key management – Part 3: Mechanisms Using Asymmetric Techniques。
- 參考資料[13]：NIST 800-57, Part 1。

5.6 對稱金鑰之建立

5.6.1 概觀

要求對稱密碼金鑰之原因有二：

- (a)其係用以傳送過程中資料之加密及解密。
- (b)其係用於 ICV 之產生及查證。

出於安全原因，用於成對通訊之金鑰，預期於任意 2 對通訊個體間將不相同。2 個體間之對稱金鑰可以不同方式建立：

- (a)藉助本系列標準其他部所定義之方式，特別是：

- 本系列標準第 3 部用於 TLS，藉由剖繪 TLS 選項。此處，於 2 個體間之 TLS 交握期間，使用依公開金鑰演算法的技術建立成對金鑰。
- 本系列標準第 4 部用於應用層端對端安全剖繪。針對 TLS，依公開金鑰演算法於 2 個通訊個體間建立成對金鑰。
- 本系列標準第 5 部用於 IEC 60870-5-101/104 及 IEEE 1815 (DNP3)之應用層安全機制，亦依賴公開金鑰演算法的應用。

- (b)使用金鑰協議建立成對金鑰，依 Diffie-Hellman 金鑰協議方法(5.6.2)所述。

- (c)藉由使用金鑰衍生函數(key derivation function, KDF)方法(5.6.3)，例：依既有

對稱金鑰。

(d)藉由使用金鑰配送，例：使用某些 TLS 密碼套組中使用的公開金鑰加密。

依循(a)至(d)之 2 個體間所建立的對稱金鑰，通常不直接適用於保護通訊，而是用以衍生安全服務特定金鑰。於 CNS 62351-4 之示例中，有不同的對稱金鑰可用於完整性保護及機密性保護。此外，此等金鑰係屬方向相依，導致 2 個通訊個體間存在多個金鑰。此等金鑰亦具生命期，要求以安全方式建立初始對稱金鑰，並於通訊連接之整個生命期中對其管理。如上述項目符號清單中所概述，對稱金鑰之建立通常由其他方法支援，以限制管理通訊個體間的純對稱金鑰之額外負擔。能考量用以收容依賴多播通訊之網路個體的 1 種方法為群組式金鑰管理。特別是，群組式金鑰可用於電力自動化系統中。為此，採用群組式金鑰管理協定，其包括用以管理群組中經鑑別成員之金鑰及相關聯政策的金鑰管理組件。群組金鑰管理描述於 5.6.4 中。

5.6.2 Diffie-Hellman 金鑰協議方法

Diffie-Hellman 金鑰協議方法容許須交換所謂之 Diffie-Hellman 公開金鑰的雙方，以不容許竊聽者瞭解此共享秘密的方式共同達到共享秘密。

關於經典曲線之橢圓曲線 Diffie Hellman 的 Diffie Hellman 金鑰協議之細節，參照 B.8。

5.6.3 金鑰衍生函數(KDF)方法

金鑰衍生函數(KDF)係屬密碼演算法，其自使用擬隨機函數自秘密值(諸如另一對稱金鑰、密碼或密碼短語)衍生 1 或多個對稱金鑰。B.9 中提供有關 KDF 之細節。

5.6.4 群組金鑰管理

5.6.4.1 群組金鑰之目的

針對形成具嚴格效能要求事項之群組個體間的多播互動，群組金鑰之應用較該群組中具分離同級關係更有效。此外，於此情況下，金鑰管理可能於適用金鑰之實際協定的全景外部執行。群組金鑰管理通常使用非對稱與對稱加密技術之組合。非對稱部分係用以識別及鑑別個體，而對稱部分則保護實際金鑰及政策傳送。為實現群組式金鑰之設置，通常將 1 個系統或裝置指定為群組控制器，其轉而經

由其他個體的憑證或預先共享共享金鑰鑑別其他個體。成功鑑別個體後，群組控制器將實際之群組金鑰配送予該等個體。因此，群組控制器類似於金鑰配送(key distribution centre, KDC)之功能(參照圖 3)。

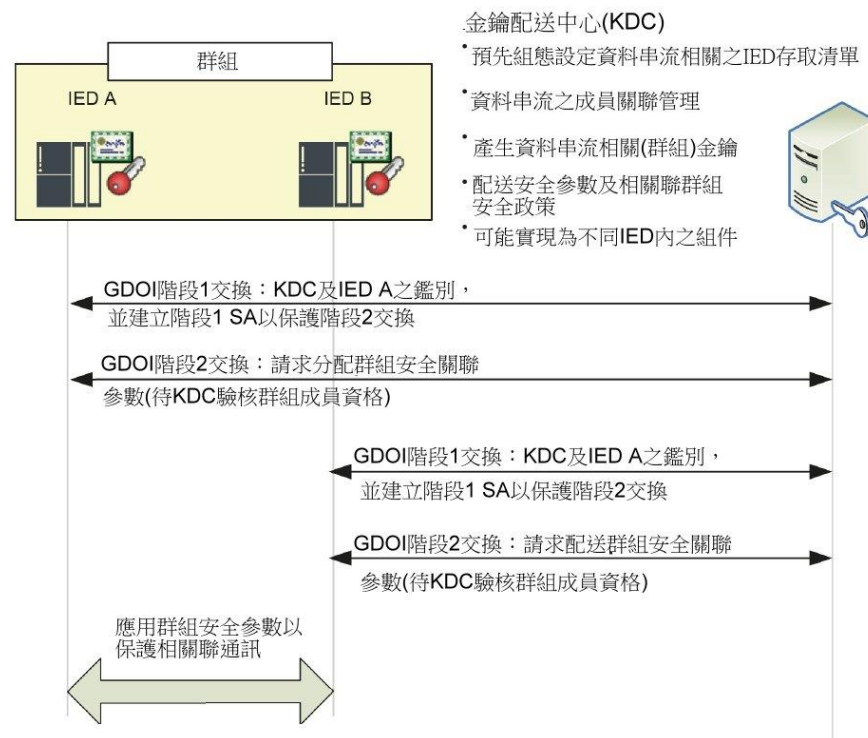


圖 3 GDOI 示例上群組金鑰管理之概觀

圖 3 顯示智慧電子裝置(IED)用以訂用資料串流安全參數。資料串流與通訊群組相關聯。需注意，群組控制器可能為分離之個體或部署於任何 IED 內。亦需注意，所示版本使用憑證式鑑別，並採用數位簽章。

存在用以配送群組金鑰之多種不同協定。然而，解譯之群組領域(group domain of interpretation, GDOI)經選擇為最適切電力系統自動化的協定，並進行進一步描述於 5.6.4.2 中。

5.6.4.2 解譯之群組領域(GDOI)

5.6.4.2.1 一般

RFC 6407 中所定義解譯之群組領域(GDOI)支援將對稱群組金鑰(亦即訊務加密金鑰，TEK)，配送予所有預先組態設定或以其他方式登錄的個體(通常為裝置)。此方法須金鑰配送中心(KDC)，其負責依循 GDOI 過程將對稱會期金鑰集配送予已登錄之個體。此過程使用 KDC 與各群組成員(group member, GM)間之點對點

通訊，以配送對稱群組金鑰及相關聯安全政策。然後依所提供之安全政策適用群組金鑰自身，以保護群組內的後續通訊。

需注意，KDC 失效將中斷群組通訊，因此 KDC 備援勢在必行。然而，達成 KDC 備援之方法超出本標準適用範圍。

GDOI 規定為分 2 個階段進行，於後續節次中更詳細地描述。

5.6.4.2.2 GDOI 階段 1：網際網路金鑰交換(IKE)階段 1

GDOI 階段 1 安全關聯提供相互鑑別及授權。該結果係由協定參與者用以執行受安全 GDOI 階段 2 交換。GDOI RFC 合併(亦即使用但未重新定義)源自網際網路 DOI [RFC2407]、[RFC2409]之 IKEv1 階段 1 安全關聯定義，如圖 4 所示。自 KDC 至個體之對稱金鑰傳送，係於相互鑑別後啟始。

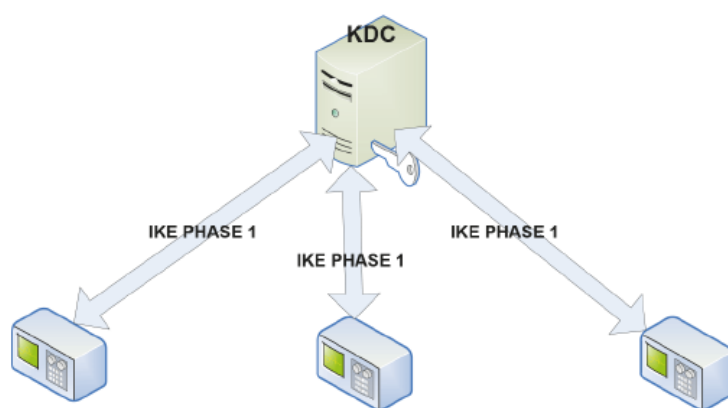


圖 4 GDOI IKE 階段 1 - 鑑別及保全通訊通道

備考：雖 RFC 2407、2408 及 2409 已由 RFC 4306 (以及隨後之 RFC 5996)作廢，但 GDOI 仍在使用的，因協定定義仍與 IKEv2 外的 ISAKMP 協定相關。

5.6.4.2.3 GDOI 階段 2：GDOI 對稱金鑰配送

5.6.4.2.3.1 一般

GDOI 過程(RFC 6407)中定義 2 種如何將金鑰自 KDC 傳送予個體之方法。第 1 種方法為 PULL 方法(由個體自 KDC 拉取金鑰)，第 2 種方法為 PUSH 方法(金鑰自 KDC 推播予個體)模型。GDOI 階段 2 交換受 GDOI 於階段 1 中所建立 SA 之保護。

備考：PUSH 方法要求可自 KDC 直接抵達群組成員。當設計系統架構時須遵守

此，因防火牆或 NAT 裝置可能阻礙此通訊。

GROUPKEY-PULL 交換或 GROUPKEY-PUSH 交換可用以將對稱金鑰配送予個體。要求 GDOI 支援 GROUPKEY-PULL，因其係唯一與階段 1 鑑別及授權結合使用之方法。此 2 種方法各有優點。GROUPKEY-PULL 提供透過訊務遞送之控制，而 GROUPKEY-PUSH 則容許及時撤銷或驅逐個體並提高效率。

GDOI 已延伸為支援 RFC 8052 中之 IEC 62351 安全服務。此等描述於 5.6.4.2.4 中。

5.6.4.2.3.2 GROUPKEY-PULL 註冊協定交換

GDOI 拉取(pull)方法如圖 5 所示。

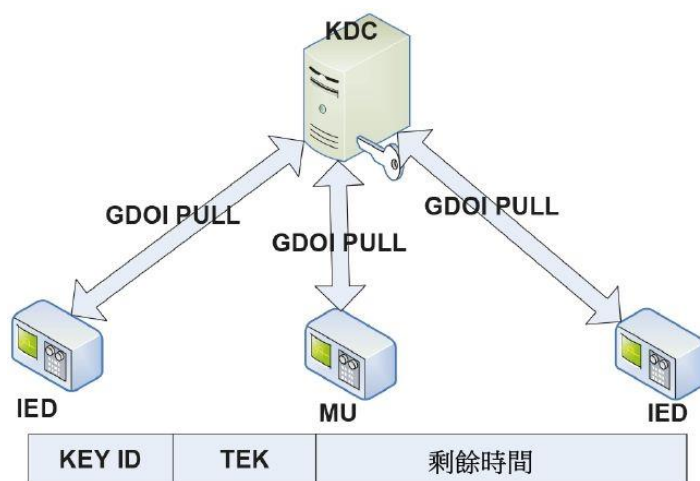


圖 5 GDOI 拉取階段 2

GDOI GROUPKEY-PULL 方法中具 2 個階段之通訊：

- GDOI 階段 1：2 個參與個體(群組成員及 KDC)之連接建立及鑑別，依 5.6.4.2.2 中所述。
- GDOI 階段 2：判定請求群組所使用之政策並下載金鑰：此係透過群組成員(GM)對 KDC 的 GDOI 識別酬載請求所完成。KDC 以所支援之政策(例：加密及簽章演算法)回應此請求。政策係使用 GDOI SA 回傳，其回傳 SA TEK 酬載。若 GM 未支援該等政策，則通訊宜中止。若 GM 能支援該等政策，則其發出確認，且 KDC 回覆金鑰下載(key download, KD)酬載。

5.6.4.2.3.3 GROUPKEY-PUSH 金鑰更新協定交換

KDC 政策可包括針對重新產生金鑰使用“推播(push)”方法，於該情況下，由 KDC 啟始(“推播”)之資料包將使用 IP 多播位址遞送予所有群組成員，或使用 IP 單播發送予特定 GM。GROUPKEY-PUSH 方法針對驅逐可能已遭損害且憑證可能遭撤銷之群組成員係屬有用。使用此方法，KDC 可對所有授權群組成員重新產生金鑰，同時排除遭驅逐之群組成員。

於使用 GROUPKEY-PUSH 之情況下，RFC 8263 定義源自群組成員的認可訊息之提供，以告知 KDC 有關推播資訊的接收。提供認可訊息之請求係由 KDC 於發送予群組成員的相關聯政策中指示。

5.6.4.2.4 IEC 62351 安全服務之 GDOI 協定支援

RFC 8052 “GDOI Protocol Support for IEC 62351 Security Services” 係為闡明 IEC 61850 電力公用事業自動化標準系列中 GDOI 使用所發展。其描述用以配送安全轉換之方法，其係換用以保護某些 IEC 61850 相關安全協定的訊息：訊息之保護係定義於本系列標準第 6 部、CNS 61850-8-1 及 CNS 15733-9-2 中。受保護之 IEC 61850 訊息通常包括訊息鑑別碼(MAC)之輸出，並可使用諸如先進加密標準(AES)的對稱密碼加密。

5.7 公開金鑰基礎建設(PKI)及權限管理基礎建設(PMI)所支援之信任

5.7.1 一般

本節提供於電力系統個體之整個生命週期中，用以管理憑證的 PKI 基礎建設(參照圖 6)。需注意，個體可為裝置、系統，亦可為電力系統中之人類使用者。

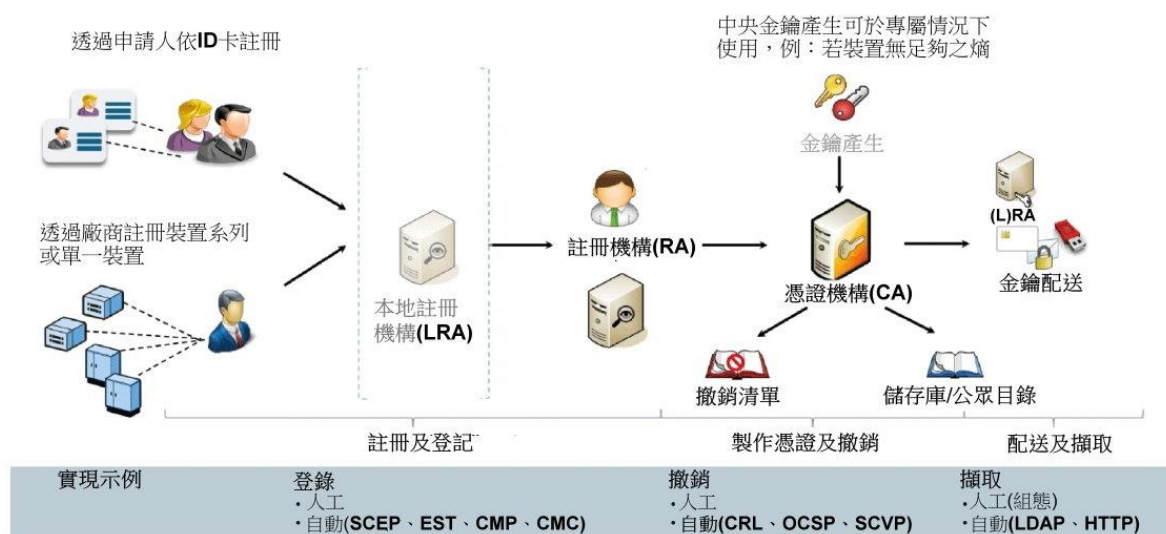


圖 6 PKI 基礎建設概觀及實現示例

5.7.2 至 5.7.6 描述註冊機構及憑證機構，以及作為受管理物件之憑證的一般功能。

5.7.2 註冊機構(RA)

於 PKI 式系統中，個體首先須透過註冊機構(RA)證明其識別資訊。就人類而言，RA 可透過出生證明、護照或其他官方文件判定個別身分(individual identity)。就系統及裝置而言，RA 可透過製造者核發之數位憑證或唯一的單次通行碼(OTP)以判定個體之識別資訊。RA 可為分離之個體，亦可是憑證機構(CA)一部分。

5.7.3 憑證機構(CA)

系統或裝置識別資訊建立後，需由憑證機構(CA)將其繫結至憑證。包含產生金鑰對之公開金鑰的 CSR，係由個體自身產生，或個體無法產生金鑰時由製造者產生，例：因遺失熵。CA 查證 CSR 並依納入 CSR 之資料核發數位憑證。透過憑證，CA 於個體之公開金鑰與公開金鑰憑證組件資料(亦即於公開金鑰及詮釋資料的組合上計算出 CA 數位簽章)間建立受信任之加密繫結。因此，此公開金鑰憑證將個體之識別資訊與其公開金鑰繫結，因此現有受信任之公開金鑰/私密金鑰群組合，其能由個體用以與其他個體交換資訊。因此，對個體金鑰之信任依賴於對 CA 金鑰有效性的信任(參照 5.7.4)。

CA 可由組織自身運作(容許封閉性、組織控制之通訊群組)，或由公眾所接受並

因而具更廣泛信任範圍的第三方(服務提供者、系統營運者或電網管理者)運作。

第三方 CA 要求安全方法，用以接受任何新個體之識別資訊，其範圍能由針對人員的親自驗核(in-person validation)至營運個體驗核，以及將先前經驗核之公開金鑰憑證鏈結至新公開金鑰憑證的安全鏈。

5.7.4 公開金鑰憑證

5.7.4.1 一般

公開金鑰憑證係屬數位文件，其以加密方式將個體識別資訊與該個體之公開金鑰繫結。公開金鑰具對應之私密金鑰。依 5.7.3 中所指出，此繫結係由核發 CA 之數位簽章所查證。除公開金鑰及公開金鑰憑證擁有者之識別資訊外，公開金鑰憑證亦持有關於有效期間及核發者識別資訊的經查證資訊。公開金鑰憑證可包括提供額外資訊之延伸。延伸係由定義延伸之組織所配置物件識別符所識別。公開金鑰憑證可能核發予 CA，稱為 CA 憑證，或核發予終端個體，稱為終端個體公開金鑰憑證。

於 PKI 環境中，公開金鑰憑證可能由個體所屬組織之 CA 進行數位簽署。於某些情況下，當個體通過自製造者至分銷者、購買者、安裝者等供應鏈時，將建立多個公開金鑰憑證。若使用，則核發 CA 之根憑證將成為信任錨。通常，組織宜僅安裝源自其所信任 CA 之 CA 憑證，包括由自有 CA 所核發的公開金鑰憑證。

公開金鑰憑證可指派予裝置、人類使用者或軟體應用等個體。

公開金鑰憑證係由基本集加上基本集之延伸所定義。延伸係由物件識別符所識別。

5.7.4.2 短暫公開金鑰憑證

短期憑證(公開金鑰憑證或屬性憑證)可能無需撤銷，因破解之可能性極低。短期公開金鑰憑證針對電力行業可能並非有用，因其可能意謂核發及配送新公開金鑰憑證之額外負擔，但可能於特殊情況下使用。

5.7.4.3 公開金鑰憑證更新

當憑證即將逾期時，個體需使用類似於登錄(enrolment)之過程申請憑證更新，但

更簡單，因憑證更新利用已可用之憑證資訊。

通常，既有登錄協定容許利用先前所核發憑證重新登錄。實作之特定過程取決於運作者的安全政策。

5.7.4.4 個體外部產生之非對稱金鑰的替代過程

若個體缺乏良好隨機數產生能力或必要之計算能力，則可於外部產生非對稱金鑰對。於該情況下，產生過程可委託予 PKI 遵循組件，諸如 PKI 工具。金鑰之配送將需使用受信任程序於帶外完成。私密金鑰可使用如 PEM、PKCS #8 或通常 PKCS #12 中之傳送金鑰加以保護，其中可能包括其他物件，諸如 CA 或根憑證。圖 7 顯示實現集中式金鑰及憑證產生之 1 種可能選項。建鑰資料的配送可藉由本地使用 PKI 工具完成之。

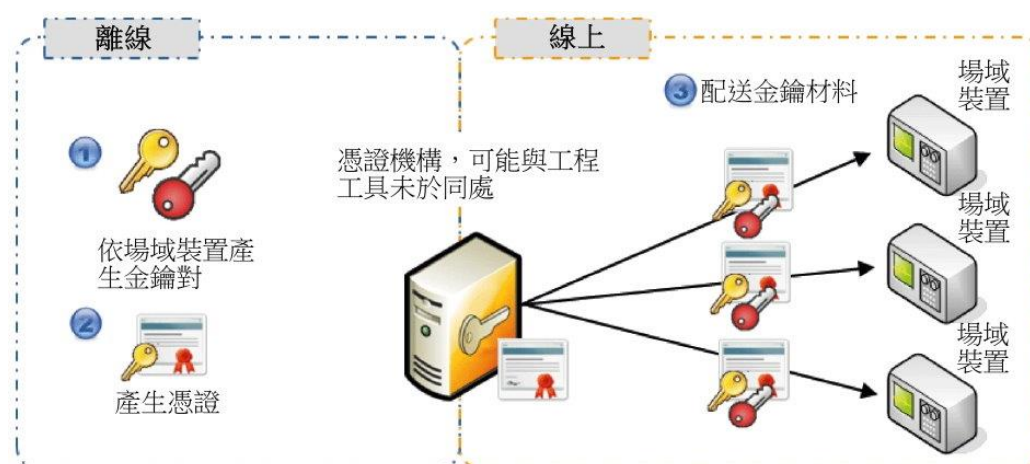


圖 7 中央憑證產生

若依製造者之信符已於場域個體中可用且受基礎建設所信任(於新部署領域中核發 CA)，則該憑證可用於識別場域個體並確保金鑰配送作業的安全。此要求 CA 已知悉該信符。

5.7.5 屬性憑證

針對識別資訊，屬性憑證提供將其識別管理，自與其相關聯授權之管理分離的有效方式。藉由以 PKI 管理公開金鑰憑證，並以「權限管理基礎建設」(其使用相同於 PKI 之 CA 技術)管理屬性憑證，即能達成完全分離。

如圖 8 所示，屬性憑證能用以延伸公開金鑰憑證中之資訊。例：其容許透過依特定角色的存取資訊暫時增強公開金鑰憑證持有者的權限。CNS 62351-8 中已採用

此作法。

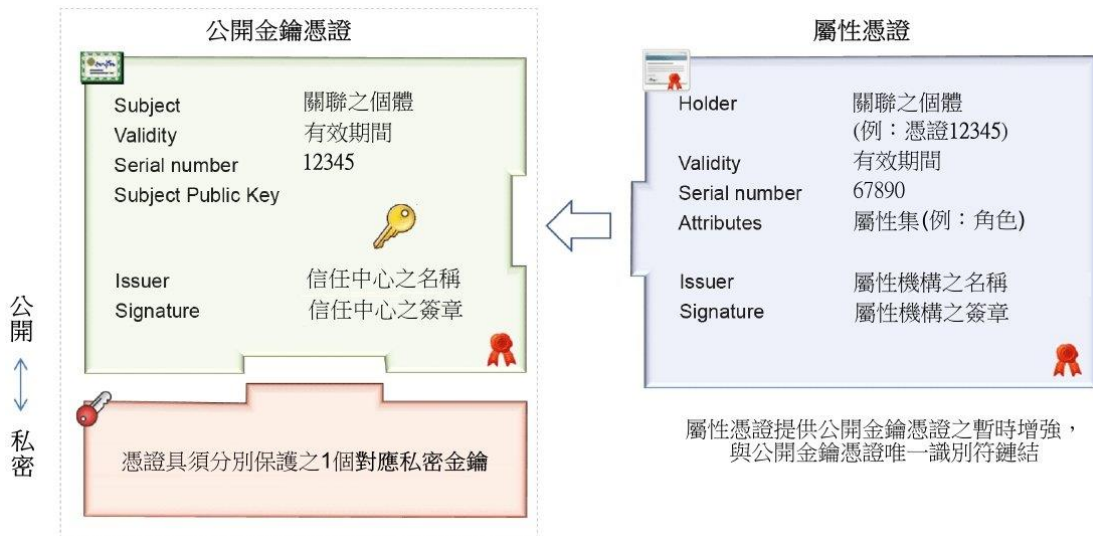


圖 8 公開金鑰憑證與屬性憑證間之關係

屬性憑證可能指派予裝置、人類使用者或軟體應用等個體。

屬性憑證係由基本集加上基本集之延伸所定義。延伸係由物件識別符所識別。

屬性憑證能視為達成對公開金鑰憑證短期或臨時延伸之另一作法 (亦參照 5.7.4.2)。短期屬性憑證能用以暫時延伸 CNS 62351-8 中所定義個體之權限，例：一般及緊急情況下之角色式存取控制 (role-based access control, RBAC)。此種屬性憑證宜包括 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019) 中所定義未撤銷資訊延伸。

5.7.6 公開金鑰憑證及屬性憑證延伸

公開金鑰憑證及屬性憑證容許選項包括延伸。各此種延伸提供額外資訊。

延伸型式由物件識別符 (參照 7.6) 組成，其識別延伸型式並規定相關資訊之語法。

此外，其亦包含規定特定延伸是否加旗標為關鍵或非關鍵之 Boolean。若延伸係加旗標為關鍵，則無法忽略，且若依賴方未支援該延伸型式，則公開金鑰或屬性憑證將視為無效。若延伸係加旗標非關鍵，且未支援延伸型式，則依賴方可忽略該延伸。更多細節，參照 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019) 之 7.3。

ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019) 規定數個通用延伸。CNS 62351-8 規定 IECUserRoles 延伸，其已針對電力系統定義，以提供角色式存取控制方

法。

5.8 公開金鑰憑證之憑證管理

5.8.1 憑證管理過程

當憑證建立、每次個體所有權或使用變更及憑證即將逾期時，可重複憑證管理過程。

除用於憑證管理之機制及協定(詳述於下列各節中)外，於憑證管理過程中針對請求者亦宜遵守 2 個重要性質：

- 識別資訊之證明，以確保於憑證管理中考量正確的個體。此能藉由使用不同方式所完成，諸如裝置相關資訊連同啟動碼(OTP)，或已可用之憑證及對應的私密金鑰。具體而言，後者容許過程之更高程度自動化。
- 擁有對應私密金鑰之證明，以確保公開金鑰提供者亦擁有私密金鑰。此係通常藉由對請求資訊(例：PKCS #10 製作憑證請求)進行數位簽章所完成，其能由中央註冊機構查證。

為請求憑證，要求識別資訊證明與擁有證明兩者之組合，以確保以授權方式針對標的個體核發公開金鑰憑證。

5.8.2 初始憑證建立

正如出生證明係個人身分之證明，且針對個人身分識別要求該人親臨註冊辦公室，通常當裝置或系統仍於製造者場所且由新擁有者接收時，亦需具其識別資訊證明。此係藉由以 RA 註冊並由製造者之 CA 核發憑證所達成。此憑證可依該製造者之信任錨查證之，因此其需公開。單 1 個體可人工註冊，大量個體註冊可批量處理。註冊過程則扮演供應鏈信任之來源或個體的來源。

於 IEEE 802.1AR 全景中，初始信符稱為 IDevID，用於初始裝置識別資訊。其係三值組，由初始裝置憑證、對應之私密金鑰，以及直至核發者(此處為製造者)信任錨的憑證鏈組成。

5.8.3 個體之加入

將個體引入網路要求於個體與運作領域間建立相互信任，通常導致裝置擁有運作

領域之信任錨點，以及其自有憑證及對應的私密金鑰，以鑑別相同領域之其他組件。此處，藉由具運作憑證以建立與初始裝置信符類似之三值組。IEEE 802.1AR 將此運作信符引用為本地重要裝置識別符之 LDevID，由本地裝置憑證、對應的私密金鑰，以及本地核發者根憑證的憑證鏈所組成。需注意，裝置可擁有多個用於不同目的之 LDevID。

針對基礎建設側上進行進一步查證，藉由將廠商之遞送資訊提供予領域，加入 (onboarding) 能為完全人工的過程。此一部分係將領域信任資訊組態設定於裝置中。此針對下一步登錄提供必要之邊界條件。後一部分，建立自個體至運作領域之信任，亦可自動化，從而自裝置觀點產生零接觸加入。為支援此自動化，可借助 IETF 於自發連網全景中定義之資訊物件及互動協定。需注意，下列示例並未構成可能方法之完整清單。

RFC 8366 [44] 規定證件製品，其能用以將資訊(新擁有者之領域憑證)自製造者傳遞予受保護(簽署)容器中的裝置。此簽章能要求裝置擁有製造者之根憑證的裝置所驗核。此處假設裝置附帶 IDevID。

RFC 8572 [76] 定義當連網裝置以出廠預設狀態啟動時，安全提供該裝置之機制 [安全零接觸提供，(Secure Zero Touch Provisioning, SZTP)]。其可能用於公眾或私用網絡，並於依 RFC 8366 中所定義證件上建構，以促進信任建立以及領域運作憑證之登錄。開機完成後，裝置能與其他系統建立安全連接。

RFC 8995 [47] 建構於所定義證件過程上，並定義架構及協定(遠端安全金鑰基礎建設之開機，BRSKI)，藉由供應新裝置建立相互信任，該裝置藉由涉及製造商發行包括此領域憑證的證件取得本地領域憑證資訊。該證件能由裝置查證，因其擁有源自製造者之信任錨。一旦裝置擁有領域憑證，其即能於標的領域中登錄，並接收新領域之 LDevID (本地裝置識別符) 憑證。

LDevID 亦為三值組，由本地裝置憑證、對應之私密金鑰，以及鏈接至核發者(此處為標的領域的運作者)信任錨之憑證組成。利用網路層級 LDevID 之開機資訊，可將進一步以應用特定 LDevID 提供予裝置，以建立與其他裝置的安全通訊連接。此外，RFC 8520 [46] (製造者使用說明，MUD) 定義支援自動化之進一步作法，

當安裝新裝置時，藉由規定製造商所使用資訊物件以提供有關設備自身，以及該裝置通訊行為/期望的資訊。後者能用以依本地安全政策採用滿足通訊需要之基礎建設。例：此資訊可用以改善基礎建設中之存取控制清單，或與外部服務相關的通訊埠。因此，MUD 藉由使用依裝置用途及功能之精細存取控制定義啟用網路分段。

5.8.4 個體之登錄

登錄係於運作環境中個體接收源自 CA 之經簽署憑證的過程。依個體既有之安全信符，能區分出不同登錄情境：

- 無需憑證之一次性唯一通行碼。
- 具 CA 所核發之憑證(此可能為製造者 CA 所核發的 IDevID)。
- 具已知(經授權)之自我簽署憑證。
- 憑證逾期或遭撤銷(此可能由製造者 CA 核發之 IDevID 或由本地 CA 核發的 LDevID)。
- CA 憑證逾期或遭撤銷。

存在支援不同功能集之不同憑證登錄及管理協定。其中 4 個係簡要描於 5.8.6 中。其中，2 個係聚焦於電力系統領域之應用，亦即 SCEP (參照 5.8.6.1)及 EST (參照 5.8.6.2)。此 2 種協定係因應管理電力系統中裝置憑證所必要之主要功能，同時保持簡單性，且提供功能相當豐富的協定 CMP (參照 5.8.6.3)及 CMC (參照 5.8.6.4)所提供之功能子集。後 2 個登錄協定於離線情境中提供較佳支援並支援撤銷處理。

圖 9 顯示使用 SCEP 登錄個體之示例。針對 SCEP，啟動碼如圖 9 所說明之 OTP (單次通行碼)，或現有憑證。針對 EST，啟動碼可為使用者名稱及通行碼或既有金鑰對[例：製造者核發(簽署)之憑證，具對應的私密金鑰及核發 CA 資訊，IDevID]。

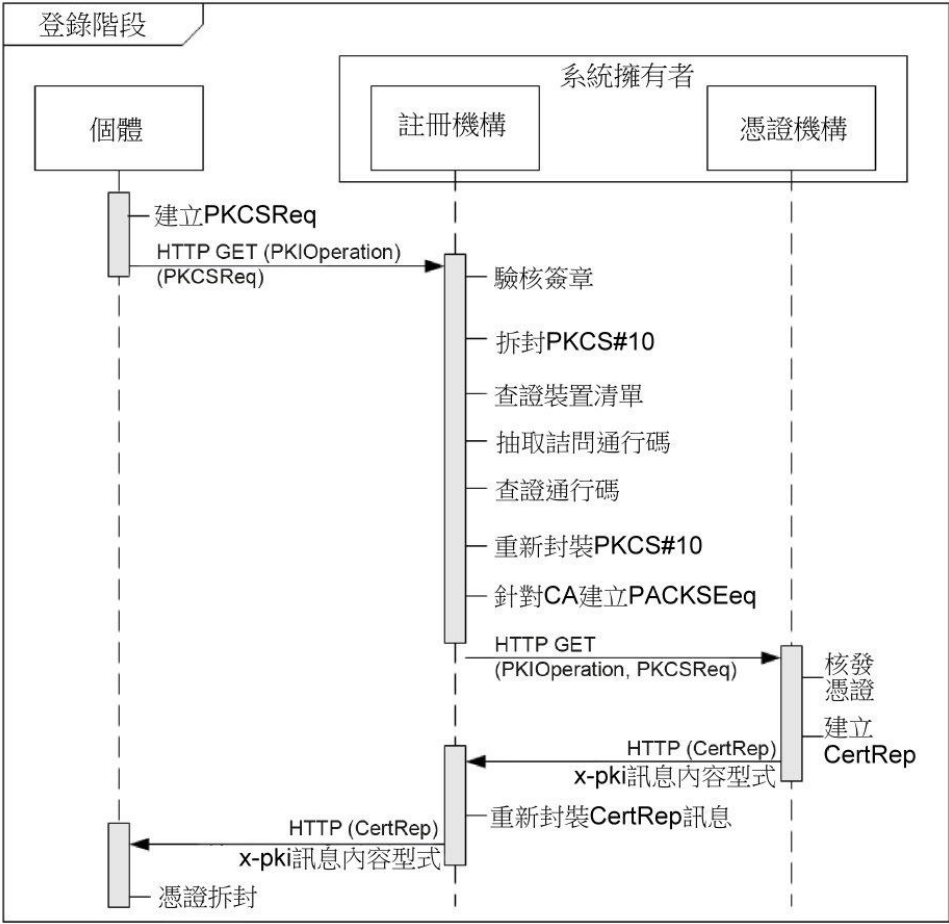


圖 9 SCEP 個體登錄及 CSR 過程之示例

圖 10 顯示使用 EST 登錄個體之示例。

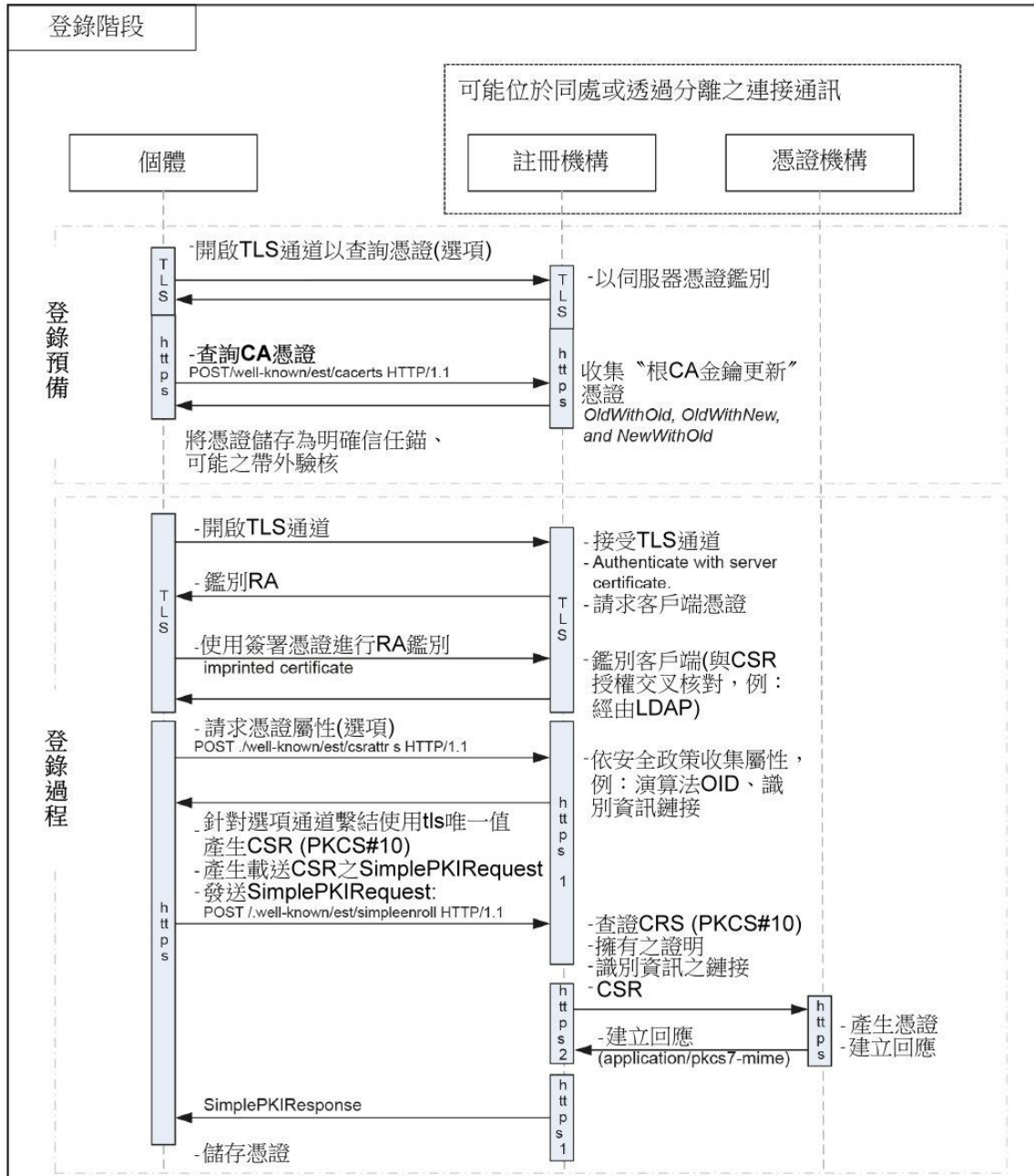


圖 10 EST 個體登錄及 CSR 過程之示例

關於圖 9 及圖 10 之註解：

- 登錄前，須組態設定裝置。除其標準組態(諸如自身 IP 位址)外，亦須提供其 PKI 登錄資料、RA/CA IP 位址、信任錨憑證(CA/根憑證)等。如 5.8.3 中所述，此過程能為人工或自動。依 5.8.3 中所述之示例協定能支援自動提供。
- 個體依 CA 之根憑證核對通訊同級的真確性。此根憑證係裝置組態設定階段期間(參照 7.3.6)，或作為自動加入之一部分饋入裝置。CA 以 CA 私密金鑰簽署

所核發之憑證。個體藉由查證使用 CA 公開金鑰之憑證中的簽章，核對所接收憑證的真確性。

5.8.5 憑證簽署請求(CSR)處理

5.8.5.1 登錄過程

登錄過程涉及由 CA 簽署之憑證，以查證個體的識別資訊、查證該個體是否擁有與公開金鑰相關聯之私密金鑰，並就該效果核發憑證。此憑證簽署要求個體(裝置)對 RA/CA 發出憑證請求。使用裝置產生之金鑰材料的 CSR 處理包括下列步驟，如圖 11 所示。

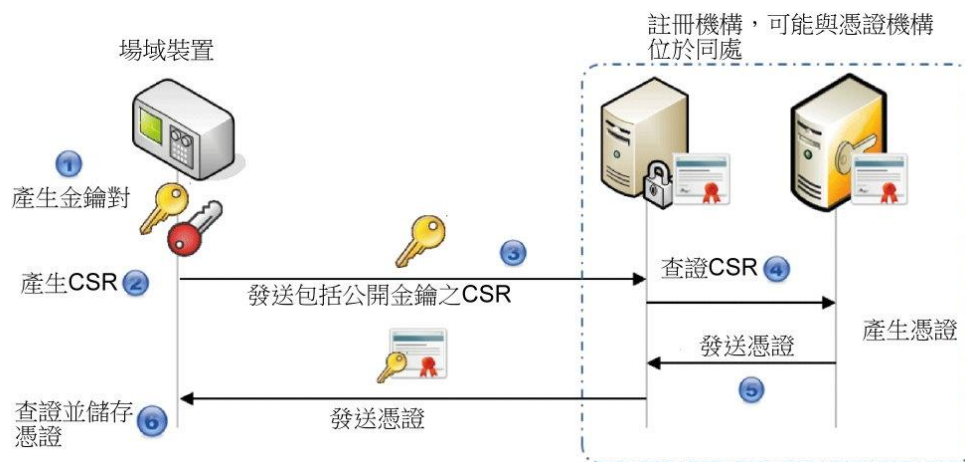


圖 11 CSR 處理

- (1)個體產生一對公開金鑰及私密金鑰。
- (2)個體產生 CertificationRequestInfo，此處使用 PKCS #10 規格格式[18]。此請求包含“主體區別名稱”、剛產生之公開/私密對中之公開金鑰(參照 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019))，以及選項屬性集。CertificationRequestInfo 係以個體之私密金鑰簽署。CertificationRequestInfo、簽章演算法識別符及個體之簽章進入 CertificationRequest 結構。參照[18]。
- (3)個體將 CertificationRequest 訊息發送予 RA/CA，用以作為登錄協定之一部分授權並製作憑證(參照 5.8.6)。
- (4) RA 藉由查證傳入請求上之簽章以驗核請求。
- (5)若請求有效，則 RA 鑑別請求之個體，若有效並經授權，則調用 CA，其自區別名稱(distinguished name, DN)及公開金鑰、核發者名稱，以及憑證機構之序

號選擇、有效期間、選項延伸，以及提供所列資料簽章資訊的數位簽章演算法，建立公開金鑰憑證。然後，CA 經由 RA 將憑證發送予個體。

(6)個體於接收自 CA 之憑證上執行簽章查證，以確保其係由受信任的 CA 所核發並簽署。需注意，此處之假設為受信任之 CA 憑證於試運轉/加入/組態設定階段期間配送並安裝於個體中。個體借助此等受信任之 CA 憑證查證接收自運作 CA 的憑證上之簽章。若 CA 簽章有效，則當儲存係屬檔案式時(例：.der、.pem、.cer 或 .crt 等)，個體以實作優選格式及適切之檔案副檔名儲存憑證。

CSR 過程可要求人員參與管理角色以啟動、啟用或核可 CSR 過程。此人工支援可能有必要與 CSR 申請同時進行，亦可能提前，取決於個體鑑別程序。若個體以廠商核發之信符(IDevID)或單次通行碼鑑別，則能提前對 RA 提供此資訊。

下列 2 節描述憑證請求格式 PKCS #10 及 CRMF。

5.8.5.2 PKCS #10 憑證請求

依 IETF RFC 2986 [18]所定義，憑證請求語法係由不同公開金鑰憑證管理協定所使用，以將憑證請求自客戶端(終端個體)傳遞予 CA 或介接 CA 之個體，例：RA 或 EST 伺服器(參照 RFC 7030)。

IETF RFC 2986 並未規定任何回應格式或如何進行憑證請求，而是留待參考規格。憑證請求於 RFC 2986 [18]中規定為 PKCS #10。憑證請求自個體發送予註冊機構(RA)，註冊機構可與 CA 位於同處，或為實體分離。

圖 12 說明憑證請求之結構。其具下列組件：

- (a) Version 組件指示憑證請求之版本。IETF RFC 2986 所規定之版本為版本 1，且由值“0”所指示。
- (b)主體組件規定所請求公開金鑰憑證之主體組件中使用的名稱。
- (c)主體公開金鑰資訊組件規定待納入所請求公開金鑰憑證之 subjectPublicKeyInfo 組件中的資訊。
- (d)屬性組件持有一組目錄屬性，其針對所請求公開金鑰憑證之產生提供額外資

訊。

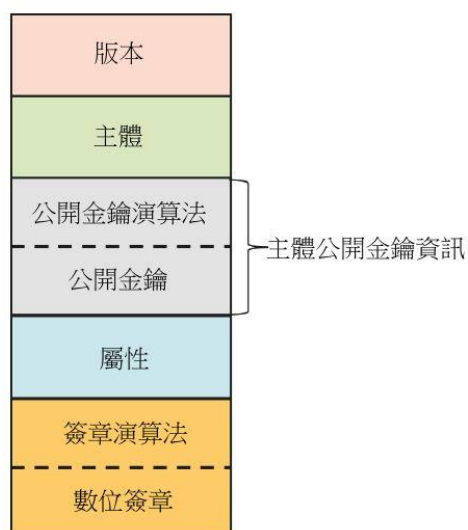


圖 12 憑證請求格式

憑證請求係使用對應於憑證請求中所提供之公開金鑰的私密金鑰進行數位簽署。

若接收者能使用憑證請求中所提供之公開金鑰驗核該簽章，則證明核發者擁有對應於所提供公開金鑰的私密金鑰。

IETF RFC 2985 [19]定義 2 種視為與包含於憑證請求中相關之屬性型式：

- (a)可能包括 challengePassword 屬性型式之屬性，若出現，則相同屬性應用於撤銷請求。
- (b)可能包括 extensionRequest 屬性型式之屬性，且該屬性隨後應持有待納入公開金鑰憑證中的公開金鑰憑證延伸序列。

5.8.5.3 憑證請求訊息格式(CRMF)

憑證請求訊息格式(CRMF)規定於 IETF RFC 4211 [20]中，如圖 13 所示。



圖 13 憑證請求訊息格式

有如 5.8.5.2 中所述之憑證請求，CRMF 並未構成協定，而是納入參引的協定型式中的資料型式規格。

IETF RFC 4211 提供 CRMF 之細節。CRMF 不同部分的概觀如下：

- (a) 憑證請求 ID 可用以配對請求及回應。
- (b) 憑證模板容許請求者規定或省略所請求公開金鑰憑證之各組件的內容。儘管 ASN.1 容許某些組件出現，但省略某些組件之規格可能有點令人困惑。出現單一組件(公開金鑰資訊)，但仍列為選項。有關細節，參照 IETF RFC 4211。
- (c) 控制項係非屬公開金鑰憑證一部分之屬性，但提供有關如何核發公開金鑰的全景之資訊。IETF RFC 4211 定義許多控制項，如有關公開金鑰憑證主體之額外鑑別資訊、有關如何發布公開金鑰憑證的建議、有關宜如何歸檔私密金鑰之建議、有關可能的舊公開金鑰憑證之資訊，以及由 CA 用以加密回應的加密金鑰。
- (d) 擁有之證明(若出現)提供如何證明擁有私密金鑰的詳細規格，取決於金鑰是否係旨在用於數位簽章加密(RSA)或用於金鑰協議。
- (e) 請求資訊。

憑證請求訊息格式(CRMF)語法及語意係用以可能經由註冊機構(RA)將憑證請求傳遞予 CA，用以產生公開金鑰憑證。該請求通常將包括公開金鑰及相關聯之註冊資訊。

5.8.6 登錄協定

5.8.6.1 簡單憑證登錄協定(SCEP)

簡單憑證登錄協定(simple certificate enrolment protocol, SCEP)之開發係為簡化大量裝置的登錄，並使數位憑證之核發具可延伸性。SCEP 之功能僅限於憑證登錄及更新，以及 CA 憑證及 CRL 配送。個體能使用透過 HTTP 之 SCEP 使用 CMS 及 PKCS #10，以電子方式請求其數位憑證。金鑰材料僅產生於客戶端。

登錄請求之客戶端側鑑別可能藉由使用自我簽署憑證或 CA 所核發憑證所完成。針對自我簽署憑證，有必要使用額外秘密(詰問通行碼)容許憑證請求之授權。針對 CA 核發之憑證，若其能於 RA 側驗核，則能直接鏈接至 CA 所核發的憑證。SCEP 將識別資訊證明及擁有證明與憑證請求客體(object)繫結。

需注意，SCEP 利用加密及數位簽章保護所交換之訊息。所交換之請求及回應訊息係依 SCEP 傳訊物件(依賴 CMS)。訊息之加密取決於所使用的非對稱密碼演算法，如下所示：

- 針對 RSA 式憑證(個體或 CA 側)，資料係使用接收者之公開金鑰所加密。
- 針對 ECDSA 式憑證(個體或 CA 側)，資料係依詰問通行碼加密。需注意，此設計於運作期間產生影響，因其亦要求於憑證更新前配送詰問通行碼。

SCEP 係由 IETF 定義，可作為參考性 RFC 8894。初始標準之修訂部分係自 PKCS #7 至 CMS 之變遷，此容許更廣泛覆蓋密碼演算法。因此，其可視為 CMC 之剖繪。

5.8.6.2 透過安全傳送登錄(EST)

透過安全傳送登錄(EST)定義於 RFC 7030 中，且係依 CMC 中之簡單 PKI 處理。其將某些 CMC 功能定義為選項，從而降低協定之複雜度。其可視為 CMC 之簡化剖繪。由 EST 所支援之功能包括 CA 憑證及 CRL 配送、於產生 CSR 前檢索憑證請求屬性以查詢額外資訊或邊界條件、憑證登錄及憑證更新。其容許客戶端或

伺服器側金鑰產生。

於 EST 中，僅簡單 PKI 請求/回應互動係屬必備，而完整 PKI 程序支援則為選項。EST 利用 TLS 作為安全通道，並藉由將 CSR 繫結至實際之 TLS 會談，利用 TLS 通道的鑑別識別並授權請求者。除識別資訊證明外，CMC 部分亦提供於 CSR 中對應公開金鑰之私密金鑰的擁有證明。

除憑證登錄及管理功能外，EST 亦容許依已安裝之信任錨，管理源自核發 CA 的裝置上之信任錨。

EST 可直接於 RA 處或 CA 處終止。於 RA 處終止 EST 不影響 RA 與 CA 間之通訊。於 RA 處終止 EST，要求 RA 於用以對 CA 鑑別之憑證中具特定延伸，以確保請求授權已由正確之個體所完成。需注意，亦可於 RA 與 CA 間使用其他登錄協定。

備考：實作者宜注意 IETF RFC 8951 關於傳送編碼及 ASN.1 之釐清。

5.8.6.3 網際網路 X.509 PKI 憑證管理協定(CMP)

憑證管理協定(CMP)係用以於 PKI 環境中取得公開金鑰憑證之網際網路協定。其定義客戶端與 PKI 組件間互動之協定。除 CRL 檢索、憑證請求處理、請求者之識別/授權選項，以及相關聯私密金鑰的擁有證明外，CMP 亦提供如跨域憑證(cross certification)及憑證撤銷等額外功能。CMP 支援客戶端及伺服器側產生金鑰材料。CMP 將識別資訊證明及擁有證明與憑證請求客體繫結，使其獨立於傳送。CMP 使用 CRMF 作為 PKI 訊息之訊息格式。亦支援 PKCS #10 請求之傳送。CMP 定義於 RFC 4210 [30]中。透過 HTTP 之 CMP 傳送定義於另份標準 RFC 6712 [42]中。

由於 CMP 功能豐富，目前正標準化輕量級剖繪[48]，以藉由將功能限制為必要之交換以因應工業使用案例。

5.8.6.4 透過 CMS 之憑證管理(CMC)

透過密碼訊息語法(CMC)之憑證管理建構於密碼訊息語法(CMS，定義於 RFC 5652 中)、PKCS #10 (RFC 2986)及 CRMF 的基礎上，以支援憑證管理。類似於 CMP，CMC 支援 CRL 檢索、憑證請求處理、請求者識別/授權選項，以及相關聯

私密金鑰之擁有證明。CMC 亦提供跨域憑證及憑證撤銷等額外功能。然而，CMC 定義簡單且完整之 PKI 請求/回應交換，但要求同時實作兩者。CMC 支援客戶端及伺服器側產生金鑰材料。

使用完整 PKI 請求時，CMC 將識別資訊證明及擁有之證明繫結至憑證請求客體。

針對簡單 PKI 請求，須藉由其他方式提供識別資訊證明。

CMC 定義於 RFC 5272 中。CMC 自身之傳送定義於另份標準 RFC 5273 ([35])中。

5.8.7 信任錨管理協定(TAMP)

先前幾節中討論之登錄協定特定涉及終端個體憑證的處理，但亦針對作為信任錨的其下根憑證之管理提供部分支援。信任錨管理協定(TAMP)建構於 CMS 之上。

TAMP 規定於 RFC 5934 中，並提供裝置信任錨儲儲存處中之信任錨(TA)的傳送獨立管理。

5.9 公開金鑰憑證之撤銷

5.9.1 憑證撤銷清單(CRL)

CRL 係遭撤銷憑證之序號清單，連同指示憑證撤銷時間的時戳，以及核發 CA 之數位簽章。亦可提供撤銷原因，因其定義為 CRL 之延伸。撤銷之憑證宜視為不再有效，任何個體不宜依賴。

每當憑證遭撤銷時，宜更新 CRL。宜及時對所有受影響之個體提供此等資訊。跨個體及建立 CRL 之系統的適切精密之時間同步，針對確保 CRL 中的時間資訊準確，以及個體擁有有關遭撤銷憑證之準確資訊係屬必要。對時鐘同步及準確度之支援定義於不同的協定中。示例為：

- 網路時間協定(NTPv4，IETF RFC 5905)。
- 精密時間協定(PTP，IEEE 1588v2.1)。

針對此 2 種協定，已定義安全增強(亦參照 7.7)。

圖 14 顯示 CRL 之示例。

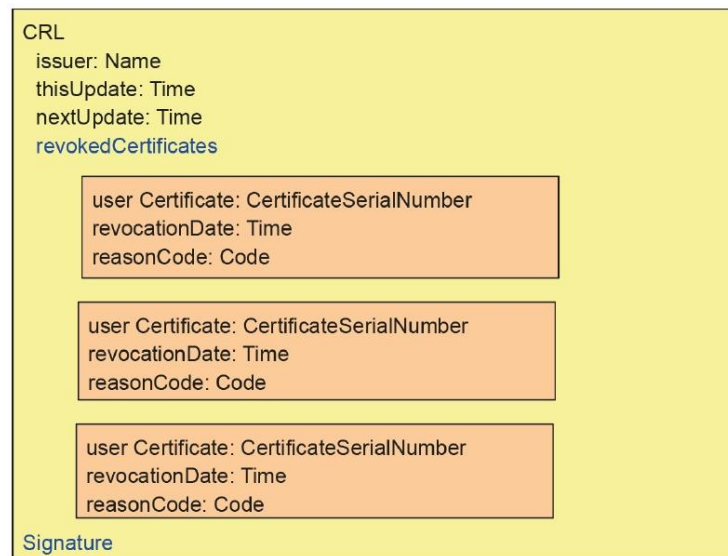


圖 14 憑證撤銷清單

由於 CRL 隨時間推移累積撤銷之憑證，因此其可能成長且變得極大。對嵌入式系統，大量 CRL 可能是問題，因嵌入式系統可能無足夠之可用記憶體容量可儲存。因此，可將 CRL 分區，作為最小化任何特定個體清單之方法。替代撤銷核對方法可能更有效，如 5.9.2 中所述。

宜依下列原因撤銷憑證，並使用 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019) 之 9.5.3.1 中所定義的原因代碼。

- 私密金鑰疑似外洩。
- 懷疑與 CA 憑證相關聯之 CA 私密金鑰遭破解。
- 個體之隸屬已變更。
- 公開金鑰憑證遭取代。
- 該個體已停止運作。
- 憑證被保留。
- 權限遭撤銷。
- 懷疑屬性機構之私密金鑰遭破解。

5.9.2 線上憑證狀態協定(OCSP)

當核對公開金鑰憑證之撤銷狀態時，RFC 6960 所定義線上憑證狀態協定(OCSP)係 CRL 檢索的替代方法。

若依賴方顧慮特定公開金鑰憑證是否仍有效，其可將 OCSP 撤銷狀態請求發送予負責個體憑證之 OCSP 伺服器(或 CA)。此 OCSP 請求包含協定版本、服務請求、個體之憑證識別符及延伸。為避免重演攻擊，須使用“單次隨機數(nonce)”(一次性值)區分此狀態請求與任何先前之狀態請求。然後，OCSP 回應者驗核憑證並回傳“good”、“revoked”或“unknown”，並使用自有數位簽章以鑑別回應。此 OCSP 序列如圖 15 所示。

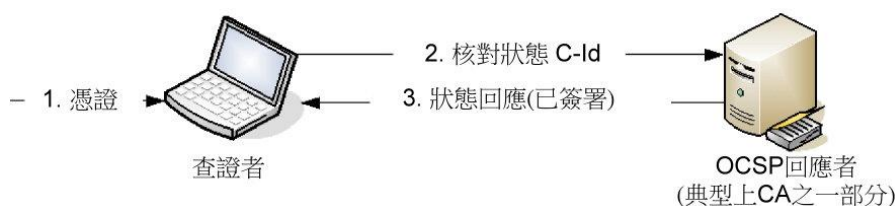


圖 15 線上憑證狀態協定(OCSP)概觀

通常，個體與 OCSP 回應者間要求線上連接以傳送 OCSP 請求及 OCSP 回應。然而，針對場域個體之某些組態而言，連續連接可能具挑戰性。此外，處理 OCSP 回應之運算工作量及通訊延遲就某些個體而言可能不可行。此外，OCSP 回應之有效期間宜較短，因 OCSP 回應者不發出非懇求性狀態更新，即使憑證於狀態核對後不久遭撤銷。

OCSP 快取係容許 OCSP 回應之接收者將回應快取一段時間之選項。此可避免於特定時框期間內重複 OCSP 查詢。其亦使發送者能將 OCSP 回應釘於其憑證上，從而避免回應者與 OCSP 伺服器互動。本系列標準第 3 部使用此選項。

因此，取決於系統設置及個體之能力，可利用 CRL 及 OCSP 的混合組合，其中通常具連接性之個體扮演代理 OCSP 回應者。此代理個體於特定時段內(諸如每小時或 24 小時內)擷取 CRL。然後，代理個體(例：站所控制器)扮演通常未連接至 OCSP 之其他個體的 OCSP 回應者。圖 16 描繪此作法。

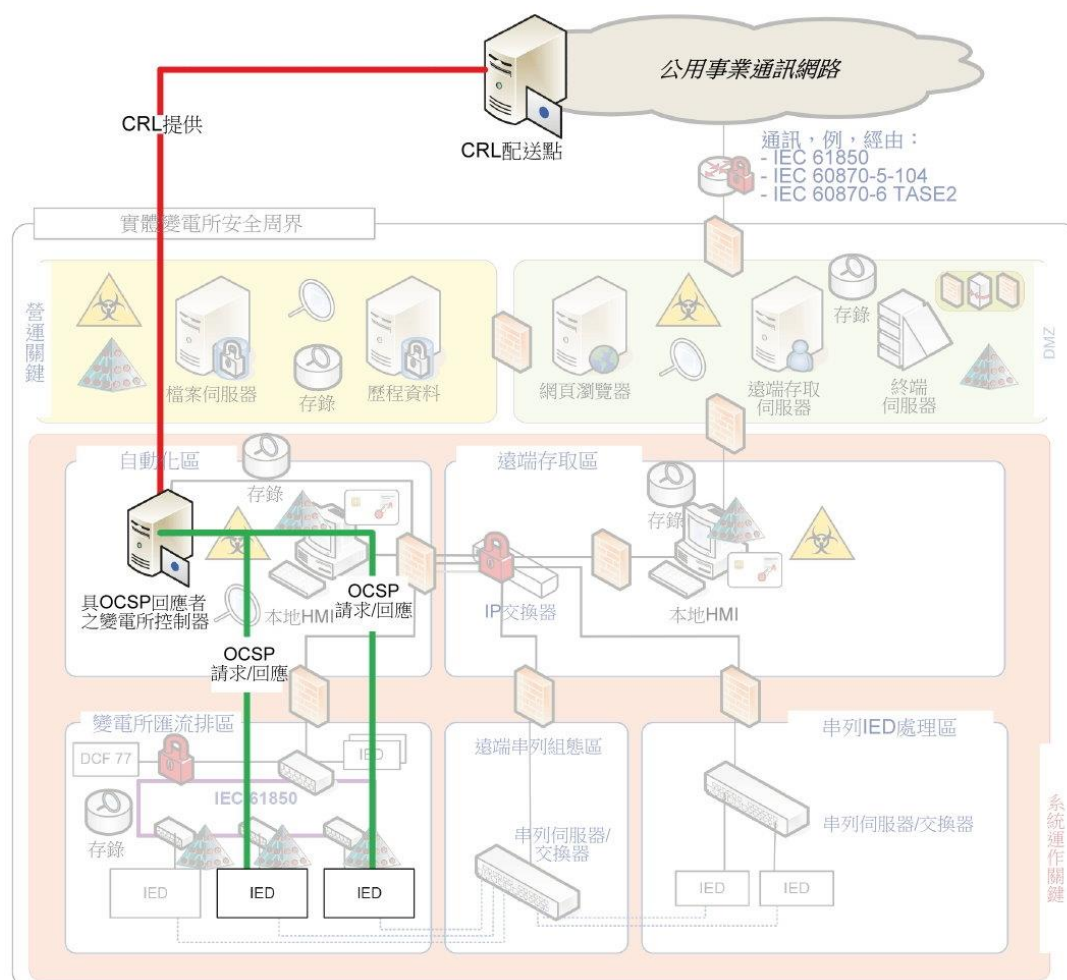


圖 16 使用 CRL 及 OCSP 過程組合之圖表

此作法之明顯優點為，其容許於缺乏與中央 CRL 資料的永久連接之本地網路中使用 OCSP 過程。此外，此亦減少與後端的資料訊務，此針對低頻寬連接可能必要。

個體宜存取受信任之即時時鐘，以核對並確保 OCSP 時戳的準確度。若於可設定之逾時(例：15 秒)內無回應抵達，則個體宜觸發 OCSP 不成功告警，並假設憑證尚未遭撤銷(特別是於可用性至關重要的情況下)。

為實作此作法，代理 OCSP 個體(例：站所控制器)有必要擁有憑證及對應之私密金鑰以扮演扮演 OCSP 回應者。因此，OCSP 回應者將組態設定為具 CA 簽署憑證之受信任回應者節點。

OCSP 請求亦可於同級 OCSP 回應者間鏈接，使得查找及查詢核對中之個體憑證的適切 CA，回應者使用其自有 OCSP 請求依根 CA 驗核彼此之回應。

OCSP 請求可主動或被動執行，如圖 17 所示。於主動情況下，個體提前對 OCSP 回應者請求其憑證狀態，並將 OCSP 回應與其憑證一起發送予正驗核該個體之同級節點。此稱為「OCSP 裝訂」，並將 OCSP 通訊之負擔置於主動個體上。於被動情況下，接收節點執行 OCSP 請求以核對同級個體所提供憑證之撤銷狀態。被動式選項較常用，但 TLS 1.2 (RFC 5246)等協定使用 RFC 6066 [41]中所定義之延伸，以支援主動式選項，容許 TLS 1.2 伺服器將 OCSP 回應作為 ServerHello 訊息的一部分傳送。此與圖 17 中所示之主動伺服器案例相關。

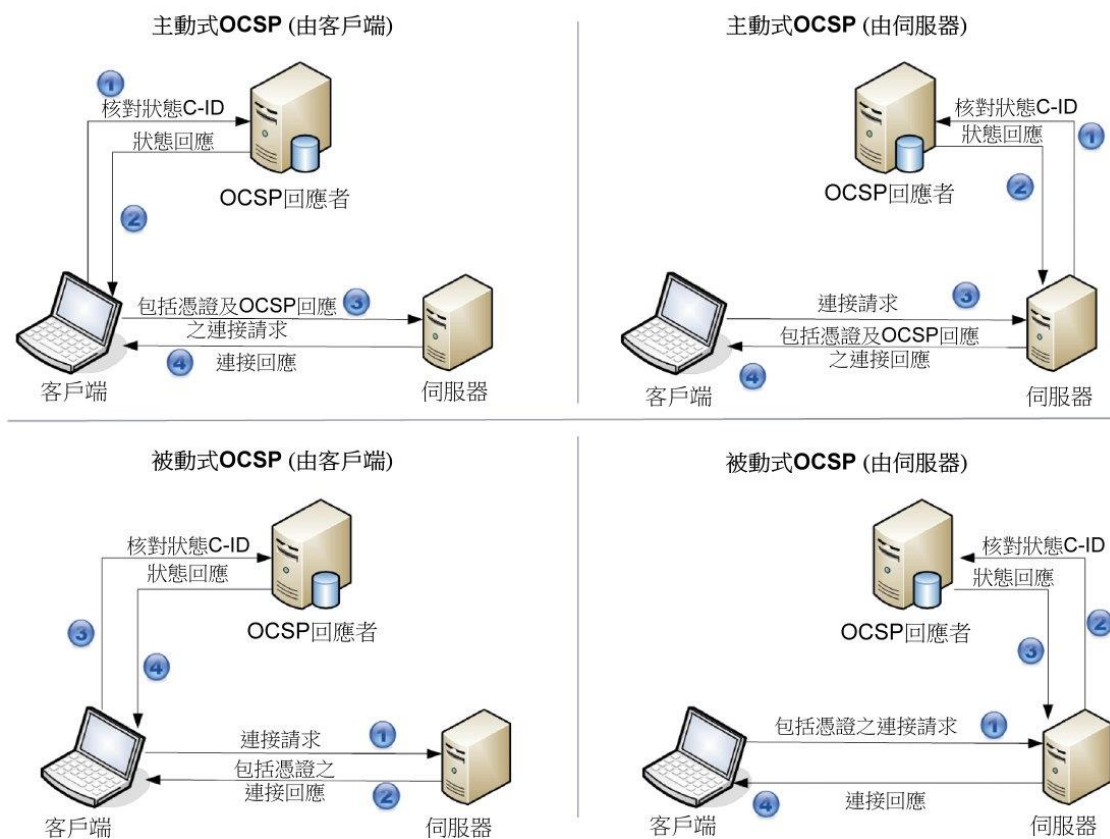


圖 17 線上憑證狀態協定(OCSP)之調用過程

需注意，TLS 1.3 (RFC 8446 [45])亦容許對 TLS 客戶端憑證進行 OCSP 裝訂。若憑證撤銷或憑證有效性核對不成功，則於大多數情況下，預期個體將於發送 OCSP 告警以警告運作者可能存在未經鑑別之通訊後連續運作。此可防止由於 OCSP 回應者不可用所導致之阻絕服務攻擊。

5.9.3 伺服器式憑證驗核協定(SCVP)

憑證之有效性核對可能變得複雜，尤其於憑證路徑相當長的情況下。針對此情況，伺服器式憑證驗核協定(SCVP)容許個體將憑證路徑建構及憑證路徑驗核委託予“主”節點。此協定定義於 RFC 5055 ([34])中。SCVP 可能與 CRL 及 OCSP 結合使用(如圖 18 所示)。

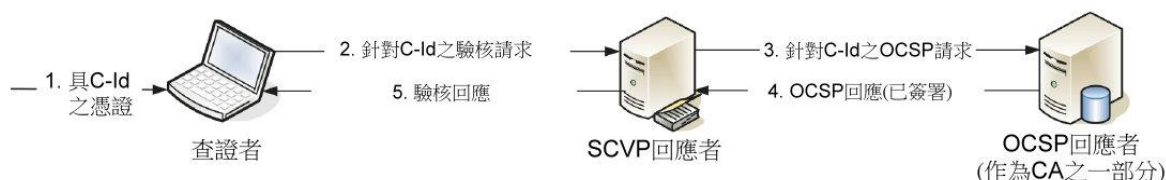


圖 18 使用 OCSP 後端之伺服器式憑證驗核協定概觀

此外，建議保持 CA 階層盡可能扁平且緊湊，以減少驗核憑證鏈時招致效能損失。

5.9.4 自終端個體之憑證撤銷復原

終端個體憑證可能因 5.9.1 所述之不同原因而遭撤銷。為自此情況中復原，進一步處理取決於實際撤銷原因。此原因之評估及適切的反應通常係由組織之安全政策(復原計畫)所定義，亦反映於憑證核發者之 CPS 中。因此，下列討論瞄準關於如何為裝置取得新憑證以保持其運作之可能方式概觀。

若因裝置中私密金鑰遭破解或攻擊者與裝置進行實體接觸而導致撤銷，則強烈建議服務技術人員執行裝置本地程序以變更/更新憑證及對應之私密金鑰。此亦宜涉及查證裝置及其運作設定值(實體及邏輯)完整性，以確保其無法遭誤用為攻擊啟始者，且亦確保裝置能安全運作。

一般而言，自憑證撤銷中復原可能涉及容許遠端更新憑證之管理方式。示例包括：

- 裝置擁有用以管理安全信符之專屬憑證。此憑證可為運作憑證(LDevID)或製造者提供之憑證(IDevID)。若未撤銷，則此憑證可用以登錄新憑證。裝置可自主查證其憑證之撤銷狀態，並立即觸發新憑證登錄。允許新登錄之決策可由裝置特定實作所支援。例：裝置可支援安全元件或專屬安全硬體以安全儲存及/或管理 IDevID，而運作信符(LDevID)可儲存於不同位置。然後，運作 PKI 之工作即為決定更新憑證。
- 能使用管理通道觸發裝置更新憑證。此可能為使用 Web (https)、SNMP、ssh 或其他協定之分別連接，其信符已於帶外或於初始加入期間提供。亦可按下裝置

上之專屬按鈕重新啟始開機。

如上所述，強烈建議評估撤銷原因，使得能據此規劃後續步驟。

5.10 經由非 PKI 核發之(自我簽署)憑證信任

自我簽署憑證於 PKI 環境中發揮重要作用。PKI 中之信任階層或信任鏈係以“根憑證”為根(參照 5.7.4)。PKI 根憑證可為稱做信任錨之自我簽署憑證，由容許配送此信任之受信任 CA 所建立。

於某些情況下，為建立信任，非 PKI 核發之自我簽署憑證可能較更複雜的 PKI 簽署憑證更易於實作。於僅有限數量之個體的小型部署中尤其如此。非 PKI 核發之自我簽署憑證為個體內部產生的公開/私密金鑰對，其中私密金鑰係用以簽署個體自有公開金鑰及額外資訊(例：主體名稱、有效期間等)。其可能以相同於 PKI 式憑證之方式使用(例：鑑別 TLS 連接中的互動)，自我簽署公開金鑰憑證須遵循 ISO/IEC 9594-8 中所述的公開金鑰憑證結構。

此等自我簽署憑證無法普遍認為值得信任。因此，針對鑑別為使受限制之個體群組接受自我簽署憑證，其宜僅與授權及驗核清單結合使用(參照 5.11)。

使用特定於個體之自我簽署憑證以及授權及驗核清單的複雜程度，可與使用預先共享共享金鑰比較。自我簽署憑證係逐個體核發，而預先共享共享金鑰則為逐配對連接核發。因此，雖自我簽署憑證之數量將取決於端點數量，但預先共享共享金鑰的數量將取決於端點間之連接的數量。

由於自我簽署憑證需為公開金鑰憑證，因此其應用能開啟 PKI 式公開金鑰憑證實作之移轉路徑，使得一旦此等憑證可用，自我簽署憑證即可易於替換為 PKI 式憑證。

5.11 授權及驗核清單

5.11.1 一般

授權及驗核清單(AVL)提供有關可能通訊個體之資訊，以及於特定環境中與此類個體通訊的可能限制。其規定於 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)之第 11 節中。

當個體扮演依賴方時，AVL 係由該個體使用。此種個體稱為 AVL 個體。AVL

係置放於稱為授權者之個體中，其負責 AVL 之內容，亦即授權者受 AVL 個體信任以提供有效資訊。AVL 係由核發授權人所簽署。

授權者與 AVL 個體間之通訊須依任何其他通訊般於完整性、真確性，以及可能的機密性受保護。為簡化 AVL 之驗核，建議授權者與其服務之 AVL 個體密切相關，例：位於相同組織內，使得授權者與其服務之 AVL 個體間建立信任關係（參照 B.1）。

AVL 可用於非受限制環境或受限制環境，依 5.11.2 及 5.11.3 中所詳述。

5.11.2 非受限制環境中之 AVL

非受限制環境係 AVL 個體能對所接收憑證執行傳統驗核之環境。

AVL 係用於限制所規定之個體集合內的通訊關係。其可能對此類個體施加超出 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)之 11.3 中詳述之路徑長度、政策及名稱限制等限制。

可與其進行通訊之個體於 AVL 中藉由引用其公開金鑰憑證，或藉由個體所屬組織的名稱結構所識別。

5.11.3 受限制環境中之 AVL

個體可能會受到多種方式所約束：

- 其係電池驅動，需限制處理以節省電池。
- 其處理能力很小。
- 其通訊通道之頻寬受限制。
- 其具有限之儲存體。
- 其可能有嚴格時間限制，須極快速地回應事件，不容許外部通訊有時間驗核所接收之公開金鑰憑證。

AVL 授權者負責查證 AVL 中表示之所有公開金鑰憑證，是否有效且於核發 AVL 時可信任。授權者亦有責任更新其 AVL 中公開金鑰憑證之有效性。於撤銷可能影響關鍵個體之情況下，授權者亦可判斷何時宜或不宜使用逾期或遭撤銷的公開金鑰憑證。AVL 個體假設列出之公開金鑰憑證可有效使用。

此種運作模式要求授權者與核發 AVL 中列出之公開金鑰憑證的 CA 間通訊。

6. 金鑰管理(規定)

6.1 一般

金鑰管理適用於非對稱金鑰材料、對稱金鑰材料，以及兩者組合之處理。針對非對稱金鑰材料之處理，特別是於裝置及金鑰材料生命週期內管理憑證及對應的私密金鑰，應適用第 7 節。針對對稱金鑰之管理，特別是針對群組金鑰的管理，應適用第 8 節。

6.2 安全事件之處理

於整個文件中定義安全事件。此等安全事件旨在支援錯誤處理，從而提高系統韌性。實作宜提供一種機制來宣布安全事件。

有關安全事件的資訊和可能細節僅能由個體依該資訊通過其下平台或所使用的組件的可用性來提供。

強烈建議藉由本系列標準第 14 部中規定之網宇安全事件及/或本系列標準第 7 部中規定的監視物件，使整個標準中所定義安全事件於運作基礎建設可用。附錄 D 提供本標準中所定義事件與本系列標準第 14 部概念之對映。

需注意，通知、警告、錯誤及告警係用以自安全觀點指示事件之嚴重性。使用本系列標準第 14 部中的下列概念：

- 通知係指個體日常使用或維護過程中與網宇安全相關之活動。其與網宇安全漏洞或攻擊或偏離個體正常運作狀況無關。
- 警告(warning)係個體正常運作狀況的偏離，但未必為網宇攻擊。
- 錯誤(error)描述非預見之情況，此可能指示未經授權的活動。可能無須要立即採取行動。
- 告警(alarm)係嚴重問題之指示，其可能指示未經授權的活動。建議立即採取行動。

無論如何，預期組織之安全政策依運作環境判定事件的最終處理。例：對多個告警之一的評估可能上升至事故層級。

6.3 要求之密碼材料

引用本標準之標準應依第 9 節的協定實作符合性聲明(Protocol Implementation

Conformance Statement, PICS)表單，規定用以建立安全通訊所要求的加密資料。

6.4 隨機數產生

與金鑰管理相關之任何隨機值的產生應依循 ISO/IEC 18031 [87]。金鑰對產生器應負責提供統計上適足之隨機數產生器(RNG)並適切使用。

備考：指引參照 NIST SP 800-90A [61]及 IETF RFC 4086 [62]。

針對無法於內部產生金鑰之個體，金鑰應於外部產生。CA 或其他授權系統可提供此外部金鑰產生設施。然後，金鑰應安全地安裝於此等個體中。亦參照 B.12。

6.5 物件識別符

6.5.1 物件識別符之概念

物件識別符(object identifier, OID，由 ITU-T 及 ISO/IEC 所發展)係屬將任何型式之物件與持久名稱相關聯的識別機制。其通常以階層方式建構(如 OID 樹)。亦參照 ISO/IEC 9834-1 | Rec. ITU-T X.660。

OID 係由各種國際標準所配置，包括 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)，並可註冊私人使用。本系列標準之 OID 名稱空間(根)值為 1.0.62351 及 1.2.840.10070。CNS 62351-8 利用後一作法定義存取符記(授權)。本標準及本系列標準之新的各部宜使用第 1 個 OID (1.0.62351)。

6.5.2 本標準所識別物件之使用

ISO/IEC 9834-1 | Rec. ITU-T X.660 中規定物件識別符(OID)之配置政策。本標準之 OID 配置定義為：

```
id-IEC62351-9 OBJECT IDENTIFIER ::= { 1 0 62351 9 }
```

下列分支係用以定義 AVL 延伸之 OID：

```
avl62351Extion OBJECT IDENTIFIER ::= { id-IEC62351-9 1 }
```

下列分支係用以定義 AVL 資料項延伸之 OID：

```
avl62351EntryExt OBJECT IDENTIFIER ::= { id-IEC62351-9 2 }
```

下列分支係用以定義協定識別符之 OID：

id-62351prot OBJECT IDENTIFIER ::= { id-IEC62351-9 3 }

7. 非對稱金鑰管理(規定)

7.1 一般

本節描述處理非對稱金鑰材料之規定性要求事項。本標準全景中之非對稱金鑰材料係視為憑證的 3 個元素：公開金鑰、私密金鑰，以及有關核發憑證機構之資訊(信任錨、憑證鏈)。需注意，於 IEEE 802.1AR 全景中，此稱為 DevID (裝置識別)。本節定義終端個體上非對稱金鑰對之產生、其透過 PKI 的驗證，以及透過 PKI 之生命週期處理。

7.2 憑證組件

7.2.1 公開金鑰憑證組件

用於非對稱金鑰管理之公開金鑰憑證應為 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)中所定義的公開金鑰憑證。大多數一般延伸由 ISO/IEC 9594-8 | REC. ITU-T X.509 所規定。其他標準規定更特定之延伸。例：CNS 62351-8 針對存取控制規定支援使用者角色之延伸。

表 1 包括電力系統個體應識別並處理之公開金鑰憑證的必備及選項組件：

表 1 公開金鑰憑證組件

組件名稱	支援	內容
Version (版本)	M	憑證之支援版本：參照 7.4.4.2。
Serial Number (序號)	M	整數值，由核發 CA 所定義。針對由給定 CA 核發之各憑證，其應係唯一。
Signature (簽章)	M	用以產生憑證之簽章演算法，由 OID 所決定，參照 7.4.4.4。
Issuer (核發者)	M	核發 CA 之區別名稱，參照 7.4.4.3。
Validity (有效性)	M	憑證有效時間，參照 7.4.4.5。
Subject (主體)	M	識別與公開金鑰相關聯之個體，參照 7.4.4.6。

組件名稱	支援	內容
Subject Public Key Info (主體公開金鑰資訊)	M	公開金鑰之演算法識別符及公開金鑰自身，參照 7.4.4.7。
延伸		
Authority Key Identifier (機構金鑰識別符)	M	核發 CA 之金鑰識別符：決定用以查證憑證簽章的金鑰，參照 7.4.4.10.2。
Subject Key Identifier (主體金鑰識別符)	C1	個體公開金鑰之金鑰識別符，參照 7.4.4.10.3。
Key Usage (金鑰使用)	M (c)	識別公開金鑰憑證之預期用途，參照 7.4.4.10.6。
Extended Key Usage (延伸之金鑰使用)	C	識別公開金鑰憑證使用之其他目的(選擇係條件式，取決於使用案例)，參照 7.4.4.10.7。
Certificate Policy (憑證政策)	O	針對終端個體憑證，其指示核發憑證所依據之政策，以及 OID 可使用憑證的目的[36]。
Subject Alternative Name (主體替代名稱)	C	包含憑證主體之 1 或多個替代名稱。參照 7.4.4.10.4。
Basic Constraints (基本限制事項)	C (c)	待設定為核發 CA 憑證，否則 CA=false(或為空值/缺失)；額外組件 pathLenConstraint 可用以限制憑證路徑，取決於組織之安全政策，參照 7.4.4.10.5。
CRL Distribution Point (CRL 配送點)	C2	http 或/及 LDAP 之 CRL 位置，參照 7.4.4.10.9。
Authority Information Access (機構資訊存取)	C2	指示如何存取憑證授權者之資訊及服務：若經由 OCSP 提供撤銷資訊，則其包含 OCSP 回應者(id-ad-ocsp)的位置，參照 7.4.4.10.10。
Role-based Access control (角色式存取控制)	C3	依 CNS 62351-8 A 剖繪啟用角色式存取控制。參照 7.4.4.10.11。
Authorization Validation (授權驗核)	O (c)	若使用，則應將其設定為“c”，以確保依賴方於接受終端個體憑證前查證 AVL，亦參照 7.4.4.10.8。
SOA identifier (SOA 識別符)	C4	核發 AA 憑證之機構來源。參照 7.4.4.10.13。

組件名稱	支援	內容
<p>C1：應於 CA 憑證中設定。</p> <p>C2：設定此延伸係核發 CA 之責任。此容許 CA 亦核發無須撤銷核對之短期憑證。短期憑證之效期宜由運作者仔細評估並選定，特別是若核發的憑證中未包含 CRLDP 或 OCSP 回應者資訊。若無此訊息，則依賴方可能無法識別公開金鑰憑證之撤銷。因基礎建設須支援 CRL 及 OCSP，故可提供此 2 種延伸以容許依賴方核對撤銷狀態。</p> <p>C3：當支援 CNS 62351-8 之 A 剖繪時，應於終端個體憑證中設定。</p> <p>C4：應於核發 AA 憑證時設定，以使核發 CA 能識別 AA。</p>		
<p>表中使用下列記法：</p> <p>M 必備：應包括並處理。</p> <p>O 選項：能包括。</p> <p>C 條件式使用(參照表 1 底部備註)</p> <p>(c) 此延伸係屬關鍵。若實作辨識出現「關鍵」延伸，但該實作無法解譯該延伸，則該實作應拒絕該憑證。</p>		

憑證查證過程期間核對憑證內容。依查證期間所識別之問題進行錯誤處理。憑證查證描述於 7.4 中。

7.2.2 屬性憑證組件

若使用屬性憑證，則應為 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)中所定義之屬性憑證。憑證之延伸可能定義於其他標準中。

表 2 包括屬性憑證之必備及選項組件，其宜能由利用屬性憑證的電力系統個體所辨識並處理。

表 2 屬性憑證組件

組件名稱	支援	內容
Version (版本)	M	支援之憑證版本：參照 7.4.5.2。
Holder (持有者)	M	包含對持有者之公開金鑰憑證或其他個體名稱的參引，依 7.4.5.3 中所概述。
Issuer (核發者)	M	包含核發 AA 之區別名稱，參照 7.4.5.4。
Signature (簽章)	M	用以產生憑證之簽章演算法，由 OID 判定，參照 7.4.5.5。

組件名稱	支援	內容
Serial Number (序號)	M	整數值，由發行 AA 所定義。針對給定 AA 核發之各憑證，其應係唯一。
Attributes (屬性)	M	參照 7.4.5.6。若使用依 CNS 62351-8 之 B 剖繪的角色式存取控制，則所定義屬性應適用於屬性憑證。
attrCertValidityPeriod (屬性憑證效期)	M	包含屬性憑證之效期，參照 7.4.5.7。
延伸		
Authority Key Identifier (機構金鑰識別符)	O	核發 AA 之金鑰識別符。參照 7.4.5.8.2。
CRL Distribution Point (CRL 配送點)	C1	相同於公開金鑰憑證中使用之延伸名。於屬性憑證全景中，其係用以提供 ACRL 之位置，參照 7.4.5.8.3。
Authority Information Access (機構資訊存取)	C1	指示如何存取屬性憑證核發者之資訊及服務，參照 7.4.5.8.3。
No Revocation Available (noRevAvail) (無撤銷資訊可用)	C1	指示未針對此屬性憑證提供撤銷狀態資訊，參照 7.4.5.8.3。
C1 若提供 noRevAvail，則不應提供 CRLDP/AIA。若提供 CRLDP 或 AIA，則不應提供 noRevAvail，以避免不一致。由核發 AA 負責設定此等延伸。此容許 AA 亦可核發效期很短的屬性憑證，並且無須撤銷核對。		
表中使用下列記法： M 必備：應包括並處理。 O 選項：可包括。 C 條件式使用(參照表 2 底部之備註)。		

憑證查證期間核對憑證內容。應依查證期間所識別之問題進行錯誤處理。憑證查證描述於 7.4 中。

需注意，本系列標準中屬性憑證之功能支援僅規定用於 RBAC。其他用法超出本標準適用範圍。

7.3 憑證產生及安裝

7.3.1 私密金鑰及公開金鑰之產生及安裝

執行非對稱加密功能之個體應擁有至少一對非對稱金鑰。個體應產生自有非對稱密碼金鑰對並接觸 PKI 基礎建設以驗證，或因應其提供外部產生之密碼金鑰對，

包括源自核發 CA 的憑證。金鑰對中之私密金鑰應安全儲存。集中產生之密碼金鑰對的提供宜於受保護位置執行。

於下列條件下，個體應產生或提供新的金鑰對：

- 啟動時不出現金鑰對(若不出現或相關聯公開金鑰憑證逾期)。
- 個體控制權變更(所有權、控制機構變更及/或個體重新組態)。
- 藉由源自授權個體之命令(例：針對更新憑證的請求)。
- 個體之私密金鑰遭破解。
- 個體之 IP 位址(或 FQDN)已變更。

強烈建議電力系統中之裝置支援客戶端金鑰產生，以避免私密金鑰於裝置外部傳送。

金鑰提供所使用之格式描述於 7.3.2 中。

7.3.2 密碼金鑰保護

各個體之私密金鑰及長期對稱金鑰(包括預先共享金鑰)應受保護，防止未經授權的修改、檢索及複製。

於傳送期間，應藉由使用 PEM (RFC 7468)、PKCS #8 (RFC 7468)及 PKCS #12 (RFC 7292)中所定義之傳送金鑰加密，以保護私密金鑰免遭竊聽及篡改。所有個體應支援 PKCS #12 之處理。PKCS #12 容器亦宜包含所有核發之(子)CA 憑證。由於格式問題而無法處理 PKCS #12 物件將引發安全事件(“警告：PKCS #12 格式不匹配”)。實作宜提供發布安全警告之機制。

若支援 PKCS #8 物件但因格式問題而無法處理，則應引發安全事件(“警告：PKCS #8 格式不匹配”)。實作宜提供發布安全警告之機制。

若技術上可行，則任何破壞金鑰之嘗試都應係可偵測。此種事件應存錄並觸發告警。

備考：有關密碼金鑰保護之指引，參照 NIST SP 800-57 Part 1 [57]及 FIPS 140-2 [53]。此外，IEEE 1686 [5]、IEEE c37.240 [75]及 IEC 62443-4-2 [74]提供保護敏感資訊之要求事項。

7.3.3 使用既有安全金鑰管理基礎建設

只要核發 CA 提供直至根 CA 憑證之完整信任鏈(中間 CA)憑證，並支援所要求的憑證管理/登錄冊協定，亦即應容許使用依 7.3.7 中所述之既有安全公鑰管理基礎建設(PKI)與裝置/個體介接。

強烈建議僅安裝根 CA 憑證，其係運作環境中所必要，並用以完成裝置之工作。

選擇所支援之根 CA 憑證通常為組織安全政策的一部分。

7.3.4 憑證政策

強烈建議建立憑證政策[關於指引，參照 RFC 3647 ([26])]。

7.3.5 用於識別資訊建立之個體註冊

組織中待試運轉之所有個體應於至少 1 個註冊機構(RA)註冊，其可能未與該組織所核可的憑證機構(CA)位於同處。此 RA 應能查證憑證簽署請求(CSR)上之個體識別資訊。註冊可人工完成(例：針對少量個體)，或藉由運行腳本或組態設定產生自工程資料之正清單自動進行。註冊可於帶外、異地或現場進行。CSR 能人工匯出及匯入，或經由登錄協定傳送，依 7.3.7 中所述。

註冊資料應至少包括下列元件之一：

- 個體之主體，其識別個體以及將出現於個體憑證中之唯一名稱或主體的另一唯一識別符，例：序號。需注意，憑證可包括裝置之實體序號，如 X520SerialNumber 及 OID 標籤 id-at-serialNumber。參照表 1。
- 若 SCEP 係用於憑證登錄，則應提供唯一之一次性啟動碼(或 OTP)作為註冊資料，該碼容許個體於執行憑證請求(CSR)時對 RA 自我鑑別。
備考：如何建立 OTP 並將其配送予登錄個體超出本標準適用範圍。
- 製造者內建公開金鑰憑證的憑證序號及核發者，容許已使用此公開金鑰憑證對個體進行鑑別。
- 用於鑑別登錄之個體的公開金鑰憑證特徵。
- 受信任之核發 CA，其啟用以源自該核發 CA 之任意憑證登錄。

7.3.6 個體組態

除 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)中所定義基本憑證參數外，個體組態資料應包括下列內容：

- 組織之 CA 憑證，個體應信任並以其通訊(參照 5.6.4)。宣稱符合本標準之實作應支援至少 5 個與憑證機構相關的信任錨。實際數量取決於標的使用案例。需注意，此要求係對齊本系列標準第 3 部。
- 容許執行 PKI 運作(諸如 CSR 處理)之組織的 IP 位址或領域名稱(諸如 IEC62351.LocalCA)。
- 個體憑證之一部分係包含裝置主體的主體(例：共同名稱(CN)或其他主體值)，其唯一地識別該個體。此個體名稱出現於個體之憑證中。亦參照 7.2。

該個體可使用其 IP 位址查詢其 DNS 名稱。個體可列出多個 `dnsName` 及對應之 IP 位址。IP 位址可於無 DNS 服務之環境中使用。

CSR 逾時參數係本地實作議題，若裝置未取得憑證，則該裝置將重新登錄。預期將由營運者之安全政策處理。

註冊資料應分別安裝並組態設定進各個體，以確保 RA 於執行 CSR 時能鑑別個體。

針對營運者 PKI 基礎建設網路中之登錄，應支援啟動碼(一次性唯一密碼)或製造者提供的憑證，此容許個體以 CA 自我鑑別。登錄期間使用之鑑別方法將取決於系統(部署之 PKI)能力。

需注意，可使用組態設定或工程工具人工執行個體組態設定。此組態設定亦可能受依 5.8.3 中安全參數所概述之加入協定所支援。

7.3.7 個體登錄

7.3.7.1 一般

一旦個體已以所須之註冊資料組態設定，並產生自有非對稱金鑰對，其應於開始運作前依組織的憑證安全政策執行 CSR 程序。針對憑證登錄要求對組織之 RA/CA 的線上連接，除非執行帶外登錄。

僅容許經註冊之個體於 RA/CA 處登錄(參照 7.3.5)。

針對人工登錄，個體應使用 PKCS #10 ([18])格式產生憑證簽署請求(CSR)。針對自動登錄，個體應將 CSR 提供予組態設定期間所規定之負責 RA。針對帶外登

錄，應使用任意方式將 CSR 傳送予負責之 RA/CA。RA 應藉由查證 PKCS #10 (CSR) 簽章，以查證對應私密金鑰之擁有證明，從而核對請求的有效性。

若請求有效，RA 將對對應之 CA 發送請求。CA 應產生公開金鑰憑證並將其提供予 RA，使得進一步配送予請求個體。用於 RA 及 CA 間通訊的協定超出本標準適用範圍。

若請求無效，則 RA 不應將任何請求發送予 CA。

備考：RA 及 CA 可能會作為 1 個個體一起部署。上述過程仍適用。

針對自動登錄，基礎建設(RA/CA)應支援下列登錄協定以與終端個體(登錄之客戶端)互動：

- 簡單憑證登錄協定(SCEP、RFC 8894)，用於聚焦於 RSA 式公開金鑰憑證之回溯相容。
- 透過安全傳送登錄(EST、RFC 7030)，用以支援 RSA 或 ECC 式公開金鑰憑證作為首選登錄協定。

使用自動登錄容許藉由利用啟動碼(OTP)，或已可用之憑證及對應的私密金鑰，連同 RA 上的註冊資料，證明識別資訊。

客戶端個體(登錄之個體)可支援至少 1 種登錄協定。

若登錄係受 TLS 保護，則建議使用本系列標準第 3 部中定義之 TLS 剖繪。若使用 TLS 保護登錄通訊之 PKI 功能介面能支援本系列標準第 3 部，則強烈建議使用。

憑證應依登錄協定中所規定傳送。關於憑證儲存，參照 7.3.2。

7.3.7.2 使用 SCEP 之個體登錄

SCEP 之應用應依循 RFC 8894 中所述之必備要求事項。支援 SCEP 之個體應支援該必備項目，以實作 RFC 8894 之 2.9 中所述的功能性：

- 查詢 CA 能力(GetCACaps)。
- CA 憑證之配送(GetCACert)。
- 憑證登錄(PKCSReq)。
- 憑證更新(RenewalReq)。

若成功執行使用 SCEP 之個體登錄，則應引發安全事件(“通知：使用 SCEP 之登錄成功執行”)。

若使用 SCEP 之個體登錄因錯誤而取消，則應引發安全事件(“錯誤：使用 SCEP 之登錄因錯誤而取消。”)。宜依 RFC 8894 提供詳細資訊。

7.3.7.3 使用 EST 之個體登錄

EST 之必備要求的功能支援對齊 RFC 7030 中所述的必備要求事項，連同新增憑證屬性檢索之必備支援。使用 EST 之個體應支援：

- 使用/cacerts 端點配送 CA 憑證，使得能依隱式信任錨查詢 CA 憑證。此功能性容許於初始情況下配送 CA 憑證以建立信任錨資料庫，亦可更新 CA 憑證。
- 經由 RA 處之/simpleteenroll 端點交換 SimplePKIRequest/Response (簡單登錄)，並經由 RA 處的/fullcmc 端點支援 FullPKIRequest/Response 交換。
- 使用 RA 處之 simplereenroll 端點重新登錄(憑證更新或重新產生金鑰)。

可選項支援 csrattrs (憑證屬性請求)訊息，以能查詢將於 CSR 中使用之 CSR 憑證屬性，以容許源自 RA/CA 側的明確要求事項。若登錄之個體已藉由其他方式(例：藉由組態)接收該資訊，則可省略該訊息。

要求 CSR 屬性請求/回應處理以支援簽署演算法及相關聯參數之選擇(金鑰長度、橢圓曲線式演算法的曲線選擇)。

實作者宜注意 IETF RFC 8951 關於針對傳送編碼及 ASN.1 之釐清。

若成功執行使用 EST 之個體登錄，則應引發安全事件(“通知：使用 EST 之登錄成功執行”)。

若使用 EST 之個體登錄因錯誤而取消，則應引發安全事件(“錯誤：使用 EST 之登錄因錯誤而取消。”)。宜依 RFC 7030 提供詳細資訊。

7.3.8 信任錨資訊更新

若支援自動更新信任錨資訊，則應依使用/cacerts 端點之既有信任錨，使用 EST (參照 7.3.7.3)執行信任錨憑證的更新。選項使用信任錨管理協定(TAMP)、RFC 5934 以執行信任錨更新。

若使用 TAMP，則應支援下列 TAMP 訊息：

- TAMP 狀態查詢：TAMP 狀態查詢訊息係用以請求有關目前安裝於信任錨儲存處中之信任錨的資訊，以及該儲存所屬之社群清單。
- TAMP 狀態查詢回應：TAMP 狀態回應訊息係信任錨儲存處對有效 TAMP 狀態查詢訊息之回覆。TAMP 狀態回應訊息提供有關目前安裝於信任錨儲存處中之信任錨資訊，以及信任錨儲存處所屬的社群清單(若有)。
- 信任錨更新：信任錨更新訊息係用以新增、刪除，以及變更管理及識別資訊信任錨。信任錨更新訊息無法用以更新頂級信任錨。
- 信任錨更新確認：信任錨更新確認訊息係信任錨儲存處對有效信任錨更新訊息之回覆。信任錨更新確認訊息提供各請求之更新的成功及不成功資訊。
- 頂級信任錨更新：頂級信任錨更新訊息取代運作之公開金鑰，且選項替換與頂級信任錨相關聯的緊急公開金鑰。各信任錨儲存處僅 1 個頂級信任錨。無任何限制事項與頂級信任錨相關聯。運作公開金鑰之公開金鑰識別符係用以識別後續 TAMP 訊息中的頂級信任錨。頂級信任錨更新訊息上之數位簽章依 RFC 使用目前運作的公開金鑰或目前緊急公開金鑰予以驗核。
- 頂級信任錨更新確認：頂級信任錨更新確認訊息係信任錨儲存處對有效頂級信任錨更新訊息之回覆。頂級信任錨更新確認訊息提供頂級信任錨更新之成功或不成功訊息。
- TAMP 錯誤：TAMP 錯誤訊息係信任錨儲存處對任何無效 TAMP 訊息之回覆。TAMP 錯誤訊息針對該錯誤提供原因之指示。

7.4 憑證組件及憑證查證

7.4.1 一般

個體憑證(包括公開金鑰憑證、屬性憑證及 CA 憑證)，應由依賴方查證。所有憑證組件應依循 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)。下列各節描述憑證組件及其查證。依憑證之查證結果，若發生錯誤，則將產生特定安全事件。建議使用憑證授權及驗核清單查證自我簽署憑證，依 7.8 中所述。

7.4.2 憑證格式及編碼

應查證憑證之正式結構。為此，依賴方應驗核 ASN.1 DER 編碼以及 ASN.1 憑證

結構的有效性。

若因解碼錯誤而無法處理憑證，則應引發安全事件(“警告：憑證格式不匹配。查證不成功。”)。

7.4.3 憑證簽章查證

公開金鑰憑證與屬性憑證之憑證簽章查證過程類似。於此兩者情況下，簽章係係於依由 AlgorithmIdentifier 所識別之 signatureAlgorithm 的憑證組件上計算。有關簽章演算法支援，亦參照 7.4.4.4。

若 TBSCertificate 上之公開金鑰憑證的簽章查證不成功，則應引發安全事件(“警告：無法查證公開金鑰憑證簽章”)。

若 TBSCertificate 上之屬性憑證簽章查證不成功，則應引發安全事件(“警告：無法查證屬性憑證簽章”)。

7.4.4 公開金鑰憑證組件

7.4.4.1 一般

公開金鑰憑證組件係依表 1 中所述內容。

7.4.4.2 Version(版本)

憑證之版本編號應為 2 (指示 X.509v3)。

若憑證版本與預期版本不匹配，則應引發安全事件(“錯誤：憑證版本錯誤。”)。

7.4.4.3 Issuer(核發者)

核發者組件識別核發憑證之 CA。其包含核發 CA 之區別名稱。核發者之區別名稱由作為主體組件的屬性組成(參照 7.4.4.6)。核發者組件係用於憑證路徑驗核過程(參照 7.4.4.8)。

備考：ISO/IEC 9594-8 | Rec. ITU-T X.509 之附錄 M 簡短簡介區別名稱。

若核發者與已知且受信任之核發者不匹配，則應引發安全事件(“錯誤：公開金鑰憑證授權。”)。

7.4.4.4 Signature(簽章)

宣稱符合本標準之實作應支援下列憑證簽署演算法的處理：

- RSA (亦參照 B.3.2)。

- ECDSA (亦參照 B.3.4)。

實作可支援 EdDSA (亦參照 B.3.5)。需注意，截至發布時，本系列標準尚未使用 EdDSA。若本系列標準中考量 EdDSA，則可於加密敏捷性之全景中見到選項支援。

相關聯參數係金鑰長度及所選擇之橢圓曲線，解釋如下。

應支援具 2048 位元金鑰之 RSA。金鑰長度 2048 係針對 RSA 簽章所支援之最小金鑰長度。依源自 NIST SP 800-131A Rev.2 [89]或 BSI TR01202-1 [58]之建議，強烈建議亦支援 3072 位元及更高之 RSA 金鑰長度，以因應密碼學的進步。1024 位元金鑰之 RSA 支援不宜用。其使用僅限於回溯相容。簽章演算法之選擇取決於組織的安全政策。

備考 1. 有關簽章演算法所要求金鑰長度之建議將不斷地審查，參照 NIST SP 800-57 或 BSI TR01202-1。

備考 2. 處理長 RSA 金鑰係過程費時，其針對受限制裝置可能是問題。然後可考量使用橢圓曲線加密(另參照 B.3)。針對 ECDSA，最小金鑰長度為 256 位元(與 SHA-256 組合)。將使用之 ecdsa-with-SHA256 的 OID 為：
1.2.840.10045.4.3.2 [iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2]。

用於 ECDSA 之曲線至少應為 secp256r1。此曲線之 OID 為：1.2.840.10045.3.1.7 [iso(1) member-body(2) us(840) ansi-X9-62(10045) curves(3) prime(1) prime256v1(7)]。

可使用下列曲線提供 ECDSA 之選項支援：

- brainpoolP256r1 (依 RFC 5639 中之定義); 此曲線之 OID 為：1.3.36.3.3.2.8.1.1.7 [iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecStdCurvesAndGeneration(8) ellipticCurve(1) versionOne(1) brainpoolP256r1(7)]。

IEC 62351-5:2023 要求支援另外 3 種曲線：

- Curve 22519 (依 RFC 7748 [43]中所定義)。
- Curve 448 (依 RFC 7748 [43]中所定義)。

- Secp256k1 (依[60]中所定義): 此曲線之 OID 為: 1.3.132.0.10 [iso(1) recognize-organization(3) certicom(132) curve(0) ansip256k1(10)]

需注意, 於本標準發布時, 對 Curve 22519 及 Curve 448 之支援僅適用於 ECDH 金鑰協定全景中之本系列標準(參照本系列標準第 5 部), 而非數位簽章全景。另需注意, 若用於數位簽章, Curve 22519 及 Curve 448 僅能於 EdDSA 中使用。

引用本標準之文件可能規定將支援的其他曲線。

若未支援所規定之 signatureAlgorithm, 則應引發安全事件(“錯誤: 未支援的簽章演算法”)。

7.4.4.5 Validity(有效性)

公開金鑰憑證之效期取決於組織的運作憑證(LDevID 憑證)的安全政策, 以及製造者之初始裝置憑證(IDevID 憑證)的安全政策。效期由 notBefore 及 not After 值所決定。依賴方應核對目前日期及時間是否於憑證的 notBefore 值與 notAfter 值之間。

- 若目前時間晚於 notAfter 值, 則應引發安全事件(“錯誤: 公開金鑰憑證逾期。”)。
- 若目前時間早於 notBefore 值, 則應引發安全事件(“錯誤: 憑證尚未有效。”)。

依 ITU-T X.509, 憑證有效性之值(不早於且不晚於)可能規定為 UTCTime, 直至 2049 年底。自 2050 年起, 此等值應規定為 GeneralizedTime。需注意, RFC 5280 要求將效期規定為 UTCTime, 直至 2049 年底。

備考: 為指示憑證未明確定義逾期日期, RFC 5280 使用 GeneralizedTime 值

99991231235959 作為 notAfter 值。

個體不應接受無效憑證, 例: 於依照本系列標準第 3 部中所要求建立 TLS 會談期間。

需注意, 需存取與國際原子時間(TAI)或 UTC 同步之時鐘, 以確保準確評估憑證的逾期日期。網路中準確之時間及時鐘同步通常由 NTP 或 PTP 協定所提供, 此等協定係分別定義於 RFC 5905 [38]或 IEEE 1588 [4]中。需注意, 針對 NTP, 安全選項目前已由 IETF 修訂為 NTS(網路時間安全, RFC 8915)(亦參照 7.7)。針對 PTP, IEEE 1588v2.1 定義安全選項, 以確保提供時序資訊之完整性保護。7.7

中概述時鐘同步之要求事項。

7.4.4.6 Subject(主體)

主體組件持有關於主體之區別名稱(DN)的資訊。應支援該組件。

若 subject 未包含或僅包含未知屬性，則應引發安全事件(“警告：主體未納入公開金鑰憑證。”)。

若選擇(核對)，則整個區別名稱或僅特定欄位之查證應匹配由組織安全政策所定義的容許識別符相符。亦可選擇省略主體與 CNS 62351-8 的 A 剖繪中所述之 RBAC 相關的查證。若於此情況下，則主體僅用以記錄目的。

針對運作憑證(LDevID 憑證)或製造者提供之憑證(IDevID 憑證)，主體組件的內容預期有所不同。運作憑證主體中使用之屬性內容係由運作者所定義。實作應至少能驗核並處理下列內容：

- CN：共同名稱，裝置之唯一識別符。需注意，若裝置具多個憑證，則其用途可能反映於 CN 中。
- O：可能指派裝置之組織名稱(例：運作者、製造者)。
- OU：組織單位名稱，包括組織之更多細節。
- C：負責之組織的國家代碼(CNS 12842)。

可規定額外屬性，例：由製造者針對製造者憑證(IDevID 憑證)所包含之特定裝置資訊(例：產品型式資訊)。

7.4.4.7 Subject Public Key Info(主體公開金鑰資訊)

subjectPublicKeyInfo 包含 2 個子組件，提供有關演算法(OID)以及憑證公開金鑰之資訊。

未能發現公開金鑰之匹配演算法應引發安全事件(“錯誤：未支援公開金鑰憑證中的原生公開金鑰演算法”)。

7.4.4.8 唯一識別符

IssuerUniqueIdentifier 及 subjectUniqueIdentifier 組件應不出現。X.509 中此等組件為不宜用。

7.4.4.9 憑證路徑驗核

依賴方應驗核以信任錨核發之 CA 憑證開始，以終端個體公開金鑰憑證結束的憑證路徑。作為特殊情況，終端個體公開金鑰憑證可由信任錨直接核發(通常稱為根 CA 憑證)。

若於本地組態中找不到與憑證相對應的信任錨，則應引發安全事件(“錯誤：未支援信任錨”)。

備考：通常，中間憑證係於協定訊息內傳送，如於 TLS 中。儘管如此，依賴方應能發現包含於本地組態中之根憑證。

所有憑證應由各自的核發 CA 正確簽署，而根憑證須為自我簽署。issuer 及 authorityKeyIdentifier 須分別等於路徑中下個憑證之主體名稱及 subjectKeyIdentifier。

沿著憑證路徑驗核憑證不成功應引發安全事件(“錯誤：無法查證憑證路徑。”)。

7.4.4.10 憑證延伸

7.4.4.10.1 一般

所有延伸應依循符合 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)：

- 若延伸係加旗標為關鍵，則公開金鑰憑證應僅能用於所規定目的之一。
- 若延伸係加旗標為非關鍵，則其指示意圖之金鑰用途。若出現此延伸，且依賴方識別並處理延伸型式，則依賴方應確保公開金鑰憑證僅用於所指示目的之一。若延伸係非關鍵且未知，則可忽略。

此外，包括未知關鍵延伸，或包含無法處理資訊之關鍵延伸的憑證應遭拒絕。

若憑證包含標記為關鍵之無法識別的延伸，則應引發安全事件(“錯誤：公開金鑰憑證中未知之關鍵延伸。”)。

若憑證於標記為關鍵之延伸中包含無法識別的資訊，則應引發安全事件(“錯誤：關鍵延伸中之未知資訊。”)。

7.4.4.10.2 機構金鑰識別符

AuthorityKeyIdentifier 包含核發 CA 憑證之 subjectKeyIdentifier。

若憑證中未包含 authorityKeyIdentifier，則應引發安全事件(“錯誤：公開金鑰憑證中未包含機構金鑰識別符。”)。

7.4.4.10.3 主體金鑰識別符

subjectKeyIdentifier 延伸容許識別包含特定公開金鑰之憑證。依 RFC 5280，核發 CA 憑證係屬必備，且於終端個體憑證中可選項支援。

若 subjectKeyIdentifier 未包含於 CA 憑證中，則應引發安全事件(“錯誤：主體金鑰識別符未包含於公開金鑰憑證中。”)。

7.4.4.10.4 主體替代名稱

若憑證中 subjectAltName 延伸係可用，則其應處理。其可包含憑證主體之 1 或多個替代名稱。

針對 TLS 伺服器憑證，至少須 1 個 subjectAltName，以匹配提供憑證之 TLS 伺服器之 dNSName (例：FQDN)或 IPAddress。

若鑑別 TLS 伺服器之憑證未包含 subjectAltName，則應引發安全事件(“錯誤：未包含主體替代名稱”)。

7.4.4.10.5 基本限制事項

basicConstraints 延伸識別憑證是否為 CA 憑證。若憑證係 CA 憑證，則延伸應標記為關鍵。針對終端個體，建議省略延伸名稱。

針對核發 CA，應提供 2 個組件：

- cA：應設定為 true。需注意，此亦要求將金鑰使用設定為 keyCertSign：參照 7.4.4.10.6。
- pathLenConstraint 依組織的安全政策可用以限制憑證路徑之長度。

若 CA 憑證中未提供 basicConstraints 延伸，則應引發安全事件(“錯誤：CA 憑證中未包含基本限制事項。”)。

若於憑證路徑上之 CA 憑證中提供並使用 pathLenConstraint 組件並將其設定為 0，則下列憑證應為終端個體憑證。若下列憑證並非終端個體憑證，則應引發安全事件(“錯誤：違反 CA 憑證中的路徑長度限制事項。”)。

符合本標準之實作應支援最小 pathLenConstraint 為 2，從而容許 2 個中間 CA。

7.4.4.10.6 金鑰使用

keyUsage 延伸係關鍵性延伸，應進行查證。其識別公開金鑰憑證之意圖使用，如

digitalSignature、keyAgreement 或 keyEncipherment。

TLS 全景中之金鑰使用：

- digitalSignature

- 應針對 TLS 客戶端憑證設定。
- 若使用簽章式密碼套組，則應針對 TLS 伺服器憑證設定。

若鑑別 TLS 客戶端或 TLS 伺服器之憑證，係與須於 TLS 交握手中數位簽章的密碼套組結合使用，用以金鑰協商，但未包含 digitalSignature 之金鑰使用，則應引發安全事件（“錯誤：未包括數位簽章的金鑰使用法。”）。

- 若使用金鑰傳送式密碼套組，則應針對 TLS 伺服器憑證設定 keyEncipherment。

若鑑別 TLS 伺服器之憑證係與金鑰協定的 TLS 交握中公開金鑰加密之密碼套組結合使用，未包含 keyEncipherment 的金鑰使用，則應引發安全事件（“錯誤：未包含金鑰加密的金鑰使用”）。

PKI 運作全景中之金鑰使用：

- keyCertSign 應設定用於核發 CA 之核發憑證。若核發憑證未包含 keyCertSign 資訊，則應引發安全事件（“錯誤：簽署憑證未包含金鑰使用。”）。
- 對 CRL 簽章應設定為 cRLSign。若用以簽署 CRL 之憑證未包含 cRLSign 使用資訊，則應引發安全事件（“錯誤：未包括用於簽署 CRL 之金鑰使用。”）。
- 若鑑別之 AA 係由 CA 所核發，則應針對核發 AA 設定 digitalSignature。亦應設定 SCEP 全景中所使用之 CA 憑證，因於 SCEP 全景中，回應訊息係由 SCEP CA 所簽署。

7.4.4.10.7 延伸金鑰使用

若延伸金鑰可用，則應查證 extendedKeyUsage 延伸。其識別公開金鑰憑證使用之額外目的(此組件的支援係屬選項，取決於使用案例)。

TLS 憑證全景中之延伸金鑰使用：

- 應針對 TLS 伺服器憑證設定 serverAuth。若 TLS 伺服器憑證中未包含 serverAuth 資訊，則應引發安全事件（“錯誤：TLS 伺服器未包含延伸金鑰使用。”）。

- 應針對 TLS 客戶端憑證設定 clientAuth。若 TLS 客戶端憑證中未包含 clientAuth 資訊，則應引發安全事件(“錯誤：TLS 客戶端未包含延伸金鑰使用。”)。

PKI 運作全景中之延伸金鑰使用：

- 應針對簽署 OCSP 回應應設定 OCSPSigning (1.3.6.1.5.5.7.3.9 - OCSPSigning)。若用以簽署 OCSP 回應之憑證中未包含 OCSPSigning 資訊，則應引發安全事件(“錯誤：OCSP 簽署未包括延伸金鑰使用。”)。

系統運作全景中之延伸金鑰使用：

- AVL 簽署(avlSign)：若設定，則對應之私密金鑰可用以簽署 AVL。授權者使用其私密金鑰簽署將提交予 AVL 個體之 AVL。對應之公開金鑰憑證應包含值為 id-avlSign (= 2.5.38.2)之延伸金鑰使用延伸。此延伸金鑰使用延伸及 id-avlSign 值定義於 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)之 9.2.2.4 中。若用以簽署 AVL 之憑證中未包含 id-avlSign 資訊，則應引發安全事件(“錯誤：未包括用以簽署 AVL 之延伸金鑰使用。”)。

7.4.4.10.8 授權及驗核延伸

ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)之 9.2.2.8 中規定授權及驗核延伸。公開金鑰憑證中存在此延伸表示：僅該延伸應能成功核對特定 AVL，延伸方視此公鑰憑證為有效。AVL 之處理係由運作者負責。

若使用，則此延伸應恆加旗標為關鍵。

僅於須驗核此公開金鑰憑證之所有個體係由相同授權者所管理時，方宜使用此延伸(ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)中未提及此限制)。

7.4.4.10.9 CRL 配送點

cRLDistributionPoints 延伸識別依賴方可存取 CRL 配送清單之 CRL 配送點。CRL 之檢索由 CRL 配送清單中所述的協定規定，且於本標準的全景中可為 HTTP 或 LDAP。

符合本標準之核發 CA 須於此延伸中提供 CRL 配送點資訊。支援符合本標準之 CRL 的各終端個體實作，應能利用所包含之資訊自 CRL 配送點擷取撤銷資訊。

符合本標準之實作(核發 CA 及支援 CRL 的終端個體)，應支援使用 HTTP 作為傳

送協定檢索 CRL。預設之方法係 HTTP GET。

需注意，針對憑證相關運作，選項 LDAP 可能使用於已適用 LDAP 之環境中。當支援使用 CNS 62351-8 中定義之 A 剖繪或 B 剖繪的 PULL 模型之 RBAC 時，可能為此情況。若所使用之登錄協定及營運者 PKI 支援 CRL 擷取，則其亦可使用。

備考：CRL 自身係自給自足(數位簽署)，且能獨立於傳送安全而傳輸。

若 CRL 係由依賴方用以憑證撤銷核對，且所接收憑證中未包含 CRL 配送點(CDP)資訊，則應引發安全事件(“警告：公開金鑰憑證中未包含 CRL 配送點”)。

7.4.4.10.10 機構資訊存取

AuthorityInformationAccess 延伸指示如何存取憑證機構之資訊及服務。具體而言，此擴展可能包含 OCSP 回應者之存取資訊(回應者負責提供有關包含該延伸之憑證的撤銷狀態資訊)。於本標準全景中，要求 OCSP 回應者之支援資訊，依 RFC 5280 中所規定。

符合本標準之核發 CA 須提供關於由存取方法 id-ad-ocsp 所指示 OCSP 配送點的資訊。

符合支援 OCSP 之本標準的終端個體實作，應能利用所包含資訊自使用 OCSP 之 OCSP 回應者擷取撤銷資訊。

若所接收憑證中未包含 OCSP 回應者資訊，則應提供安全事件(“警告：公開金鑰憑證中未包含 OCSP 回應者資訊”)。

7.4.4.10.11 RBAC 延伸

CNS 62351-8 定義延伸 IECUserRoles，用以載送與主體相關之資訊(涉及主體可能扮演的角色)，以及提供更多關於使用角色之資訊(如責任範圍)的額外屬性。有關延伸的定義以及驗核，參照 CNS 62351-8 之 A 剖繪。

7.4.4.10.12 AVL 配送點延伸

AVL 係與營運者相關之本地議題，且核發 CA 可能未知悉。因此，AVL 配送點之處理係本地實作議題，且可透過例如組態設定所完成。ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)中提供管理 AVL 之協定。

7.4.4.10.13 SOA 識別符延伸

ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)中描述 sOAIentifier 延伸，並指示公開金鑰憑證主體可扮演機構來源(SOA)。依此，公開金鑰憑證主體可使用私密金鑰核發對持有者指派權限之屬性憑證。

核發 CA 負責設定此延伸。若 CA 核發 AA 憑證，則應包含此延伸。其容許 CA 與 AA 間具緊密繫結。

除 sOAIentifier 延伸外，AA 亦需指派金鑰使用 digitalSignature 以核發屬性憑證。

於本標準全景中，僅容許 CA 核發包含 SOA 識別符之 AA 憑證。

7.4.5 屬性憑證組件

7.4.5.1 一般

屬性憑證組件係依 7.2.2 表 2 所述之內容。若屬性憑證或其組件之一無法查證，則持有者應視為不具特定角色。

7.4.5.2 Version(版本)

屬性憑證之 version 組件應為 1 (指示 v2)。

若憑證版本與預期之版本不匹配，則應引發安全事件(“錯誤：屬性憑證版本錯誤”)。

7.4.5.3 Holder(持有者)

holder 組件應傳遞屬性憑證持有者之識別資訊。依 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)不同組件，於此係屬可能。符合本標準之實作應支援下列評估：

- baseCertificateID 組件。若出現，則其識別特定之公開金鑰憑證，其係用以當以此屬性憑證宣稱特殊權限時，依 issuer 的區別名稱及持有者公鑰憑證之 serialnumber，鑑別持有者的身分。依 RFC 5755，公開金鑰憑證應具非空值核發者區別名稱，其須出現於 holder.baseCertificateID.issuer 組件之 directoryName 欄位中。
- entityName 組件。若出現，則持有者鑑別係藉由公開金鑰憑證以外之其他方式完成。

備考：RFC 5755 亦容許依 `entityName` 中將包含之 `subject` 或 `subjectAltName`，以識別公開金鑰憑證的持有者。本標準中採用更嚴格之作法，並簡化依公開金鑰憑證的持有者鑑別與其他型式持有者鑑別間的區別。

- `entityName` 之屬性係於由運作者定義。需注意，依 CNS 62351-8，持有者可能與人類使用者或技術使用者（例：應用）相關。實作應準備接收並處理 `entityName` 中至少下列屬性之一：

- `otherName`：由 OID 及對應值所識別之任何形式的替代持有人名稱。

- `directoryName`：依 ITU-T X.501 | ISO/IEC 9594-2 之持有人的區別名稱。

依循 RFC 5755 中提供的建議，此規格要求屬性憑證中應僅包含組件之一。另外，於使用 `entityName` 之情況下，應僅提供該組件之 1 個屬性。此係為避免混淆，哪個組件係處理為規定性。

若持有者鑑別係依對應之公開金鑰憑證所完成，則應查證憑證，依 7.4.4 中所描述。

若無法依對應之公開金鑰憑查證持有者，則應引發安全事件（“警告：無法依公開金鑰憑證查證屬性憑證的持有者。”）。於此情況下，持有人應視為不具特定角色。

若藉由其他方式完成持有者鑑別，則於查證屬性憑證之前，鑑別程序應已成功完成。

若持有者無法依替代之非公開金鑰憑證式鑑別查證，則應引發安全事件（“警告：無法依替代鑑別查證屬性憑證的持有者。”）。於此情況下，持有人應視為不具特定角色。

7.4.5.4 Issuer(核發者)

`issuer` 組件識別核發屬性憑證之 AA。其包含核發 AA 之區別名稱。依循 RFC 5755，其應僅於核發者組件之 `DirectoryName` 欄位中包含單一區別名稱。

依 RFC 5755，可藉由組態或其他方式信任 AA。

若核發者不匹配組態設定之已知且受信任核發者，則應引發安全事件（“錯誤：屬性憑證核發者不受信任(未組態設定)。”）。

於本標準全景中，「其他方式」係由營運者之核發 AA 及核發 CA 的緊密整合所提供。於此情況下，CA 可能核發 AA 憑證。屬性憑證之查證者應查證核發的 AA 憑證：

- 包含 sOAIdentifier (亦參照 7.4.4.10.13)。
- 包含金鑰使用 digitalSignature (亦參照 7.4.4.10.6)。
- 係由受信任 CA 所核發。

若依延伸查證及 AA 憑證之核發者，無法將 AA 查證為受信任核發者，則應引發安全事件(「錯誤：屬性憑證核發者不受 (受信任之 CA)信任。」)。

7.4.5.5 Signature(簽章)

signature 包含用以驗核屬性憑證簽章之演算法識別符。針對屬性憑證，適用相同於 7.4.4.4 中概述之公開金鑰憑證的條件。

7.4.5.6 Attribute(屬性)

attributes 組件包含與持有者相關之屬性。

針對電力系統，CNS 62351-8 定義 IECUserRoles 之屬性值及型式，用以載送與主體相關涉及主體可能扮演的角色之資訊，以及提供有關使用角色的更多資訊之額外屬性，如責任範圍。有關屬性之定義以及驗核，參照 CNS 62351-8 的 B 剖繪。

7.4.5.7 attrCertValidityPeriod

屬性憑證之效期取決於組織的安全政策。效期係由「not before」及「not after」值所判定。依賴方應核對目前日期及時間是否於憑證之 notBeforeTime 與 notAfterTime 值之間。

- 若目前時間晚於 notAfterTime 值，則應引發安全事件(「錯誤：屬性憑證逾期。」)。
- 若目前時間早於 notBefore 值，則應引發安全事件(「錯誤：屬性憑證尚未生效。」)。

相較於 RFC 5280，針對屬性憑證之 RFC 5775 要求 not before 及 not after 的值應恆規定為 GeneralizedTime。

備考：為指示憑證無明確定義之逾期日期，RFC 5280 使用 GeneralizedTime 值

99991231235959 作為 notAfter 值。

7.4.5.8 屬性憑證延伸

7.4.5.8.1 一般

針對屬性憑證 AC 所定義之延伸，提供將額外屬性與持有者相關聯的方法。

若屬性憑證包含標記為關鍵之無法辨識的延伸，則應引發安全事件(“錯誤：屬性憑證中未知之關鍵延伸。”)。

若憑證於標記為關鍵之延伸中包含無法辨識的資訊，則應引發安全事件(“錯誤：屬性憑證關鍵延伸中無法辨識之資訊。”)。

若憑證包含無法辨識之延伸，則應引發安全事件(“警告：屬性憑證中的未知延伸。”)。

7.4.5.8.2 機構金鑰識別符

AuthorityKeyIdentifier 可納入屬性憑證，且係旨在協助屬性憑證查證者核對核發 AA 之屬性憑證簽章。

若 authorityKeyIdentifier 包含於屬性憑證中但無法查證，則應引發安全事件(“錯誤：屬性憑證中之機構金鑰識別符無法查證。”)。

7.4.5.8.3 屬性憑證撤銷處理

屬性憑證係旨在暫時增強持有者之屬性。其簽發效期可能很短。

若組織之安全政策容許短的效期而無須撤銷，則應藉由使用 noRevAvail (無撤銷可用)延伸指示。於此情況下，不應設定 CRL 配送點及機構資訊存取延伸。

若所接收之屬性憑證中包含 noRevAvail 資訊，則應提供安全事件(“通知：屬性憑證中無意圖的撤銷資訊”)。

處理 CRL 配送點延伸(參照 7.4.4.10.9)及機構資訊存取延伸(參照 7.4.4.10.10)，依循相同於公開金鑰憑證之方法，但引用 AA 而並非 CA。

若組織之安全政策要求撤銷資訊，則符合本標準的核發 AA 應於 cRLDistributionPoints 延伸中提供 CRL 配送點資訊，並於 authorityInformationAccess 延伸中提供關於 OCSP 配送點的資訊。

符合支援 CRL 之本標準的終端個體實作，應能利用所包含資訊自 CRL 配送點擷取撤銷資訊。

符合本標準之實作(核發 CA 及支援 CRL 的終端個體)，應支援使用 HTTP 作為傳送協定以檢索 CRL。預設之方法為 HTTP GET。

需注意，針對憑證相關運作，選項 LDAP 可於已適用 LDAP 之環境中使用。當支援使用 CNS 62351-8 中定義之 A 剖繪或 B 剖繪的 PULL 模型之 RBAC 時，可能發生此情況。

備考：CRL 自身係自給自足(數位簽署)，且能獨立於傳送安全而傳輸。

若 CRL 係由依賴方用於憑證撤銷核對，且若所接收屬性憑證中未包含 CRL 配送點(CRLDP)資訊，則應提供安全事件(“警告：屬性憑證中未包含配送點”)。

符合支援 OCSP 之本標準的終端個體實作，應能利用所包含之資訊自使用 OCSP 的 OCSP 回應者擷取撤銷資訊。

若所接收之屬性憑證中未包含 OCSP 回應者資訊，則應提供安全事件(“警告：屬性憑證中未包含 OCSP 回應者資訊”)。

7.4.6 憑證撤銷狀態

宣稱符合本標準之實作應能核對所接收憑證的撤銷狀態。若憑證撤銷核對係為正，則應引發安全事件(“告警：憑證已遭撤銷。”)。若可用，可於安全事件中新增撤銷原因。ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)中所定義之可能原因代碼為：

- unspecified (0),
- keyCompromise (1),
- cACompromise (2),
- affiliationChanged (3),
- superseded (4),
- cessationOfOperation (5),
- certificateHold (6),
- removeFromCRL (8)。
- privilegeWithdrawn (9)。
- aACompromise (10)。

- weakAlgorithmOrKey (11)。

CRL 之提供係屬本地事務，且可能於本地(檔案式)完成，或取決於憑證中 CRL 配送點組件中的 URI 資訊完成，並可使用 HTTP 或 LDAP (依 7.4.4.10.9 中所述)。

CRL 不可用應引發安全事件(“警告：CRL 配送點非可存取”)。

CRL 逾期應引發安全事件(“警告：CRL 逾期”)。

驗核 CRL 簽章不成功應引發安全事件(“警告：CRL 簽章無法查證”)。

或者，個體可使用線上憑證狀態協定(OCSP)查證憑證之撤銷狀態。

若 OCSP 係用以取得已接收憑證之 OCSP 回應，以執行憑證撤銷核對，則依賴個體應使用 Authority Info Access 延伸之 id-ad-ocsp accessMethod 的 accessLocation 欄位提供之 URI，以查詢 OCSP 回應者的同級憑證。可能出現不同錯誤狀況：

- 個體無法存取 OCSP 回應者，應引發安全事件：(“警告：OCSP 回應者無法存取”)。
- 自個體至 OCSP 回應者之連接回應逾時，應引發安全事件：(“警告：OCSP 回應者連接逾時”)。需注意，此可能與正常之 TCP/IP 逾時相關，亦可能係由阻絕服務攻擊引起。
- 若 OCSP 回應者未知悉請求訊息中之憑證，則其將以憑證狀態值“未知”回應。此情況將引發安全事件(“警告：OCSP 回應者未知悉憑證”)。需注意，此可能指示此回應者不服務之無法識別的核發者。

個體上之 OCSP 回應逾期，應引發安全事件(“警告：OCSP 回應逾期”)。

驗核 OCSP 回應訊息簽章不成功，應引發安全事件(“警告：無法查證 OCSP 回應簽章”)。

依 7.4 所述，組織之安全政策決定對安全事件的最終反應。個體不應接受遭撤銷之憑證，例：如於本系列標準第 3 部之要求建立 TLS 會談期間。

7.5 憑證撤銷

個體之憑證至少應於下列條件下撤銷，使用 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)的 9.5.3.1 中所規定之原因代碼：

- 個體之私密金鑰遭破解。
- CA 遭破解。
- 個體之隸屬關係已變更。
- 個體之生命結束。

組織之撤銷政策可能提供撤銷憑證的額外原因。無須要求撤銷已更新或逾期之憑證。

提供撤銷資訊係針對 PKI 環境之要求，而非特定個體的要求。

公開金鑰基礎建設(PKI)應至少支援下列 2 種安全撤銷方法：

- 憑證撤銷清單(certificate revocation lists, CRL)。
- 線上憑證狀態協定(online certificate status protocol, OCSP)。

PKI 應至少每 24 小時傳播一次撤銷資訊(此可能有所不同，取決於組織之 PKI 政策、特定裝置的重要性，以及同級連接之數量)。

個體應支援 CRL 或 OCSP 或兩者以擷取撤銷資訊。執行憑證查證核對須撤銷資訊。需注意，於選擇撤銷方法(CRL 或 OCSP)時需抉擇。選擇取決於標的裝置及標的環境。

- CRL 可能變大，且可能無法由受限制之 IED 處理。該處理包括 CRL 之初始查證，亦包括資訊的儲存，直至下次 CRL 更新。CRL 通常每 24 小時擷取一次。製造者可宣告所支援 CRL 之最大大小。
- 支援 OCSP 之 IED 須處理各憑證的 OCSP 回應(包括查證及快取)。此可要求與 OCSP 回應者更頻繁之通訊，以擷取所接收憑證的 OCSP 回應。需注意，OCSP 回應之快取(由組織的安全政策處理)，可減少與 OCSP 回應者的通訊，但可增加 OCSP 回應快取之本地儲存需要。

備考：CRL、CRL 更新或 OCSP 回應者不可用時之系統行為，預期於本系列標準的另一部中定義或作為組織安全政策之一部分。

7.6 憑證逾期及更新

本標準既未規定公開金鑰憑證之最小及最大生命期。宜取決於憑證型式及本地安全政策選定憑證逾期日期(參照 7.3.4)。

公開金鑰憑證選項包括私密金鑰使用延伸，其規定其擁有者可使用對應私密金鑰之期間。此期間通常設定為短於憑證效期，以確保憑證於其擁有者使用後於最短期限內保持有效。ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)之 9.2.2.5 中簡介有關私密金鑰使用延伸的使用細節。

個體於其公開金鑰憑證逾期日期接近憑證效期結束日期後，應產生新的金鑰對，並於具 PKI 之環境中執行 CSR。需注意，處理通常由組織之憑證政策所規定。個體應於其公開金鑰憑證逾期之前更新其公開金鑰憑證，並應存錄其公開金鑰憑證更新動作(作為成功或不成功事件)。

個體應容許組態設定公開金鑰憑證更新政策，諸如：

- 是否支援自動更新。
- 公開金鑰憑證逾期前應進行更新之時間長度。

7.7 時鐘同步及準確度

應確保時鐘同步及準確度，以容許可靠的查證憑證有效性資訊。

因此，時間同步至關重要，強烈建議實作時間同步協定之安全選項：

- 若 PTP (IEEE 1588v2.1)係用於時間同步，則宜使用整合安全選項。需注意，針對 IEC 61850 變電所自動化，CNS 15733-9-3/IEEEc37.248 中定義 PTP 剖繪。另需注意，安全將包含於該剖繪的下個版本中。
- 若 NTP 係用於時間同步，則宜考量應用 NTS (網路時間安全，RFC 8915)。
- 或者，可使用其他安全協定以確保時間同步。

7.8 授權及驗核清單

7.8.1 一般

AVL 及關聯協定之支援係屬選項，但若使用則應滿足 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)，以及 ISO/IEC 9594-11:2020 | Rec. ITU-T X.510 (2020)中的要求事項，如下：

- ISO/IEC 9594-08:2020 | Rec. ITU-T X.509 (2019)之第 11 節規定 AVL。
- ISO/IEC 9594-11:2020 | Rec. ITU-T X.510 (2020)之第 8 節至第 12 節規定針對其他協定提供安全封裝協定。

- ISO/IEC 9594-11:2020 | Rec. ITU-T X.510 (2020)之第 13 節規定授權及驗核管理協定(AVMP)，用於授權者與其所支援 AVL 個體間的通訊。其利用封裝協定之服務。
- ISO/IEC 9594-11:2020 | Rec. ITU-T X.510 (2020)之第 14 節規定 CA 訂用協定(CASP)。授權者使用該協定自相關 CA 訂用公開金鑰憑證狀態資訊。此協定僅由授權者於受限制環境中使用(參照 5.11.3)。終端個體亦可使用此協定作為取得公開金鑰狀態資訊之替代方式。此協定要求更新 CA 以支援 CASP 協定及關聯能力。

7.8.2 公開金鑰憑證之授權及驗核清單(AVL)語法

ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)之第 11 節中描述 TBSCertAVL 資料型式的不同組件。下列僅描述與電力系統相關之特定 AVL 層面：

- 提供 serialNumber 組件係藉由容許授權者於 AVL 個體中置放多個 AVL，以容許更先進之功能性。多個授權者亦可能將 1 或多個 AVL 置放於相同 AVL 個體中。
- constrained 組件應取值 FALSE，以指示 AVL 個體為非受限制 AVL 個體。宜設定此值，直至 CA 支援公開金鑰憑證狀態訂用為止。
- 針對各公開金鑰憑證及/或由 AVL 表示之個體群組，entries 組件應持有元素。各元素應規定如下：

idType 組件應採取下列 2 個替代方案之一：

- 若採用 certIdentifier 替代方案，則應識別此資料項所表示之特定公開金鑰憑證。此可藉由規定 CA 核發者名稱連同公開金鑰憑證序號所完成，或可藉由公開金鑰憑證之特徵或僅藉由公開金鑰所識別。若公開金鑰憑證係自我簽署憑證，則可僅使用特徵識別公開金鑰憑證。
- 若採用 entityGroup 替代方案，則應持有該群組中所有個體共有之區別名稱部分。此替代方案僅適用於非約束環境。

AVL 之進一步延伸為：

- EntryExtensions 組件(若出現)應持有 1 或多個特定於相關資料項之延伸。7.8.3

至 7.8.6 中規定之延伸可包含於此。若特定延伸型式係用作資料項延伸，則其不應納入 `avlExtensions` 組件中。

- `avlExtensions` 組件(若出現)應持有 1 或多個適用於 AVL 中資料項之延伸。7.8.3 至 7.8.6 中規定之延伸可包含於此。若此處包含特定延伸型式，則其不應出現於任何資料項之 `entryExtension` 組件中。

需注意，延伸可新增至個別資料項及整個 AVL 中。此種延伸規定於 7.8.3 至 7.8.6 中。

7.8.3 AVL 範圍限制

AVL 範圍旨在限制公開金鑰憑證之適用性。於某些情境下，可能亦需將範圍納入公開金鑰憑證中作為選項延伸。實際範圍限制事項係以分別之型式定義。此亦容許分別使用限制事項。

`scopeConstraints` 延伸語法定義為：

```
scopeConstraints EXTENSION ::= {
  SYNTAX      ScopeConstraints
  IDENTIFIED BY { avl62351Extion 1 } }
```

```
ScopeConstraints ::= SEQUENCE Of (SIZE (1..MAX)) OF ScopeConstraint
```

```
ScopeConstraint ::= SEQUENCE {
  - contains the scope information
  aor UTF8String (SIZE(1..64)),
  -- Def. of "Area of Responsibility" of CA cert
  revision INTEGER (0..255) OPTIONAL
  - optional revision if aor changes
}
```

責任區域(area of responsibility, aor)限制公開金鑰憑證之適用性於某些地理或組織區域。本標準定義 aor 之欄位及格式如下：

欄位名稱	編碼，最大長度(位元組)	示例
Area of responsibility (責任區域)	UTF8，64	BAVARIA.DE

aor 係識別符，定義階層命名空間或對命名空間之參引。需注意，此等識別符通常為文數字。aor 將依政策提供，例：由負責之運作者提供。

備考：已於 CNS 62351-8 中引入描述地理或組織限制之 aor (或範圍)概念，並於此重複使用。

7.8.4 AVL 協定限制延伸

ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)之 9.7.2 中定義 AVL 協定限制資料項延伸。其係用以列舉與個體(或 **entityGroup** 之多個個體)通訊時容許使用的相關聯協定。若省略此 AVL 資料項延伸，則對將採用協定之型式無限制。

協定應由規定該協定之通訊標準所識別。物件識別符應依循規定於 ISO/IEC 9834-1 | Rec. ITU-T X.660 之 A.2 及 A.4 中的政策。

例：ISO 61850-8-1 係由下列物件識別符所表示：

```
{ iso(1) standard(0) iec61850(61850) series(8) part(1) }
```

備考：ISO/IEC 9834-1 | Rec. ITU-T X.660 不考量標準編號由 3 個項目組成之情況。此示例顯示本標準所使用之記法。

```
id-P-IEC61850-T    OBJECT_IDENTIFIER ::= { id-IEC62351prot 1 }
id-P-IEC61850-A    OBJECT_IDENTIFIER ::= { id-IEC62351prot 2 }
id-P-IEC60870-5-T  OBJECT_IDENTIFIER ::= { id-IEC62351prot 3 }
id-P-IEC60870-5-A  OBJECT_IDENTIFIER ::= { id-IEC62351prot 4 }
id-P-IEC62325-T    OBJECT_IDENTIFIER ::= { id-IEC62351prot 5 }
id-P-IEC62325-A    OBJECT_IDENTIFIER ::= { id-IEC62351prot 6 }
id-P-IEEE1518-T    OBJECT_IDENTIFIER ::= { id-IEC62351prot 7 }
id-P-IEEE1518-A    OBJECT_IDENTIFIER ::= { id-IEC62351prot 8 }
```

7.8.5 憑證及相關聯識別符之 AVL pinning

此 AVL pinningId 資料項延伸提供獨特識別符與公開金鑰憑證之關聯。此識別符很可能為 IP 位址，但亦可能為其他識別符。於某些使用案例中，公開金鑰憑證僅能於專屬 IP 位址上使用。若憑證自身未提供 IP 位址資訊作為 subjectAltName 延伸之一部分，則 pinningId 延伸支援將憑證與 IP 位址(或其他識別符)關聯。

```
pinningId EXTENSION ::= {
    SYNTAX PinningId
    IDENTIFIED BY { avl62351Extion 2 } }
PinningId ::= GeneralNames
GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
GeneralName ::= CHOICE {
    otherName                [0] OtherName,
    rfc822Name                [1] IA5String,
    dNSName                   [2] IA5String,
    x400Address               [3] ORAddress,
    directoryName              [4] Name,
    ediPartyName               [5] EDIPartyName,
    uniformResourceIdentifier  [6] IA5String,
    iPAddress                  [7] OCTET STRING,
    registeredID               [8] OBJECT IDENTIFIER,
```

... }

ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)之 9.3.2.1 中定義 GeneralNames 資料型式，並描述 GeneralName 之替代方案。為易於參引，GeneralNames 資料型式複製至此。

iPAddress 應以“網路位元組序”儲存於八位元組串中，依 RFC 791 中之規定。各八位元組之最低有效位元(LSB)係網路位址中對應位元組之 LSB。針對 IPv4 (依 RFC 791 中所規定)，八位元組串應恰好包含 4 個八位元組。針對 IPv6 (依 RFC 2460 中所規定)，八位元組串應恰好包含 16 個八位元組。

7.8.6 AVL 使用相關之公開金鑰憑證延伸

特別是若 AVL 係用於 PKI 全景中，則建議使用某些公開金鑰憑證延伸。需注意，若使用自我簽署憑證，則此等延伸之包含於實務上可能無法強制執行。與 AVL 相關之公開金鑰憑證延伸描述於 7.4 中，亦即：

- 7.4.4.10.8 中之授權及驗核延伸。
- 7.4.4.10.7 中之用以核發 AVL 的延伸金鑰使用。

AVL 配送點係由營運者處理，核發 CA 可能不知悉。若使用 AVL，則可透過組態提供此資訊。

7.8.7 AVL 之核發

核發 AVL 係專屬電力系統營運者(授權者)之責任。預期 AVL 將依特定系統部署的工程資料編譯。依工程資料，通訊關係以及通訊個體間所使用之協定係已知。假設個體特定之公開金鑰憑證已可用，則可同時編譯 AVL。若個體特定群組件於工程時不可用，則核發憑證之 CA 可使用工程資訊組態設定，並於登錄期間將該資訊提供予個體。

需注意，若系統中之通訊同級方變更，則需更新 AVL。若系統之組件遭移除、更新或新引入，則可能發生此情況。假設至少組件之移除或引入係伴隨著工程設計。

7.8.8 AVL 之端點處理

於連接建立期間(例：TLS 交握期間)查證所接收公開金鑰憑證之過程、公開金鑰憑證自身的驗核，以及針對本地可用 AVL 之核對，係概述於 ISO/IEC 9594-8：

2020 | Rec. ITU-T X.509 (2019)。

8. 群組式金鑰管理(規定)

8.1 GDOI 要求事項

5.6.4.2 中提供 GDOI 之概觀參考。

應使用 RFC 6407-The Group Domain of Interpretation (GDOI) 方法及 RFC 8052(“GDOI Protocol Support for IEC 62351 Security Services”)，將群組金鑰配送予群組成員(GM)。GROUPKEY-PULL 方法之係屬必備支援，而 GROUPKEY-PUSH 則屬選項。

GDOI 定義 GROUPKEY-PUSH 之應用，以將控制資訊發送予群組成員。例：此關係既有安全關聯(SA)之重新產生金鑰的實例，但亦關係群組成員的變更。為能確認接收自 GCKS 之資訊，RFC 8263 中規定 GROUPKEY-PUSH 認可訊息。使用連線建立時交換之 GDOI 客戶端公開金鑰憑證信符，進行群組成員鑑別的能力係屬必備。

KDC 應於安全位置維護金鑰及相關聯參數之儲存庫。

KDC 應組態設定會期金鑰更新政策，其應係依金鑰生存期。

需注意，每當提及公開金鑰(於 GDOI 中)，其係意指作為憑證之一部分。公開金鑰具對應之私密金鑰，其被部署以產生簽章。

8.2 網際網路金鑰交換第 1 版(IKEv1)

GDOI RFC 6407 提供 ISAKMP 實作，其中 GDOI 係新 ISAKMP 解譯領域(DOI)。RFC 6407 定義如何將 IKEv1 (RFC 2409)用作 GDOI 之階段 1 協定。KDC 應使用 IKEv1 作為其 GDOI 階段 1 協定。KDC 無需支援 IKEv1 之所有功能及特徵，但至少應支援表 3 中列出的 IKEv1 要求事項。需注意，容許針對 IKEv1 及 IKEv2 之 ECDSA 應用的其他鑑別演算法，定義於 RFC 4754 [32]中。

表 3 KDC IKEv1 要求事項

說明	值
所支援之 ISAKMP 交換。	2 - 主模式(ID 保護)。 5 - 參考性。

說明	值
所支援之 GM ID 酬載型式。	9 - ID_DER_ASN1_DN (GM 識別資訊憑證之主體 ID)。
所支援之金鑰交換	經由群組說明屬性之 Diffie-Hellman (參照下文)。
伺服器 IP 埠	UDP 848 (可組態設定)。
1 - 加密演算法屬性	7 - AES-CBC (金鑰長度：128/256)。
2 - 雜湊演算法屬性	4 - SHA2-256。 5 - SHA2-384。 6 - SHA2-512。
3 - 鑑別方法屬性	2 - DSA 簽章。 3 - RSA 簽章(必備)。 9 - 具 P-256 曲線上 SHA-256 之 ECDSA (RFC 4754)。
4 - 群組說明屬性	14 - MODP-2048。 15 - MODP-3072。 16 - MODP-4096。 17 - MODP 6144 (RFC 3526)。 18 - MODP-8192 (RFC 3526)。
11 - 生命期型式(選項)	1 - 秒。
12 - 生命持續時間(選項)	120：86,400 秒(預設 - 120)。
14 - 金鑰長度	AES-CBC (金鑰長度：128/256)。

備考：符合本標準並實作 GDOI 之實作應支援表 3 中列出的下列演算法：

- 加密：AES-CBC-128 (針對 IEC 61850 TEK 酬載亦為必備)。若須執行填墊以匹配演算法區塊長度，則應使用 PKCS#7 填墊。
- 雜湊：SHA2-256。
- 鑑別：RSA-2048 簽章。
- DH 群組：
 - 符合之 GDOI 伺服器(KDC)實作應支援 DH 群組 14-18。依德國 BSI TR 02102-3 及 NIST SP 800-56A，DH 群組 14(MODP-2048)係視為不夠安全，宜僅用於回溯相容之情況。

- 符合之 GDOI 客戶端實作應支援 DH 群組 16-18，並選項的支援 DH 群組 14-15。

可選項支援表 3 中列出之其他演算法。

表 3 中列出之必備或選項演算法以外的其他演算法之偵測，應引發安全事件(“錯誤：IKEv1 階段 1 提議未規定之密碼演算法”)。

建立 DH 秘密並衍生會期金鑰後，IKEv1 使用 MAC 後再加密(MAC-then-encrypt)作法。於下列各節中，加密藉由記法 HDR*指示，以指示標頭之後的資料已加密。於解密任何已加密訊息期間偵測出填墊錯誤，將引發安全事件(“錯誤：IKEv1 交握解密期間填墊錯誤。”)並應中止 GDOI 交握。

8.3 階段 1 IKEv1 主模式交換型式 2

8.3.1 一般

IKEv1 (RFC 2409)定義 2 種執行階段 1 交換之方法：“主模式”及“積極模式”。

IKEv1 主模式交換之支援係屬必備，並禁止支援 IKEv1 積極模式交換。IKEv1 主模式交換係 ISAKMP 識別資訊保護交換之實例。IKEv1 主模式交換使用 ISAKMP 交換型式 2。

取決於初始 SA 酬載中提供之鑑別方法(IKE 鑑別方法 SA 屬性，值 3)，IKEv1 規定 4 種主模式交換：

- 具數位簽章之鑑別。
- 具公開金鑰加密之鑑別。
- 具公開金鑰加密之修訂鑑別方法。
- 具預先共享金鑰之鑑別。

依 RFC 6407，針對以 RSA 2048 位元金鑰之 RSA 數位簽章鑑別的支援係屬必備。

RSA 數位簽章係 IKEv1 鑑別方法屬性值 3。除 RSA 外，亦選項支援諸如 DSA 及 ECDSA 之其他簽章演算法，依 RFC 6407 的 5.3.6 中所概述。需注意，就運作觀點而言，強烈建議於群組內或 KDC 領域內僅支援 1 個簽章方案，以容許 GDOI GROUPKEY-PUSH 訊息之單播及多播傳送。此外，於 1 個領域中支援不同簽章方案可能要求各組件支援多個憑證，此增加管理之額外負擔。使用公開金鑰加密

及預先共享金鑰鑑別係屬選項，本標準中未進一步規定。

數位簽章之主模式交換如圖 19 所示。

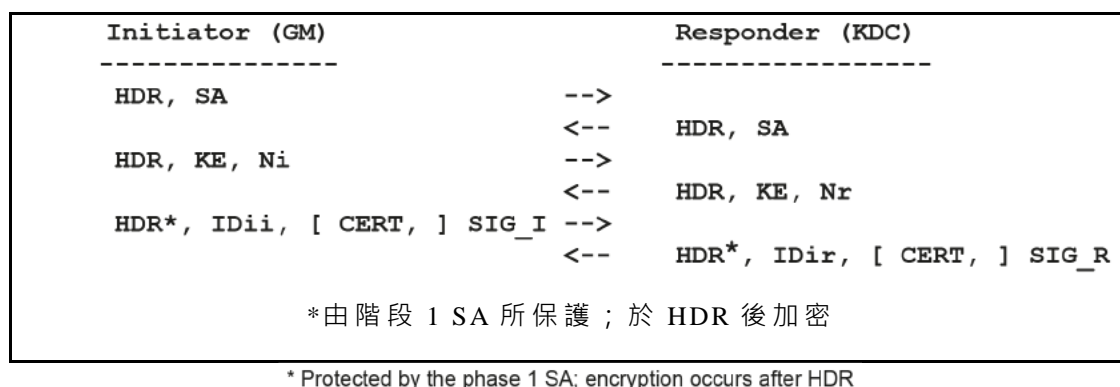


圖 19 具 RSA 數位簽章之 IKEv1 (RFC 2409) 主模式交換

如圖 19 所示，群組成員恆為交換之啟始者。KDC 恆為交換的回應者。此等記法 (亦即 HDR、SA、KE 等) 係取自 RFC 2409。有關記法之定義，參照 RFC 2409 section 3⁽¹⁾。

註⁽¹⁾ <http://tools.ietf.org/html/rfc2409#page-3>.

8.3.2 至 8.3.5 描述各訊息並註釋 KDC 與 IKEv1 協定不同或限制之處。

8.3.2 憑證請求酬載

GM 及 KDC 不應使用 ISAKMP RFC 2408 及 IKEv1 RFC 2409 中所述之憑證請求酬載。此係因 8.3.5.3 中敘述之要求，憑證酬載應恆於階段 1 交換之第 3 次交換中發送。依此，GM 及 KDC 不宜預期接收憑證請求酬載作為符合本標準之 GDOI 使用的一部分。

8.3.3 安全關聯交換(1)

8.3.3.1 一般

所交換之前 2 個訊息應用以判定 IKE SA 之安全關聯，如圖 20 所示。標記為紅色之交換指示目前討論的步驟。

Initiator (GM)		Responder (KDC)
(1) HDR, SA	-->	
	<--	HDR, SA
(2) HDR, KE, Ni	-->	
	<--	HDR, KE, Nr
(3) HDR*, IDii, CERT, SIG_I	-->	
	<--	HDR*, IDir, CERT, SIG_R

圖 20 IKEv1 主模式交換及安全關聯訊息

GM 應依優先序發送所提議之轉換清單，KDC 應選擇第 1 個相容的轉換。

由 GM 發送之初始訊息應包含 RFC 2409 第 5 節交換中所定義的 1 個 SA 酬載。

IKEv1 SA 酬載定義為嵌入於所提議酬載中的 1 或多個轉換酬載，而所提議酬載又嵌入 SA 酬載。不應支援多個提議之酬載。

8.3.3.2 SA 酬載

SA 酬載(SA)應相同於 RFC 2408 之 3.4。KDC 應支援 GDOI RFC 6407 之 2.1，其要求階段 1 SA 酬載 DOI 欄位應設定為 GDOI (2)。SA 酬載情況欄位為 4 個八位元組，應設定為 0。任何其他值將導致錯誤。

8.3.3.3 提議酬載

提議(proposal)酬載應相同於 RFC 2408 之 3.5。KDC 預期 SPI 大小為 0，但若 SPI 大小非為 0，則應忽略 SPI 之內容。KDC 應支援多種轉換。

8.3.3.4 轉換酬載

轉換(transform)酬載應相同於 RFC 2408 之 3.6。所要求之 SA 屬性定義於 RFC 2409 第 4 節中，如下所示：

- 加密演算法，值 1。
- 金鑰長度，值 14。若加密演算法未規定金鑰長度(亦即 AES_CBC)，則要求。
- 雜湊演算法，值 2。
- 鑑別方法，值 3。
- 群組說明，值 4。

KDC 可能支援之選項 SA 屬性為：

- 生命型式，值 11。

- 生命持續期間，值 12。

各屬性之領域定義於表 3 中。具額外屬性之轉換酬載將導致 KDC 拒絕該酬載。

8.3.4 金鑰交換(2)

一旦安全關聯協商完成，GM 及 KDC 應能依 SA 中議定之 DH 群組說明交換 Diffie-Hellman (DH)公開值。金鑰交換序列如圖 21 所示。標記為紅色之交換指示目前討論的步驟。

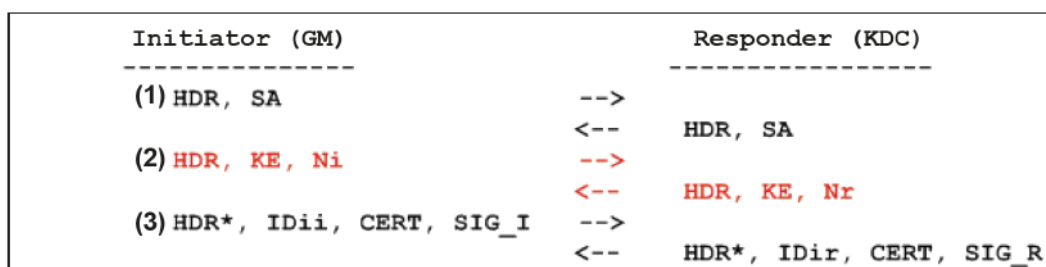


圖 21 IKEv1 主模式交換：金鑰交換訊息

於此金鑰交換序列中，KDC 應接收具金鑰交換(KE)酬載及單次隨機數(Ni)酬載之 ISAKMP 訊息。KE 酬載包含 GM 之 DH 公開值，Ni 酬載包含 GM 的單次隨機數。依所接收 GM 之 DH 公開值，可計算出 DH 秘密。同樣，GM 於金鑰交換(KE)酬載中接收 KDC 之 DH 公開金鑰，以及 Nr 酬載中所包含源自 KDC 的單次隨機數。針對各 SA，單次隨機數須加密安全且彼此不同。

然後，DH 秘密及接收自 Ni 酬載之單次隨機數資訊，係用以於階段 1 衍生進一步的金鑰。然後，公開 DH 參數、單次隨機數及源自交換之進一步資訊，係用以依階段 1 交換的第 3 次交換之 HASH_I (啟始者)及 HASH_R (回應者)計算簽章(參照 8.3.5)。

依 RFC 2409 第 5 節所述，單次隨機數應係於 8 個位元組至 256 個位元組間。

KDC 應建立至少為雜湊區塊大小一半之單次隨機數。

KE 及 Ni/Nr 酬載應分別相同於 RFC 2408 之 3.8 及 3.14 中所定義。

8.3.5 ID 鑑別交換(3)

8.3.5.1 一般

一旦連接已受保護，最後一次安全訊息交換將執行相互鑑別。ID 鑑別序列如圖

22 所示。紅色標記之交換指示目前討論的步驟。

Initiator (GM)		Responder (KDC)
(1) HDR, SA	-->	
	<--	HDR, SA
(2) HDR, KE, Ni	-->	
	<--	HDR, KE, Nr
(3) HDR*, IDii, CERT, SIG_I	-->	
	<--	HDR*, IDir, CERT, SIG_R

圖 22 IKEv1 主模式交換：ID 鑑別訊息

接收自 GM 之最後訊息應包含 GM 的 ISAKMP 識別(識別酬載)、其公開金鑰憑證(憑證酬載)，以及分別使用其 X.509 公開金鑰憑證的私密金鑰之 HASH_I 或 HASH_R 簽章(簽章酬載)。

8.3.5.2 識別酬載

ID 酬載(IDii 或 IDir)應相同於 RFC 2408 之 3.8 中所定義。ID 型式技術上係 DOI 特定。GDOI RFC 6407 未規定其自有型式，但隱示為 IPsec DOI 所定義型式，並使用於 GDOI 中。此等型式係由 IANA 依 IKEv2 (RFC 5996 [39])所維護。因此，支援之 ID 型式應為 ID_DER_ASN1_DN，其值為 9。酬載之內容應為源自 GM 的 X.509 公開金鑰憑證之 DER 編碼主體 ID。不應支援所有其他 ID 型式，並應導致錯誤。

需注意，主體 ID 亦為 8.3.5.3 中所述憑證酬載之一部分。儘管如此，此處保留係保持與 RFC 2409 之相容性。

8.3.5.3 憑證酬載

憑證酬載(CERT)應包含 DER 編碼之 X.509 公開金鑰憑證，且應依 RFC 2408 的 section 3.9 中所定義。應支援值為 4 之 X.509 公開金鑰憑證 - 簽章憑證編碼型式。不應支援所有其他編碼型式，且應導致錯誤。

儘管 RFC 2409 規定選項包括 1 或多個憑證酬載，但 KDC 應恆於 ISAKMP 訊息中包含 1 個且僅 1 個憑證酬載。

若 GM 確實提供 KDC 無法查證之憑證，則 KDC 應發送包含刪除酬載的階段 2 資訊交換，其使用階段 1 SA 金鑰材料加密(亦參照 8.4.3)。

8.3.5.4 簽章酬載

簽章酬載(SIG_I 及 SIG_R)應依 RFC 2408 之 3.12，不修改其定義。該內容應為藉由使用對應發送者識別之公開金鑰憑證的啟始者或回應者私密金鑰所產生的簽章，分別為 RFC 2409 第 5 節中所定義 HASH_I(啟始者)或 HASH_R(回應者)，如圖 23 所描繪。

$$\begin{aligned}\text{HASH_I} &= \text{prf}(\text{SKEYID}, g^{\text{xi}} \mid g^{\text{xr}} \mid \text{CKY-I} \mid \text{CKY-R} \mid \text{SAi_b} \mid \text{IDii_b}) \\ \text{HASH_R} &= \text{prf}(\text{SKEYID}, g^{\text{xr}} \mid g^{\text{xi}} \mid \text{CKY-R} \mid \text{CKY-I} \mid \text{SAi_b} \mid \text{IDir_b})\end{aligned}$$

圖 23 IKEv1 HASH_I 計算

有關記法之定義，參照 RFC 2409 的第 3 節。

值得注意者，RSA 簽章並非標準 PKCS #1 格式之簽章，而是使用憑證對應的 RSA 私密金鑰進行簡單加密，依 RFC 2409 之 5.1 中所述：

“由於所使用之雜湊演算法係已知，因此無需將其 OID 編碼入簽章中。此外，PKCS #1 中用於 RSA 簽章之 OID 與本文件中使用的 OID 間並無繫結。因此，RSA 簽章須以 PKCS #1 格式編碼為私密金鑰加密，而非 PKCS #1 格式之簽章(其包括雜湊演算法之 OID)。”

8.4 階段 1/2 ISAKMP 資訊交換型式 5

8.4.1 一般

KDC 應使用 ISAKMP 資訊交換以通知其同級方已發生錯誤。KDC 不應使用 ISAKMP 資訊交換提供 IKEv1 RFC 2409 之 5.7 中所定義狀態 SA。

資訊交換可於階段 1 或階段 2 交換期間發送。階段 1 資訊交換未加密，且 ISAKMP 標頭中之訊息 ID 欄位設定為 0。階段 2 資訊交換係經加密且具唯一之訊息 ID。應提供唯一之訊息 ID，使得可計算適用的加密初始化向量(IV)。

8.4.2 階段 1 資訊交換

8.4.2.1 一般

當建立 ISAKMP 連接時，可啟始階段 1 訊息交換，以指示階段 1 交換中發生錯誤。階段 1 資訊交換如圖 24 所示。



圖 24 階段 1 資訊交換(參照 RFC 2408 之 4.8)

GM 及 KDC 可為階段 1 資訊交換之啟始者。資訊交換訊息應具 RFC 2408 之 3.14 中所定義的單一通知酬載(N)。

階段 1 資訊交換應支援 RFC 2408 之 3.15 中所定義刪除酬載(D)，如 RFC 2408 的 3.15 中所定義。

階段 1 資訊交換不應支援雜湊酬載。因此，KDC 不應發送具雜湊酬載之階段 1 資訊交換，且應忽略於階段 1 資訊交換中所接收的任何雜湊酬載。階段 1 資訊交換訊息應將 ISAKMP 標頭中之訊息 ID 欄位設定為 0，且不應加密。

8.4.2.2 通知酬載

通知(notification)酬載定義於 RFC 2408 之 3.14 中。針對階段 1 資訊交換，酬載欄位值定義為：

- 解譯領域 - 值為 2，GDOI。
- 協定 ID - 值為 0。
- SPI 大小 - 值為 0。I-Cookie 及 R-Cooki 係用作 SPI。
- 通知訊息型式 - RFC 2408 之 3.14.1 中所定義之任何值。
- SPI - 未包含於酬載中。
- 通知資料 - 未包含於酬載中。

8.4.2.3 刪除酬載

刪除(delete)酬載定義於 RFC 2408 之 3.15 中。刪除酬載係用以反應階段 1 協商期間之可能錯誤，如 SA 逾時、憑證錯誤或 Diffie Hellman 相關錯誤(例：錯誤的 MODP 等)、無傳送集匹配等。針對階段 1 資訊交換，酬載欄位值定義為：

- 解譯領域 - 值為 2，GDOI。
- 協定 ID - 值為 0。
- SPI 大小 - 值為 16。

- SPI 之數量 - 刪除酬載中所包含的 SPI 數。
- SPI - 將刪除之 SPI。I 訊錄(cookie)及 R 訊錄係用作 SPI。

8.4.3 階段 2 資訊交換

建立 ISAKMP 連接後，可**啟始**階段 2 資訊交換以提供通知酬載或刪除酬載，指示階段 2 交換中所發生之錯誤。階段 2 資訊交換如圖 25 所示。

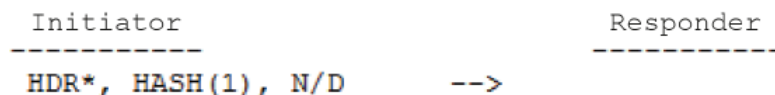


圖 25 階段 2 資訊交換(參照 RFC 2409 之 5.7)

GDOI RFC 6407 提及關於 GM 不接受 SA 政策之資訊交換。若 GM 不接受 SA 酬載中之政策，則“GM 宜於使用包含刪除酬載的 ISAKMP 資訊交換通知 KDC 後，刪除階段 1 會談”(RFC 6407 之 3.3)。

然而，未提及 KDC 或 GM 宜如何處理雜湊不正確，或 GM 未具對群組之存取權限，或特定 SA 之生命期逾期的情況。為涵蓋此等情況，本標準新增 KDC 應於 GROUPKEY-PULL 交換自身中嵌入通知酬載之要求。若於處理源自 GM 之 GROUPKEY-PULL 訊息時發生不成功，則 KDC 將於相同交換上回傳 GROUPKEY-PULL 訊息，連同指示錯誤碼的單一通知酬載。GROUPKEY-PULL 交換應終止。

KDC 應支援接收嵌入於 GROUPKEY-PULL 交換中之通知酬載，並接收具刪除酬載的資訊交換。若通知/刪除酬載之 SPI 匹配現有 GROUPKEY-PULL 交換的 SA，則應停止交換。

若使用具刪除酬載之資訊交換傳訊此錯誤，則其應包含雜湊值。訊息之安全應依賴階段 1 中建立之金鑰材料 SKEYID_e 及 SKEYID_a。雜湊值應依 SKEYID_a，依 RFC 2409 之 5.7 中的 HASH(1)定義計算，依描繪於圖 26 中。

$$\text{HASH}(1) = \text{prf}(\text{SKEYID}_a, \text{M-ID} \parallel \text{N/D})$$

圖 26 IKEv1 HASH(1)計算

此外，當發送具刪除酬載之資訊交換時，應使用階段 1 SA 產生之 SKEYID_e 對其進行加密，依 RFC 2409 的 5.7 中所述。

8.5 階段 2 GDOI GROUPKEY-PULL 交換型式 32

8.5.1 一般

GDOI (RFC 6407) 定義階段 2 GROUPKEY-PULL 交換，以容許群組成員針對單一安全多播群組，拉取共享安全關聯。依階段 1 IKEv1 主模式交換期間建立之 IKE SA 安全連接後，執行 GROUPKEY-PULL 交換。RFC 6407 之 3.2 定義圖 27 中之 GROUPKEY-PULL 交換。

Group Member		KDC
(1) HDR*, HASH(1), Ni, ID	-->	
(2)	<--	HDR*, HASH(2), Nr, SA
(3) HDR*, HASH(3) [,GAP]	-->	
(4)	<--	HDR*, HASH(4), [SEQ,] KD

*由階段 1 SA 所保護；於 HDR 後加密

* Protected by the phase 1 SA; encryption occurs after HDR

圖 27 RFC 6407 中定義之 GDOI GROUPKEY-PULL

有關記法、首字母縮寫詞及縮寫，參照 RFC 2409 之 3.2 及 RFC 6407 的 1.3。

群組成員應恆啟始 GROUPKEY-PULL 交換。KDC 應恆為 GROUPKEY-PULL 交換之回應者。

當 KDC 接收源自 GM 之初始 GROUPKEY-PULL 交換訊息時，驗核該訊息，並開始新的 GROUPKEY-PULL 交換。抽取酬載且計算並驗核 HASH(1)。KDC 上之錯誤雜湊計算將導致交換不成功，且應由指示錯誤型式 INVALID_HASH_INFORMATION (值 23) 的 KDC 啟始階段 2 資訊交換。

於 GM 處之不正确雜湊計算將導致交換不成功，且 GROUPKEY-PULL 回應訊息應發送回 GM，連同指示 INVALID_HASH_INFORMATION 錯誤型式(值 23)的通知酬載。

應抽取安全多播群組 ID，若未發現安全多播群組或 GM 並非授權群組成員，則交換應不成功，且應將 GROUPKEY-PULL 回應訊息發送回 GM，其中通知酬載

分別指示錯誤 INVALID-ID-INFORMATION (值 18) 及 AUTHENTICATION_FAILURE (值 24)。

群組成員應確保金鑰之階段 2 交換，應於該 SA 中的任何其他新金鑰請求前完成。

若群組成員於多次重試後仍無法針對特定群組抽取相同之群組金鑰，則其應發送包含刪除酬載的階段 2 資訊交換，該酬載使用階段 1 SA 金鑰材料加密(亦參照 8.4.3)。此本質上將終止與該 GM 之 SA。重試次數取決於本地安全政策。

8.5.2 雜湊計算

針對 GROUPKEY-PULL 交換計算之雜湊值，應使用階段 1 SA 中的安全雜湊演算法。雜湊值應以階段 1 鑑別秘密 SKEYID_a 保全，依 RFC 6407 之 3.2 中所定義。GROUPKEY-PULL 交換中使用之不同雜湊值，應依圖 28 中所規定的資訊計算。

```

HASH(1) = prf(SKEYID_a, M-ID | Ni | ID)
HASH(2) = prf(SKEYID_a, M-ID | Ni_b | Nr | SA)
HASH(3) = prf(SKEYID_a, M-ID | Ni_b | Nr_b [ | GAP ])
HASH(4) = prf(SKEYID_a, M-ID | Ni_b | Nr_b [ | SEQ ] | KD)

```

圖 28 GROUPKEY-PULL 雜湊計算

8.5.3 多重發送者及計數器模式加密演算法

IEC 61850 SA (參照 8.5.7)應支援 AES-GCM 及 AES-GMAC 計數器模式演算法。計數器模式演算法提供於單一 SA 上存在多個發送者之能力。此係藉由確保各發送者針對發送之各封包使用唯一的初始化向量(IV)所達成。GDOI RFC 6407 之 3.5 規定 KDC 實作 RFC 6054，以將 IV 空間的一部分指派予群組中之各發送者⁽¹⁾。

註⁽¹⁾ RFC 6054—使用封裝安全酬載(ESP)及鑑別標頭(AH)之計數器模式，保護群組訊務 (<http://tools.ietf.org/html/rfc6054>)。

無須支援源自 GM 之依計數器模式的 IEC 61850 群組金鑰的發送者 ID 請求。若自 GM 接收具發送者 ID GAP 屬性(值 3)之群組關聯政策(GAP)酬載，則 KDC 將使 GROUPKEY-PULL 交換不成功。應於資訊交換中回傳錯誤型式 ATTRIBUTES-NOT-SUPPORTED (值 13)。

備考：本標準之未來版本是否支援單一 DATA SA 上的多個發送者尚待確定。

8.5.4 SA KEK、SEQ、KEK/LKH 金鑰下載酬載支援

由於 GROUPKEY-PUSH 係屬選項，因此 GROUPKEY-PULL 交換無須支援金鑰下載酬載中之 SA KEK 酬載、SEQ 酬載或 KEK/LKH 金鑰封包。因此，於 GROUPKEY-PULL 之全景中，不宜使用 SA KEK 金鑰。依 RFC 6407 之 5.3.2，KEK 金鑰僅能用於 GROUPKEY-PUSH。

GROUPKEY-PUSH 之既有 SA 的重新產生金鑰，描述於 8.6 中。

有關 GDOI 酬載指配之資訊，特別是金鑰下載型式，參照 IANA [52]。依此定義，TEK 之金鑰下載型式為 1，而 KEK 的金鑰下載型式為 2。

附註：IEC 61850 安全協定何時支援 GROUPKEY-PUSH 交換尚待確定。

8.5.5 GROUPKEY-PULL 群組 SA 請求交換

8.5.5.1 一般

初始 SA 請求交換如圖 29 所示。紅色標記之交換指示目前討論的步驟。



圖 29 GROUPKEY-PULL 初始 SA 請求交換

GM 應藉由將訊息(1)發送予 KDC 啟始 GROUPKEY-PULL 交換。HASH (1)及 Ni 酬載定義於 RFC 6407 第 3 節中。ID 酬載已延伸為支援 IEC 61850 安全多播群組。

8.5.5.2 識別酬載

8.5.5.2.1 一般

於階段 2 交換之 ID 酬載(ID)相同於階段 1 交換中使用的 ID 酬載(參照 8.3.5.2)。不同之處在於階段 1 交換中，包含的識別資料係群組成員之識別資料，而針對階段 2 交換，ID 識別將拉取的 SA 之群組金鑰，如圖 30 所示。KDC 應支援 IEC 61850 安全多播群組。



圖 30 RFC 6407 識別酬載

識別酬載之格式包括：

- 下個酬載 - 有關定義及使用，參照 RFC 2408。
- 保留 - 有關定義及使用，參照 RFC 2408。
- 酬載長度 - 有關定義及使用，參照 RFC 2408。
- ID 型式(ID type) - IEC 61850 安全多播群組係由 RFC 8052 “GDOI Protocol Support for IEC 62351 Security Services” 的 2.1 中定義之 ID_OID ID 型式所識別。ID_OID ID 型式之值為 13。識別資料 ID_OID 表示 ASN.1 Object ID (OID)(1) 及其 OID 特定資料。OID 及 OID 資料係使用 DER 編碼規則進行編碼(2)。識別資料酬載內之欄位定義定義並描述於圖 31 中。例：OID 可表示 GOOSE 或取樣值協定，於其他情況下，IEC 61850 亦規定於 OID 特定酬載欄位中描述之特定多播目的地位址。

註⁽¹⁾ 物件 ID 格式定義於 ITU-T-X.683 中

<http://www.itu.int/ITU-T/studygroups/com17/languages/X.683-0207.pdf>。

註⁽²⁾ 相異編碼規則定義於 ITU-T-X.689 中

<http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf>。

- DOI 特定 ID 資料(DOI-specific ID data) - 應設定為 0。
- 識別資料(Identification data) - 特定於 ID_OID，描述於 8.5.5.2.2 中。

8.5.5.2.2 IEC 61850 物件之識別資料

GDOI GROUPKEY-PULL 交換中之 GDOI 識別酬載(例：階段 2 請求)，容許群組成員(GM)宣告其欲加入的群組。群組係依 GDOI RFC 6407，由 ID 酬載所定義。

圖 31 係抽取自 RFC 8052，定義特定之 ID 型式值及識別資料的格式。

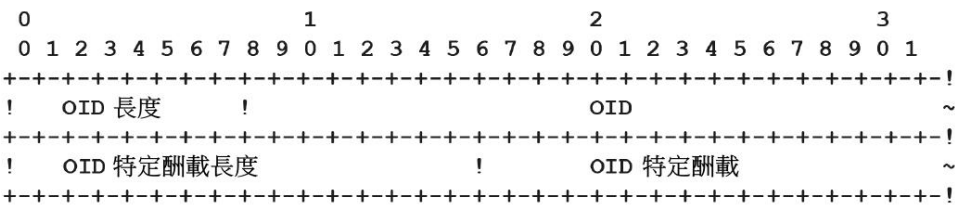


圖 31 ID_OID 識別資料

- **OID 長度**：此長度應為無正負號整數值，並應規定 ASN.1 編碼之 OID 之八位元組數，其值記於長度之後。
- **OID**：此八位元組集表示 ASN.1 編碼之物件識別符。識別符之值定義隨後的酬載。用此物件識別符使得其他組織或標準可利用此酬載延伸過程，而不至於在定義全景中發生重複。物件識別符之值於表 4 中定義為必備(m)或選項(o)。
- **OID 特定酬載長度(2 個八位元組) - OID 特定酬載之長度**。若 OID 未要求 OID 特定酬載，則設定為 0。
- **OID 特定酬載(可變長度) - 以 DER 編碼之 OID 特定選擇符(selector)**。若 OID 特定酬載長度設定為 0，則該欄位不出現於 ID 酬載中。

於 GROUPKEY-PULL 交換完成時，金鑰伺服器應已完成傳送群組政策予所有授權群組成員，從而容許接收群組成員參與安全群組通訊。

KDC 應支援表 4 中所定義必備之 IEC 61850 物件 ID，此 ID 識別 GM 請求金鑰材料之 IEC 61850 串流。

表 4 IEC 61850 物件 ID：必備(m)及選項(o)

物件識別符名稱	說明	值	m/o
61850_ETHERNET_GOOSE	規定酬載正在請求 IEC 61850-8-1 GOOSE APDU 之金鑰。	1.0.62351.9.61850.8.1.1	m
61850_UDP_ADDR_GOOSE	規定酬載正在請求傳送予特定目的地 IP 位址之可路由 GOOSE APDU 的金鑰。	1.0.62351.9.61850.8.1.2	m
61850_UDP_Tunnel	規定酬載正在請求傳送予特定目的地 IP 位址之 IEC 61850 可路由隧道 APDU 之金鑰。	1.0.62351.9.61850.8.1.4	o

物件識別符名稱	說明	值	m/o
61850_ETHERNET_SV	規定酬載正在請求 IEC 61850-9-2 SV APDU 之金鑰。	1.0.62351.9.61850.9.2.1	m
61850_UDP_ADDR_SV	規定酬載正在請求可路由 IEC 61850 SV APDU 之金鑰。	1.0.62351.9.61850.9.2.2	m
61850_IP_ISO9506	規定酬載正在請求 IEC 61850-8-1 ISO 9506 端點之金鑰。此酬載定義超出範圍。	1.0.62351.9.61850.8.1.4	o
61850_9_3_PTP	規定酬載正在請求 IEC 61850-9-3 PTP Domain 的金鑰。	1.0.62351.9.61850.9.3.1	o
所使用之 OID 已定義於 IEC 62351 中，以 1.0.62351.9.xxx 起始，而 IEC 61850-90-5 中使用之 OID 則以 1.2.840.10070.xxx 起始。			

8.5.5.2.3 IEC 61850 OID 特定酬載

GOOSE (61850_UDP_ADDR_GOOSE) 與 SV (61850_UDP_ADDR_SV) OID⁽⁹⁾ 之 UDP 版本的酬載相同。61850_UDP_ADDR_GOOSE 及 61850_UDP_ADDR_SV OID 特定資料之 ASN.1 序列規定於圖 32 中。

註⁽⁹⁾ GOOSE 與 SV 之 IP 版本的酬載相同。

```

IecUdpAddrPayload ::= SEQUENCE
{
    version      INTEGER { v1(1) },
    ipAddress    IPADDRESS,
    dsRef        VisibleString SIZE(1..128)
}

```

圖 32 61850_UDP_ADDR_GOOSE/SV ASN.1 BNF

- version 為單個八位元組值，表示特定酬載之版本。除非另有規定，VERSION 之值應為 1。
- IpAddress 係值組件，其容許與所請求金鑰相關聯之個體使用 IPv4 或 IPv6 目的地位址。IPADDRESS ASN.1 序列規定於圖 33 中。

- dsRef 值組件容許指定 IEC 61850 資料集參考(DSRef) · 依 CNS 61850-7-2 中所規定。

```

IPADDRESS ::= SEQUENCE
{
    typeOfAddress ENUMERATED { IPv4(0), IPv6(1) },
    address CHOICE {
        ip OCTET STRING (SIZE(4 | 16)),
        dns VisibleString (SIZE(1..65536))
    }
}

```

圖 33 IPADDRESS ASN.1 BNF

圖 34 係 61850_UDP_ADDR_GOOSE 或 61850_UDP_ADDR_SV OID 之 61850 OID 位址酬載示例。

```

groupaddr IecUdpAddrPayload ::=
{
    version v1,
    ipAddress
    {
        typeOfAddress IPv4,
        address dns: "www.iec.org"
    }
    dsRef "@somedataref"
}

DER Encoding:

30230201 0130100A 01001A0B 7777772E
6965632E 6F72671A 0C40736F 6D656461
74617265 66

```

圖 34 以 DER 編碼之 IecUdpAddrPayload ASN.1 資料示例

61850_UDP_TUNNEL OID 特定資料之 ASN.1 序列規定於圖 35 中。

```

IecUdpTunnelPayload ::= SEQUENCE
{
    version INTEGER { v1(1) },
    ipAddress IPADDRESS
}

```

圖 35 61850_UDP_TUNNEL 酬載 ASN.1 BNF

由於 1 個隧道 SPDU 中可傳送多個乙太網路多播訊框(例：GOOSE 或 SV) · 故

dsRef 欄位不出現於該酬載中。因此，目的地 IP 位址本身區分資料集。

GOOSE (61850_ETHERNET_GOOSE)相同於 SV (61850_ETHERNET_SV)乙太網路版本之 OID 酬載。61850_ETHERNET_GOOSE/SV OID 特定資料之 ASN.1 序列規定於圖 36 中。

```
IecEthernetAddrPayload ::= SEQUENCE
{
    version    INTEGER { v1(1) },
    dstMAC     OCTET STRING (SIZE(6)),
    dsRef      VisibleString (SIZE(1..256))
}
```

圖 36 61850_ETHERNET_GOOSE/SV 酬載 ASN.1 BNF

- version 為單個八位元組值，表示特定酬載之版本。除非另有規定，VERSION 之值應為 1。
- dstMAC 係由 6 個八位元組組成之值。該值應依乙太網路傳送序。
- dsRef 值組件容許規定 IEC 61850 資料集參考(DSRef)，依 CNS 61850-7-2 中所規定。

8.5.5.2.4 IEC 61850_9_3 特定酬載

IEC 61850-9-3 之酬載(亦即 PTP 之電力剖繪)應規定 PTP 時域(ptpDomain)以及除該時域 ID 之時域。此識別符應為 GM 與 KDC 間共同議定的值，使得可於具不同金鑰及政策之基礎建設的其他部分中重複使用相同的時域編號。

```
Iec61850PTPPayload ::= SEQUENCE
{
    ptpDomain    INTEGER - defined by the allowed range per IEEE 1588
    ptpSubDomain [0] IMPLICIT INTEGER OPTIONAL - defined by IEEE 1588
    keyMngtDomain VisibleString (Size(1..256))
}
```

keyMngtDomain 值係用以容許於公用事業企業之 2 個不相關區域中，部署相同的 ptpDomain 及 ptpSubDomain 識別符，並能對此等個體遞送不同之金鑰及政策。此值係本地組態議題，不應為 NULL 或空。GROUPKEY-PULL 中所請求之金鑰的唯一識別符係由 ptpDomain、ptpSubDomain 及 keyMngtDomain 之值組成的唯

一三值組。

預期特定 PTP 時區或 PTP 子時區之所有 PTP 實例使用相同的金鑰管理協定。

8.5.6 SA TEK 酬載

8.5.6 SA TEK payload

SA TEK 酬載應包含與群組 TEK 相關聯之單一政策集的安全屬性。將與 TEK 一起使用之政策型式係由 SA TEK 所包含的協定 ID 欄位所描述。如複製自 RFC 6407 之圖 37 所示，各協定 ID 描述特定之 TEK 協定特定酬載定義。

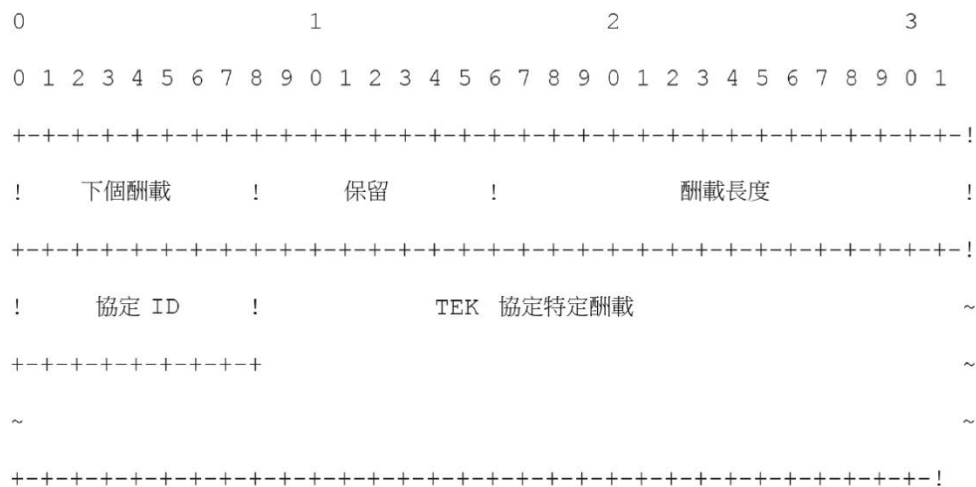


圖 37 RFC 6407 SA TEK 酬載

KDC 應遵循 RFC 8052 之 2.2 中所定義的 IEC-61850 SA TEK 酬載格式。IEC-61850 SA TEK 酬載定義 2 個選項 SA 資料屬性：啟動時間延遲(SA_ATD)及金鑰遞送保證(SA_KDA)屬性。此等屬性之值定義於 RFC 8052 的 4.0 “IANA 考量事項”中。

GDOI_PROTO_IEC_61850 之協定 ID 名稱定義於 RFC 8052 的 2.2 中，值為 3。

8.5.7 IEC 61850 SA TEK 酬載

GDOI_PROTO_IEC_61850 SA TEK 應包含 OID 及(選項)OID 特定酬載，其一起定義網路訊務之選擇符。選擇符欄位應後接安全政策欄位，指示如何保護所規定之訊務。如圖 38 所示，複製自 RFC 8052，各 61850 TEK 酬載描述特定之 TEK 協定特定酬載定義。



圖 38 IEC-61850 SA TEK 酬載

GDOI_PROTO_IEC_61850 SA TEK 酬載欄位於 RFC 8052 中定義如下：

- (a) **OID 長度**(1 個八位元組) - OID 欄位之長度。
- (b) **OID**(可變長度) - 使用 DER 編碼之 ASN.1 物件識別符。CNS 61850 中定義之 OID 宣告待保護的 IEC 61850 訊息之型式，依表 4 中所定義。
- (c) **OID 特定酬載長度**(2 個八位元組) - OID 特定酬載之長度。若政策未包括 OID 特定酬載，則此欄位設定為 0。
- (d) **OID 特定酬載**(可變長度) - 特定於使用 DER 編碼之 OID 的訊務選擇符(例：多播位址)。某些 OID 政策設定未要求使用 OID 特定酬載，於此情況下，該欄位未納入 TEK，且 OID 特定酬載長度設定為 0。
- (e) **SPI**(4 個八位元組) - 目前金鑰之識別符。該欄位表示 SPI。
- (f) **Auth Alg** (2 個八位元組) - 鑑別演算法 ID。有效值定義於 RFC 8052 之 2.2.2 中。HMAC-SHA256-128 係屬必備。此外，本標準亦要求支援 HMAC-SHA256、AES-GMAC-128 及 AES-GMAC-256。
- (g) **Enc Alg** (2 個八位元組) - 機密性演算法 ID。有效值定義於 RFC 8052 之 2.2.3

中。AES-CBC-128 係屬必備。

- (h) 剩餘生命期值(4 個八位元組) - 此 TEK 逾期前剩餘之秒數。值為 0 應指示 TEK 未逾期時間。最大生命期應與 CRL 刷新時間相關聯，以確保依組織之安全政策處理憑證逾期或撤銷憑證的群組成員。
- (i) SA 資料屬性(可變長度) - 包含 0 或多個與該 SA 相關之屬性。RFC 8052 之 2.2.4 定義屬性。

關於如何組合鑑別演算法及機密性演算法存在某些限制。此等限制彙總如下：

- (a) 若適用如 AES-GCM 之 AEAD 演算法(同時提供機密性及鑑別)，則機密性演算法應規定 AEAD 演算法，亦即 AES-GCM-128 (值 4)或 AES-GCM-256 (值 5)。鑑別演算法欄位應設定為 NONE (值 1)。
- (b) 若針對機密性規定非 AEAD 演算法，亦即 AES-CBC-128 (值 2)或 AES-CBC-256 (值 3)，則應規定鑑別演算法。RFC 8052 定義所支援之訊息鑑別演算法，必備的支援為 HMAC-SHA256-128 (值 2)。或者，可使用 HMAC-SHA256-128 (值 3)、AES-GMAC-128 (值 4)或 AES-GMAC-256 (值 5)。此處未預見 AES-GMAC 變異之使用，因其本質上於 GMAC 模式下採用 AEAD 演算法。
- (c) 由於機密性係屬選項，因此機密性演算法欄位可設定為 NONE (值 1)。鑑別演算法應依 RFC 8052 中所定義之支援演算法規定，亦即 HMAC-SHA256-128 (值 2)、HMAC-SHA256-128 (值 3)、AES-GMAC-128 (值 4)或 AES-GMAC-128 (值 5)。

8.5.8 IEC 61850-9-3 之 SA TEK 酬載

IEC 61850-9-3 (亦即 PTP 之電力剖繪、IEEE 1588:2019)之 SA-TEK 酬載，應提供保護 PTP 交換所須的參數。PTP 之整合安全選項規定於 IEEE 1588:2019 之 16.14。此節規定 AuthenticationTLV，用於為每個訊息提供完整性保護。為利用此 AuthenticationTLV，金鑰管理將提供某些參數。IEEE 1588:2019 未自行定義金鑰管理，並預期 PTP 剖繪針對所考量的時域選擇適切之金鑰管理。IEEE 1588:2019 之附錄 P 已概述 GDOI 的 1 種可能選擇。由於 GDOI 已適用於電力系統領域，配送安全參數及安全政策以保護 GOOSE 及 SV 通訊，因此針對 PTP 中之應用其亦

可用以配送該資訊。

需注意，IEEE1588:2019 定義用於立即安全處理(PTP 各參與方已有可用之群組金鑰)，或延遲安全處理(查證 PTP 訊息完整性之群組金鑰於稍後時間點發布，導致延遲驗核)的支援。GDOI 目標為電力系統所要求之立即安全處理。

IEEE 1588:2019 之 16.14.2 要求下列參數可用於提供 PTP 訊息完整性保護。需注意，所選值係旨在成為 IEEE 1588:2019 之 16.14.2 中所定義 AUTHENTICATION TLV 的一部分。

- 安全參數指標(security parameter pointer, SPP)：識別安全關聯(SA)。此應為 SA TEK SPI。
- IntegrityAlgTyp：識別用以計算 ICV 大小之完整性演算法型式。演算法型式應於 SA TEK 之 Auth Alg 欄位中規定。
- icvLength：指示所計算之 ICV 的長度。該長度係依 SA TEK 中之 Auth Alg 所要求，由演算法決定。
- Key：與所選演算法結合使用之對稱金鑰。該值應依 8.5.11 中所述，於 GROUPKEY-PULL 之 KD 酬載中提供，且以 GROUPKEY-PUSH 的 SA TEK 遞送金鑰資訊。需注意，8.5.12 亦定義 TEK 下載處理。
- keyLength：指示公開金鑰之長度(選項參數，僅當使用延遲安全處理時)。金鑰長度應透過 SA TEK GDOI 酬載所使用之金鑰演算法所決定。
- 指示選項欄位 sequenceNo 之使用以及 sequenceNo 欄位的所需長度。依 IEEE1588:2019，該欄位應為“0”。因此，SA TEK 中未提供該值。預期其係本地組態議題。
- 指示針對抗重演 sequenceID 訊窗(依 PTP 訊息標頭中的 sequenceID)。由於 IEEE 1588:2019 未定義抗重演訊窗之特定處理，而是指監視序號的遞增，因此 GDOI 將不提供此序列 ID 訊窗。
- Immediate Security：指示 SA 係用於立即安全或延遲安全之布林值。使用 GDOI 提供立即安全支援。因此 SA TEK 中未提供此值。預期其係本地組態議題。
- 指示於鑑別 TLV 中使用選項欄位 RES 及 RES 欄位所需之長度。依

IEEE1588:2019，此欄位應為“0”。因此，SA TEK 中未提供該值。預期其係本地組態議題。

此等參數對應 8.5.7 中定義之 IEC-61850 SA TEK 酬載。此對映可直接支援描述 PTP 之電力剖繪的 IEC 61850-9-3。下列將上述 IEEE 1588:2019 安全參數欄位對應至 GDOI_PROTO_IEC_61850 SA TEK 酬載欄位：

- (a) OID 長度(1 個八位元組) - OID 欄位之長度。
- (b) OID (可變長度) - 使用 DER 編碼之 ASN.1 物件識別符。IEC 61850 中定義之 OID 宣告待保護的 IEC 61850 訊息之型式，依表 4 中所定義。
- (c) OID 特定酬載長度(2 個八位元組) - OID 特定酬載之長度。若政策未包括 OID 特定酬載，則此欄位設定為 0。
- (d) OID 特定酬載(可變長度) - 特定於使用 DER 編碼之 OID 的訊務選擇符(例：多播位址)。某些 OID 政策設定未要求使用 OID 特定酬載，於此情況下，該欄位未納入 TEK，且 OID 特定酬載長度設定為 0。
- (e) SPI(4 個八位元組) - 目前金鑰之識別符。需注意，IEEE 1588:2019 中之 SPP 僅 1 個八位元組，而 SPI 的長度為 4 個八位元組。此要求 PTP 實例僅使用 SPI 值之一部分作為 SPP 以匹配所要求的長度。PTP 實例應使用 SPI 之低位元值(SPI [0..7])作為將納入 PTP 的鑑別 TLV 之 SPP。
- (f) Auth Alg (2 個八位元組) - 鑑別演算法 ID。此欄位包含 IntegrityAlgTyp。IEEE 1588:2019 要求支援 HMAC-SHA256-128，此亦定義於 RFC 8052 之 2.2.2 中。
- (g) Enc Alg (2 個八位元組) - 機密性演算法 ID。由於 IEEE1588:2019 未支援 PTP 訊息之機密性保護。因此，此值應設定為“0”。
- (h) Remaining Lifetime 值(4 個八位元組) - 此 TEK 逾期前剩餘之秒數。值為 0 應指示 TEK 無逾期時間。最大生命期應與 CRL 刷新時間相關聯，以確保依組織之安全政策處理憑證逾期或撤銷憑證的群組成員。此值於 IEEE 1588:2019 之 16.14 中並未明確規定，但金鑰管理要求確保群組金鑰可定期更新。
- (i) SA Data Attributes(可變長度)。

8.5.9 SPI 討論

8.5.9.1 一般

其針對 GDOI 中之不同目的，利用並定義 2 個不同 SPI 值。此等係包含於 SA TEK 及 SA KEK 中之 SPI 值。兩者之說明參照 8.5.9.2 至 8.5.9.3。

8.5.9.2 SA TEK SPI

RFC 6407 要求定義 SA TEK SPI 之特性。GDOI_PROTO_IEC_61850 SA TEK 中之 SPI 表示為金鑰識別符(KeyID)。SPI 大小為 4 個八位元組。SPI 係由 KDC 使用由實作選定之任何方法單方面選定。然而，實作需注意不重複目前用於特定群組之 SPI 值。

8.5.9.3 SA KEK SPI

RFC 6407 之 5.3 定義 SA KEK 為 16 個八位元組，用以加入 GROUPKEY-PUSH 標頭的啟始者訊錄(initiator-cookie)及回應者訊錄(responder-cookie)。RFC 6407 之 3.2 (GROUPKEY-PULL)定義由 GCKS 所決定的 SPI 值。此值於 GROUPKEY-PULL 與 GROUPKEY-PUSH 間提供金鑰及政策遞送之相關性。圖 39 顯示該關係。

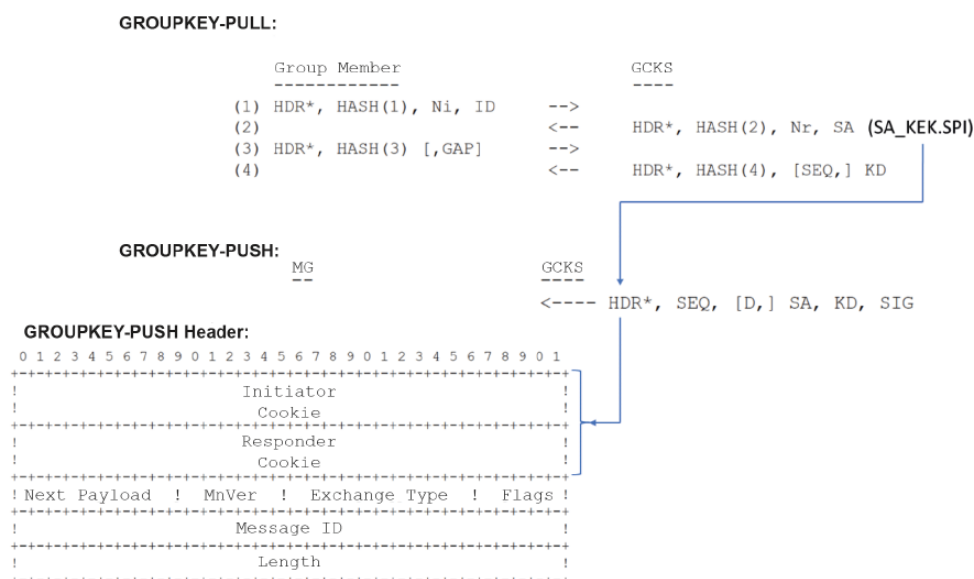


圖 39 SPI 值之相關性

此種相關性容許 GM 判定是否關注 GROUPKEY-PUSH。若 SPI 匹配 GROUPKEY-PULL 期間接收之 SA KEK SPI，則宜處理 GROUPKEY-PUSH，否則，其處理係屬本地議題。

宣稱符合本標準之 KDC (GCKS)實作，應提供對各唯一群組金鑰全域唯一的 SA KEK SPI 值，依 8.5.5.2.3 及 8.5.5.2.4 中所定義。

8.5.10 SA 資料屬性

8.5.10.1 一般

IEC 61850 SA 之 SA TEK 中應出現下列屬性。屬性應依循 RFC 8052 附錄 C 中所述之格式。

8.5.10.2 啟動時間延遲(SA_ATD) SA 資料屬性(值 1)

KDC 應於預期使用 SA TEK 前配送 SA TEK。此係與使用 SA 啟動時間延遲(SA_ATD)屬性之群組成員溝通。當 GM 接收具此屬性之 SA TEK 時，於其針對傳輸或接收安裝前，應等待屬性中所包含的秒數。KDC 應包含 SA_ATD SA 資料屬性，即使該值為 0。指派予 SA_ATD 屬性之值為 1。

8.5.10.3 金鑰遞送保證(SA_KDA) SA 資料屬性(值 2)

群組政策可包括通知多播來源(“發布者”)，關於多播接收者(“訂用者”)先前是否已接收 SA TEK 之指示。此通知容許發布者依接收受 SA TEK 保護之封包的訂用者百分比，設定是否啟動新 SA TEK 之政策。屬性值係 0 至 100 (含)間之數字。針對 KDA 之支援係屬選項。若未支援 KDA，則 KDC 應將 SA_KDA 值設定為 100。

SA_KDA 屬性所指派之值為 2。

8.5.11 GROUPKEY-PULL 群組金鑰下載交換

將 SA 政策發送予 GM 後，KDC 應針對各 SA 發送金鑰材料。此交換如圖 40 所示。



圖 40 GROUPKEY-PULL 金鑰下載交換

將金鑰材料發送予 GM 前，GM 應首先藉由發送具包含 HASH(3)計算之雜湊酬載的訊息(3)，回應 SA 交換，如下所示：

$$\text{HASH}(3) = \text{prf}(\text{SKEYID}_a, \text{M-ID} \parallel \text{Ni}_b \parallel \text{Nr}_b)$$

圖 41 GROUPKEY-PULL 群組金鑰下載雜湊計算

若 KDC 無法驗核雜湊計算，則應以指示 INVALID_HASH_INFORMATION (值 23)之錯誤啟始階段 2 資訊交換。

KDC 應以交換中之最後訊息(4)回應。此包括包含 HASH (4)之雜湊酬載及金鑰下載酬載。金鑰下載(KD)酬載之格式應依 RFC 8052 的 2.3 所定義。KDC 不應變更或規定對所定義 KD 酬載格式之任何限制。

有關 GDOI 酬載指派之資訊，特別是金鑰下載型式(依 RFC 6407 中所定義)，參照 IANA [52]。依各定義，TEK 之金鑰下載型式為 1，而 KEK 的金鑰下載型式為 2。

會期金鑰之更新通常於目前金鑰的“剩餘生命期值”逾期前觸發。“剩餘生命期值”(亦稱為生命期)係 SA TEK 酬載中回傳的參數之一，其表示關聯 SA 逾期前剩餘的秒數。

過程如圖 42 所示，序列如下：

- KDC 針對裝置群組建立會期金鑰，連同其“金鑰識別符(KeyID)”⁽¹⁾、剩餘生命期值及 SA 時間啟動延遲(SA_ATD)參數。其於整個會談期間維護群組之會期金鑰：
註⁽¹⁾ GDOI 將此稱為 SPI。
 - “KeyID”：係 KDC 於 GDOI GROUPKEY-PULL 或 GROUPKEY-PUSH 訊息酬載中發送之會期金鑰的唯一識別符。
 - 剩餘生命期值：係與其相關聯之 SA 逾期前剩餘的秒數。
 - “SA 時間啟動延遲(SA_ATD)”：此參數規定預期何時使用金鑰，因 KDC 有時提前配送 SA TEK。
- KDC 發送 2 個 SA 及相關聯金鑰，其一(K0)目前具 SA_ATD 0，因此可立即使用，第 2 個(K1) SA_ATD 非 0，稍後使用。KDC 同步 2 個 SA，使得第 2 個金鑰之時間延遲 SA_ATD 小於第 1 個金鑰的生命期。
- 當 GM 獲得 2 個會期金鑰 K0 及 K1 時，其立即開始使用 K0 並啟動(2 個)計時器，1 個用於 K0 剩餘生命期，1 個用於 K1 何時啟動之 SA_ATD 計時器。
- 當 SA_ATD 時間逾期時，GM 切換至新的金鑰 K1。

- 當 K0 剩餘生命期值逾期時，GM 將金鑰更新請求發送予 KDC，以取得下個會期金鑰 K2。需注意，KDC 宜恆保留至少 2 個 SA，其一為現用者，另一係其 ATD 設定為非 0 之下個 SA。若建立新 SA 之觸發係依目前 SA 之逾期，則 KDC 於任何時候不宜具超過 2 個 SA。然而，若建立新 SA 之觸發係依下個 SA 之 ATD 逾期，則 KDC 可能需針對群組儲存 3 個 SA：目前、下個及新的 SA。KDC 可能於拉取期間發送所有此等 SA，因此 GM 應準備好接收。然而，若 GM 於目前金鑰逾期時發送拉取請求，而並非於下個金鑰之 ATD 逾期時發送拉取請求，則其恆僅接收 2 個 SA 及金鑰。

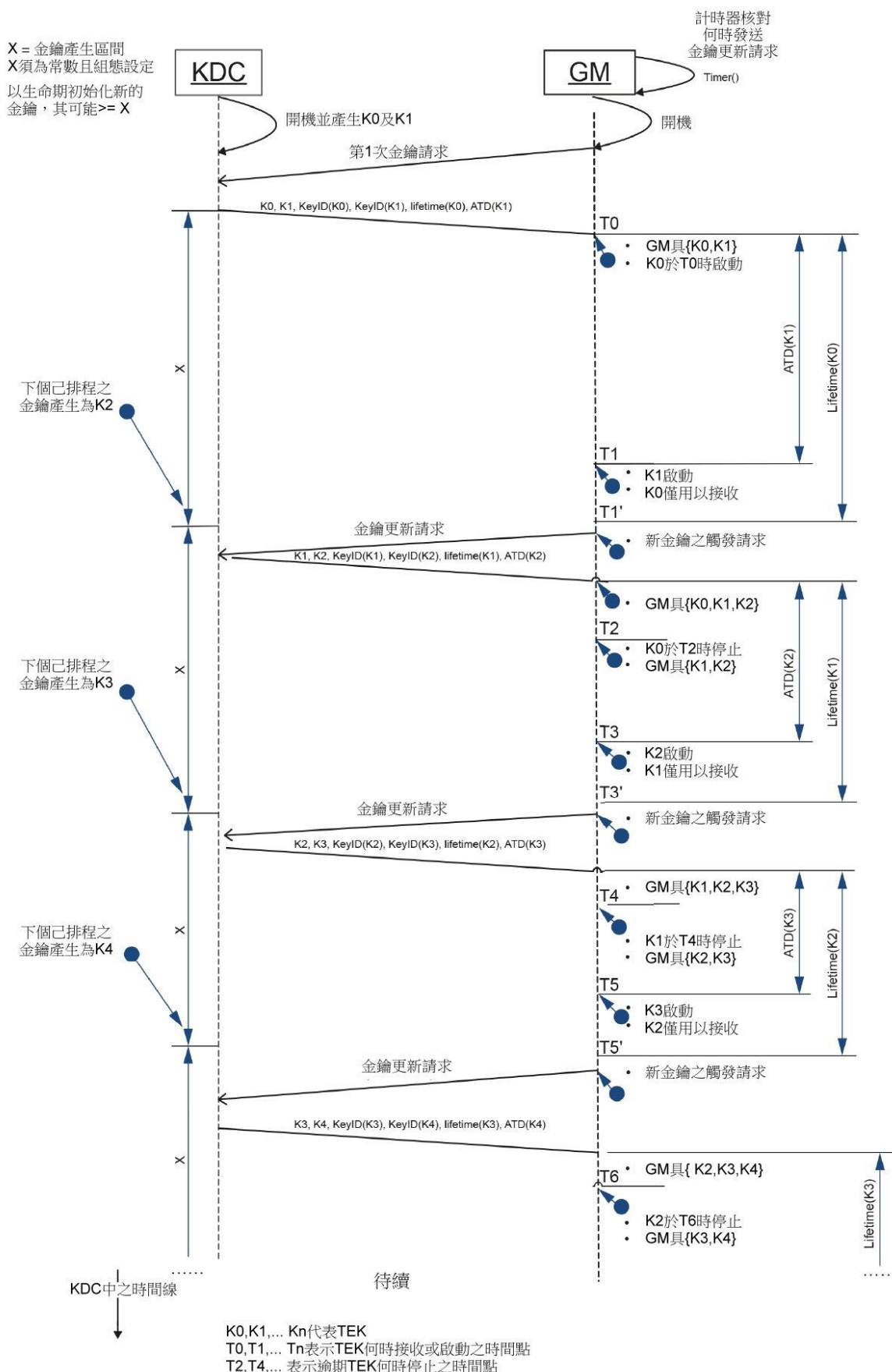


圖 42 由個體觸發之金鑰更新

若使用之 SA 逾期，則應引發事件 GROUP_PULL_EXPIRED_SA。

若 DH 演算法及金鑰大小協商不成功，則應引發 GROUP-PULL-PHASE1-KEYNEGOTIATION 事件。

若作為 GROUPKEY-PULL 階段 2 交換之一部分解密不成功，則應引發事件 GROUP_PULL_PHASE2_DECRYPTION。

若執行未知群組之金鑰的請求，則應引發 GROUP-PULL-PHASE2-GROUP-NONEXISTENT 事件。

8.5.12 TEK 金鑰下載處理

本系列標準第 9 部定義將經由 GROUPKEY-PULL 及 GROUPKEY-PUSH 所提供之 2 個金鑰下載(KD)酬載。此等 KD 具不同之啟動時間(SA_ATD)及剩餘生命期值(參照圖 42)。此等值與 1 個且僅 1 個 KEY_ID 相關，從而判定相關金鑰之使用時間及逾期時間。

8.6 階段 2 GROUPKEY-PUSH 交換型式 33

8.6.1 一般

GDOI (RFC 6407)定義階段 2 GROUPKEY-PUSH 交換，以容許 KDC 使用推播訊息將金鑰更新資訊提供予 GM (參照圖 43)。其係 ISAKMP 協定，其中密碼政策及建鑰材料(“Rekey SA”)已由 KDC 作為 GROUPKEY-PULL 交換中群組政策之一部分配送。

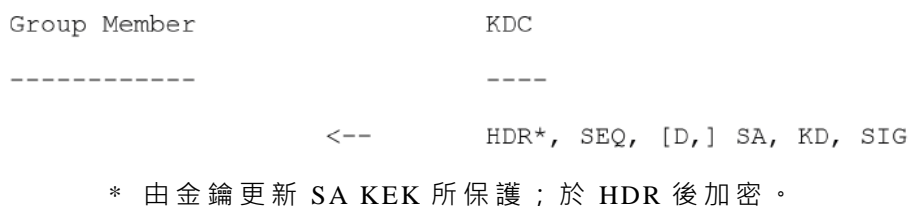


圖 43 GROUPKEY-PUSH 訊息(源自 RFC 6407)

簽章酬載係使用階段 1 交換中所指示之憑證的對應私密金鑰所建立(參照 8.3.5.3)。

KDC 可使用 GROUPKEY-PUSH 將控制資訊發送予群組以更新 SA，此亦可能導致自群組中排除一些成員。為確保 GM 已接收更新之資訊，RFC 8263 定義

GROUPKEY-PUSH 認可訊息，可用以認可對 KDC 之金鑰遞送(參照圖 44)。



圖 44 GROUPKEY-PUSH ACK 訊息(源自 RFC 8263)

8.6.2 GROUPKEY-PUSH 訊息

如圖 43 所示，當自 KDC 發送 GROUPKEY-PUSH 訊息時，應包含 SIG 酬載。依 RFC 6407，此 SIG 酬載應提供於完整之 GROUPKEY-PUSH 訊息上所計算的簽章值。此亦包括 ISAKMP 標頭 HDR。

KDC 應僅將 KEK_ACK_REQUESTED 屬性(於 RFC 8263 中定義)納入 GROUPKEY-PUSH 訊息之 SA KEK 酬載中，以避免產生 GROUPKEY-PULL 訊息的認可訊息。

若試圖將 GROUPKEY-PUSH 傳送至無法抵達之位址，則應引發 GROUP-PUSH-UNREACHABLE-DESTINATION 事件。

8.6.3 GROUPKEY-PUSH 認可訊息

RFC 8263 規定 KDC 請求 GM 使用與 KEK 相關聯之 KEK_ACK_REQUESTED 屬性，回傳接收其金鑰更新訊息的認可之能力，並規定認可方法。

如圖 44 所示，認可訊息包含 HASH 值。雜湊值依 RFC 8263 計算如下。

$$\text{HASH} = \text{prf}(\text{ack_key}, \text{SEQ} \parallel \text{ID})$$

圖 45 GROUPKEY-PUSH ACK 雜湊計算

所利用之 prf 係由對應的載送 KEK_ACK_REQUESTED 屬性之 SA-KEY 所決定。需注意(依 RFC 6407 之 5.3.5)此可直接透過 SIG_HASH_ALGORITHM 於 SA KEK 中明確定義，亦可對於演算法 SIG_ALG_ECDSA-256、SIG_ALG_ECDSA-384 或 SIG_ALG_ECDSA-521 藉由選定的 SIG_ALGORITHM 之隱式定義。

應用之 ack_key 係依 RFC 8263 自 base_key 衍生，如下所示：

$$\text{ack_key} = \text{prf}(\text{base_key}, \text{"GROUPKEY-PUSH ACK"} \mid \text{SPI} \mid \text{L})$$

圖 46 GROUPKEY-PUSH ack_key 計算

base_key 應為對應 GROUPKEY-PUSH 訊息中接收自 KDC 之金鑰。此向 KDC 提供保證可相應使用新金鑰。金鑰衍生所使用之函數應相同於 SA KEK 中所發訊者。依 RFC 8263。

- SPI：使用 I 訊錄及 R 訊錄作為 SPI。訊錄包含 PULL 交換期間所提供 SA KEK 之 SPI 的 16 位元組。此將容許匹配所關注之 GROUPKEY-PUSH 訊息。
- L：匹配 ack_key 中之位元數的長度欄位。L 應匹配 base_key 之長度。值 L 係依網路位元組順序表示為 2 個八位元組。

於本標準全景中，SA KEK 屬性係選擇於整個 GDOI 金鑰管理訊息中保持一致。因此，SA KEK 屬性係限於下列數值組合：

- SIG_HASH_ALGORITHM = 3 (對應於 SIG_HASH_SHA256)。
- KEK_ACK_REQUESTED = 1 (對應於 REKEY_ACK_KEK_SHA256)。
- 用於 ACK SIG 計算之長度“L”宜為 512 (0x02,0x00)。

或者

- SIG_HASH_ALGORITHM = 5 (對應於 SIG_HASH_SHA512)。
- KEK_ACK_REQUESTED = 3 (對應於 REKEY_ACK_KEK_SHA512)。
- 用於 ACK SIG 計算之長度“L”宜為 1024 (0x04,0x00)。

RFC 8263 規定 GM 須將認可訊息發送至 KDC 對應之 GROUPKEY-PUSH 請求的來源埠。由於需避免臨時埠以因應路徑上之 NAT 及防火牆，因此本標準強烈建議於發送 GROUPKEY-PUSH 訊息時，使用 KDC 上的埠號 848。此埠號於 IANA [51]註冊供 GDOI 使用。

依 8.6.2，GM 應僅對於所接收之包含具 KEK_ACK_REQUESTED 屬性的 SA KEK 之 GROUPKEY-PUSH 訊息，發送 GROUPKEY-PUSH ACK 訊息。

未達到對發布者提供 KDA 之等級的 GKCS，應引發 KDA-FAILURE 事件。

8.7 運作考量事項

8.7.1 一般

本節闡明用以處理群組金鑰管理之運作考量事項。

8.7.2 群組安全政策

群組安全政策宜包含有關 KDC 不可用，或由 KeyID 所識別特定金鑰於 GM 不可用之特定情況的資訊。

- 若 GM 無法抵達 KDC 且金鑰輪換時間即將到來，則應使用目前 TEK，直至 KDC 再次可用為止。GM 藉由連續使用應用協定中對應之 KeyID，發訊延長使用 TEK 金鑰。此外，GM 應發布安全事件(“警告：與 KDC 之連接不可用，延長使用 TEK”)。GM 應能組態設定為於有限時間間隔內接受使用逾期群組金鑰(TEK)安全之訊息。初始值應小於 1 小時。於此期間，GM 應嘗試重新獲得與 KDC 之連接。若 GM 於此期間無法聯繫 KDC，則可更新並於 1 小時再次後起始。於任何情況下，應使用安全事件報告此情況。
- 若 GM 偵測出其未擁有應用協定中所發訊之特定 KeyID 的 TEK，則其應立即對 KDC 啟始 GROUPKEY-PULL 請求。GM 亦應發出安全事件(“警告：目前 TEK 不可用，GROUPKEY-PULL 已啟始”)。

8.7.3 群組動態性

8.7.3.1 一般

群組可能於一段時間內保持穩定。但群組成員資格之變更可能係因新的設定或裝置替換，或識別出遭危害的裝置或其他裝置。為管理動態群組，有必要支援下列功能：

- Add(新增)：將新成員新增至群組。
- Delete(刪除)：刪除群組成員但不更新現有群組金鑰。
- Revoke(撤銷)：撤銷群組成員導致群組金鑰立即變更，並刪除遭撤銷群組成員之 KEK。

成為群組成員之先決條件係於 KDC 及 GDOI 客戶端上具信符(X.509 公開金鑰憑證)及信任錨(共同根 CA 憑證)可用性，使得能建立安全關聯。另一先決條件則為(新)群組成員(GM)組態設定 KDC 位址。客戶端與群組之關聯性係依組織的安全

政策。

此等群組功能直接與所使用的配送方法(PULL 及 PUSH)相關，以處理與該群組對應之安全參數。下列各節描述群組運作之作法。

8.7.3.2 新增群組成員

將群組成員新增至既有群組可以不同方式完成：

- PULL：GM 組態設定為群組參與，並使用 PULL 請求(GROUPKEY-PULL)查詢源自 KDC 特定群組之安全參數(KEK、TEK)。KDC 於請求之成功查證(包括鑑別)後遞送訊息。GM 能參與群組通訊(作為發布者或訂用者)。
- PUSH：若於 KDC 組態設定新 GM，則 KDC 可將目前 TEK 推播至新 GM。由於 GM 未擁有 KEK 以解密 TEK，因此其將執行 PULL 以擷取完整之安全關聯參數集(包括 KEK)。

由於新增 GM 前所交換之資料無特定的保密要求事項，因此於新 GM 之新增期間無須進行金鑰更新。

8.7.3.3 刪除群組成員

自 1 個群組中刪除群組成員無須立即自該群組中刪除 GM，因此無須立即更新金鑰。當 IED 自一檔位移至另一檔位且仍然保留與 KDC 之信任關係時，可能發生此情況。於 KDC 上，此將導致藉由將 GM 新增至不同群組以進行重新組態設定。自舊群組中刪除 GM 將於下次金鑰更新時生效，其可能以不同之方式完成：

- PULL：於下個金鑰週期前，各 GM 將使用 GROUPKEY-PULL 請求擷取新的 TEK。KDC 不將已更新之 TEK 遞送遭移除的 GM。另一方面，遭移除之 GM 預期將不要求新的 TEK。
- PUSH：金鑰更新可自 KDC 啟始，作為單播(階段 2) GROUPKEY-PUSH 資訊交換訊息，其載送依 8.6.2 中所概述之“刪除”酬載。TEK 協定 ID (GDOI_PROTO_IEC_61850)係於訊息之協定 ID 欄位中載送。然後，接收之 GM 應刪除與特定協定相關聯的 TEK，但保留 KDC 之 KEK。對所有群組成員使用具“刪除”酬載之多播 GROUPKEY-PUSH，將導致刪除群組成員處的群組關聯，且應省略。

需注意，由於 PUSH 支援係屬選項，因此有必要對支援 PULL 及 PUSH 之混合 GM 群組中的群組成員刪除進行對齊處理，以避免出現不可用情況。未支援 PUSH 之 GM 將連續使用目前的 TEK，直至下個 PULL 動作。

8.7.3.4 撤銷群組成員

撤銷 GM 須立即自群組中刪除，因此要求立即更新金鑰。當 IED 已知受危害且因此不再視為可信時，可能發生此情況。此情況下，不僅刪除 TEK，亦應變更 KEK。此過程類似於撤銷憑證。需注意，可能同時觸發憑證撤銷。群組成員之撤銷依下列方式進行：

- KDC 使用階段 2 GROUPKEY-PUSH 訊息，其中包含新的 TEK，並以新 KEK 對所有群組成員加密。此將要求所有 GM 啟始 GROUPKEY-PULL，因其未擁有新 KEK 以解密 TEK。KDC 應拒絕遭撤銷之群組成員。
- 所有 GM 將對於所指派之群組啟始安全參數的 GROUPKEY-PULL，依 8.7.3.2 中所述。遭撤銷之群組成員將遭 KDC 拒絕。需注意，此要求 GM 僅刪除特定群組之 SA 訊息，而不刪除群組資訊，使得群組成員能查詢新的安全參數。

8.7.4 金鑰遞送保證之處理(參考)

金鑰遞送保證(KDA)確保安全參數已接收並可能套用。此於所有 GM 上依新金鑰之可用性完成金鑰切換的情況下為有用。若金鑰係依時窗排程，則不宜使用。依由群組成員所接收之金鑰進行金鑰切換，如 8.5.10.3 中所述係屬選項。

GDOI 中以 2 個方向提供關於金鑰及政策資訊之遞送及接收的資訊。GM 取決於金鑰配送方法(PULL/PUSH)向 KDC 發訊 SA 參數之接收作為認可。此外，KDC 可對群組之多播來源(發布者)提供關於對所有群組參與者配送 SA 資訊的資訊(亦參照 8.5.10.3)：

- GM 向 KDC 提供 KDA，以認可接收(更新之)SA 參數(TEK)：
 - PULL：依 RFC 6407 之 3.2，GM 以 GROUPKEY-PULL 交換中的第 3 則訊息認可 TEK 及所連接政策之接收。
 - PUSH：若於 GROUPKEY-PUSH 期間由 KDC 請求，則 GM 向 KDC 發送金鑰認可。

- KDC 向 GM (群組發布者) 提供 KDA，以表示所有群組成員已收到金鑰 (TEK)。須區分此 2 種金鑰遞送方法。
 - PULL：於 PULL 情況下，KDA 僅能提供予最後擷取更新安全參數之 GM。目前除使用具資訊酬載之 GROUPKEY-PUSH 外，未向其他 GM 發送任何訊號。
 - PUSH：KDC 可使用具資訊酬載之 GROUPKEY-PUSH 對群組中的多播來源，提供有關於其他 GM 處接收 SA 資訊之資訊。群組中之 KDA 行為，其政策僅為 GROUPKEY-PULL 係屬不確定，宜避免。

9. 協定實作符合性聲明(PICS)

9.1 一般

對於宣稱符合本標準之實作，靜態符合性要求事項規定應實作什麼、可實作什麼以及不應實作什麼。

9.2 記法

下列記法係用以規定符合性要求事項：

m：必備支援。該項目應實作。

o：選項支援。該項目可但無需實作。

c：條件式支援。該項目應依條件實作。

x：排除。該項目不應支援。

9.3 一般金鑰管理要求事項之符合性

表 5 顯示一般金鑰管理之 PICS。

表 5 一般金鑰管理之 PICS

項目	說明	客戶端/伺服器	參引
G-1	要求之密碼材料。	m	6.3
G-2	隨機數產生。	m1	6.4

項目	說明	客戶端/伺服器	參引
G-3	AVL 之物件識別符分支的辨識： - AVL 延伸：avl62351Extiona。 - AVL 資料項延伸：avl62351EntryExt。 - 協定識別符 id-62351prot。	c	6.5.2
	AVL 延伸之支援： - AVL 範圍限制：scopeConstraints。 - AVL 協定限制。		7.8.3 7.8.4
	AVL 資料項延伸之支援： - 憑證之 AVL 釘住：pinningId。		7.8.5
G-4	依本系列標準第 14 部，宣告安全事件之機制。	o	6.2

m1：個體中必備支援 RNG。若個體無足夠之熵，則宜以安全的方式提供帶外種子。

c：若支援 AVL，則可支援所述之 AVL 延伸及 AVL 資料項延伸。

9.4 非對稱金鑰管理要求事項之符合性

表 6 顯示非對稱金鑰管理之 PICS。

表 6 非對稱金鑰管理之 PICS

項目	說明	終端個體	PKI	參引
A-1	依表 1 之公開金鑰憑證組件。	m	m	7.2.1
A-2	依表 2 之屬性憑證組件。	o	m	7.2.2
A-3	私密及公開金鑰產生及安裝。	m	m	7.3.1
A-4	密碼金鑰保護。	m	m	7.3.2
A-5	既有安全金鑰管理基礎建設之使用。	o	m	7.3.3
A-6	識別資訊建立之個體註冊。	-	m	7.3.5
A-7	個體組態。	m	-	7.3.6
A-8	個體登錄。	o1	m1	7.3.7
A-9	信任錨資訊更新。	o	o	7.3.8
A-10	公開金鑰憑證查證。	m	m	7.4.3 及 7.4.4
A-11	屬性憑證查證。	o	m	7.4.3 及 7.4.5
A-12	憑證撤銷。	c	m	7.5
A-13	憑證逾期及更新。	m	m	7.6

項目	說明	終端個體	PKI	參引
A-14	時鐘同步及準確度。	m	m	7.7
A-15	安全時間同步。	o	o	7.7
A-16	鑑別授權驗核清單之支援。	o	o	7.8
o1：個體之金鑰管理可為人工/EST/SCEP。 m1：PKI 須支援以 SCEP 及 EST 自動登錄。 c：終端個體應支援 CRL 或 OCSP 中至少 1 種撤銷機制。				

9.5 群組式金鑰管理之要求事項

表 7 顯示群組式金鑰管理之 PICS。

表 7 群組式金鑰管理之 PICS (對 KDC 及客戶端有效)

項目	說明	m/o/c	參引
S-1	群組式金鑰管理。	c	8
S-2	GDOI 要求事項。	c	8.1
S-3	網際網路金鑰交換版本 1 (IKEv1)。	c	8.2
S-4	階段 1 IKEv1 主模式交換型式 2。	c	8.3
S-5	階段 1/2 資訊訊息。	c	8.4
S-6	階段 2 GDOI PULL 交換。	c	8.5
S-7	階段 2 GDOI PUSH 交換。	o	8.6
c：當支援 GOOSE 或 SV 安全時。			

9.6 支援之 GDOI 酬載 OID

表 8 所示之 PICS 係針對支援 GDOI 的情況，使得為 GOOSE、SV 或 PTP 整合安全提供金鑰材料及安全政策。

表 8 識別酬載支援之 OID 的 PICS

項目	說明	m/o/c		參引
		客戶端	KDC	
P-1	61850_ETHERNET_GOOSE	o	m	8.5.5.2.2
P-2	61850_UDP_ADDR_GOOSE	o	m	8.5.5.2.2
P-3	61850_UDP_Tunnel	o	o	8.5.5.2.2
P-4	61850_ETHERNET_SV	o	m	8.5.5.2.2
P-5	61850_UDP_ADDR_SV	o	m	8.5.5.2.2

		m/o/c		
項目	說明	客戶端	KDC	參引
P-6	61850_IP_ISO9506	o	o	8.5.5.2.2
P-7	61850_9_3_PTP	o	o	8.5.5.2.2

附錄 A

(參考)

與本系列標準其他各部及其他 IEC 標準之關係

圖 A.1 說明本標準與本系列標準其他部間之連接。

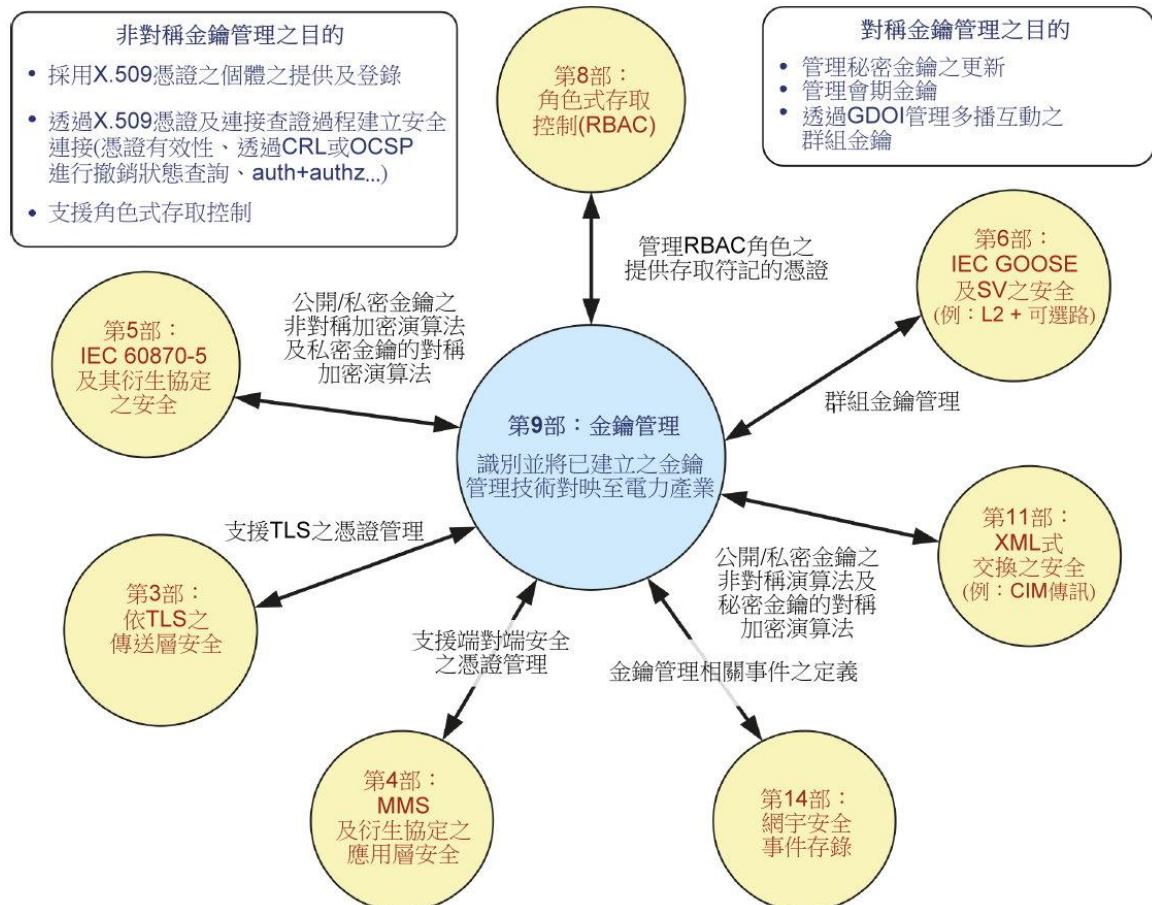


圖 A.1 本標準與本系列標準其他部之關係

本系列大多數標準使用非對稱金鑰，主要用於對稱金鑰之鑑別及安全傳送或協商：

- 本系列標準第 3 部。
- 本系列標準第 4 部。
- 本系列標準第 5 部。
- 本系列標準第 6 部。
- 本系列標準第 8 部。
- 本系列標準第 11 部。

本系列大多數標準需對稱金鑰配送。聚焦於應用層使用對稱金鑰之本系列標準各部上。此主要與本系列標準第 5 部、第 6 部，以及 CNS 61850-90-5 中群組式金鑰管理作法相關。對於使用 TLS 之各部，對稱金鑰處理係封裝於 TLS 自身，此可能僅是政策議題(密碼套組)。

- 本系列標準第 3 部及第 4 部，作為 TLS 交握之一部分。
- 本系列標準第 5 部用以保護 CNS 60870-5 及其衍出協定。
- 本系列標準第 6 部用以保護 GOOSE 及取樣值(SV)，以及 R-GOOSE 及 R-SV。
- 本系列標準第 8 部適用於 C 剖繪。

本系列標準第 10 部提供建議及指導綱要，而本標準則直接闡明金鑰處理之要求事項。

本系列標準第 14 部提供安全事件日誌存錄，亦可用於金鑰管理。本標準之安全事件係於整個標準中定義，並於附錄 D 中對映至本系列標準第 14 部。

附錄 B

(參考)

密碼演算法及機制

B.1 信任及信任錨

需要信任係保全數位通訊之重要組件。個體(系統或裝置)宜僅接受具其可鑑別並信任之個體的資料(通訊)(參照 4.2.3)。公開金鑰憑證藉由斷言公開金鑰憑證與唯一個體之關聯，提供基礎以建立此種信任。對於特定公開金鑰憑證之信任係藉由驗核其根係於信任錨中的所謂憑證路徑所建立，該信任錨受進行驗核之個體(亦稱為依賴方)所信任。憑證路徑係公開金鑰憑證鏈，起始於信任錨簽署之公開金鑰憑證，結束於待驗核的公開金鑰憑證。憑證路徑末端之公開金鑰係終端個體公開金鑰憑證。其他公開金鑰憑證(若有)則為 CA 憑證。ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)之第 6 節、7.5 及 7.7 進一步描述依賴方、信任錨及憑證路徑的概念。於某些情況下，可於信任錨與依賴方間直接建立信任。然而，若此等各方間之直接存取不可行，則可建立信任鏈(電力系統運作經常出現該情況)。若依賴方接受源自與其有信任關係之個體的公開金鑰憑證，則可不經過完整憑證路徑，而依賴信任鏈驗核該公開金鑰憑證。於此情況下，公開金鑰憑證可能無需由信任錨核發並簽署，而是可由已建立回至信任錨之信任鏈的憑證機構簽署。

對於電力系統實作，憑證機構可能為公司內的相關組織單位、公司自身、政府個體或公認第三方。

公開金鑰數位憑證之效期係屬有限，期限之後即逾期。依賴方於使用中遭破解或變更時，信任亦可能遭撤銷。公開金鑰憑證之管理與密碼金鑰管理密切相關，因此涵蓋於本標準中。

亦參照 5.7 及 5.8。

B.2 密碼演算法

B.2.1 簡介

安全密碼演算法係安全政策之重要組件。因此，其於 PKI 及相關技術中發揮重要

作用，諸如 IETF RFC 8446 定義之傳送層安全(TLS)。密碼演算法之詳細說明超出本標準範圍。關於較詳細的規格，旨在提供足夠之資訊，給予概念的高層次理解。

對於語法規格，協定未使用 ASN.1，通常使用字串或類似內容以識別密碼演算法。此種字串通常由網際網路指配號碼機構(Internet Assigned Numbers Authority, IANA)註冊以確保唯一性。例：

(a) TLS 於稱為密碼套組之通訊實例中使用多種密碼演算法。密碼套組係由 IANA 註冊之 2 個八位元組識別符所識別。需注意，本系列標準第 3 部中處理電力系統密碼套組之建議。

(b)於其他情況下(如網際網路金鑰交換版本 2 (IKEv2))，密碼演算法係同時由字串及整數所識別。

當抽象語法記法 1(ASN.1)用於通訊協定規格時，密碼演算法係由物件識別符所識別，且若相關，則藉由演算法型式之特定參數所識別。對於使用 ASN.1 記法識別協定規格中之密碼演算法，ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019) 使用下列 ASN.1 資訊物件類別：

```
ALGORITHM ::= CLASS {
    &Type          OPTIONAL,
    &DynParms      OPTIONAL,
    &id            OBJECT IDENTIFIER UNIQUE }
WITH SYNTAX {
    [PARMS          &Type]
    [DYN-PARMS     &DynParms]
    IDENTIFIED BY  &id }
```

其中，&Type 欄位用以規定參數(若有)，則提供額外演算法規格，當部署密碼演算法時，&DynParms 欄位規定相關參數。

密碼演算法定義於許多不同之規格中，通常於 IETF RFC 及美國國家標準與技術研究院(NIST)標準中定義。為方便參考並易於導入 ASN.1 模組，ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)之附錄 B 提供某些相關密碼演算法定義的複本。

密碼演算法之安全性質取決於：

(a)演算法之安全參數。此係於 B.2.2 中討論。

(b) 電腦之處理速度，其判定藉由暴力破解演算法的可行性，亦即嘗試所有可能性。據稱，可能存在擁有豐富運算能力之對手。

(c) 使用中之密碼演算法。演算法可能具容許熟練數學家發現無須完全暴力攻擊之方法以破解其功能。

演算法之實作方式可能無法提供理論上宜提供的安全等級。例：若使用較差之隨機數產生器產生密碼金鑰，則某些值較其他值更可能出現。對手可利用此減少揭露金鑰之工作量。

B.2.2 安全強度

安全強度係與破解密碼演算法所需工作量(亦即某種運算之數量)相關聯的數字。安全強度以“位元數”表示，且為源自集合{80, 112, 128, 192, 256}之離散值。NIST SP 800-57 Part 1 revision 5 [57]及德國 BSI TR 02102-1 [58]包含安全強度之詳細考量。

B.3 公開金鑰演算法

B.3.1 一般

於非對稱密碼中，對個體指派 2 個數學上相關之金鑰，其一為使用者假設保護其不遭破解的私密金鑰，另一為可較自由配送的公開金鑰。儘管此 2 個金鑰係相互關聯，但自對應之公開金鑰判定私密金鑰視為不可行。

若公開金鑰以破解私密金鑰之方式遭破解，或已知私密金鑰遭破解，則應受保護的資料現在就不受保護。例：有可能產生假數位簽章。

NIST FIPS PUB 186-5 [64]係由 NIST 所發布關於數位簽章議題之指導。除規定數位簽章演算法外，亦包括公開金鑰演算法規格。

B.3.2 RSA 公開金鑰演算法

B.3.2.1 一般

RSA (Rivest-Shamir-Adleman)係最早公開金鑰密碼系統之一。RSA 為 Ron Rivest、Adi Shamir 及 Leonard Adleman 等人姓氏之首字母縮寫。RSA 公開金鑰演算法係目前最常使用之公開金鑰演算法。

RSA 公開金鑰演算法可與不同金鑰長度(例：2048 位元、3072 位元、4096 位元)

一起使用。與其他某些公開金鑰演算法相較，RSA 公開金鑰演算法亦容許加密資料。由公開金鑰加密之資料可由對應的私密金鑰解密，反之亦然。加密/解密過程繁重，宜僅用於下列 2 個目的：

(a)數位簽章產生及查證。

(b)對稱金鑰之傳送。

不建議將用作數位簽章金鑰之私密金鑰用於金鑰傳送。

B.3.2.2 金鑰產生

RSA 公開金鑰由模數 n 及公開金鑰指數 e 組成，亦即公開金鑰為 (n,e) 。模數 n 為 2 個正值大質數 p 及 q 之乘積，亦即 $n = p \times q$ 。公開金鑰指數 e 限制於由 n 、 p 及 q 所決定之特定範圍內。通常使用質數值 $2^{16} - 1 = 65537$ 。

RSA 私密金鑰由相同模數 n 及私密金鑰指數 d 組成，亦即私密金鑰為 (n,d) ，其中私密金鑰指數 d 亦滿足由 e 、 p 及 q 所決定之某些數學要求，以此方式，若 p 及 q 已知，則可計算 d 。

B.3.2.3 安全考量事項

模數 n 及公開金鑰指數係公開可用，因此非秘密。私密金鑰指數 d 須保密。然而，若已知 2 個因數 p 及 q ，則可計算 d 。RSA 私密金鑰之安全取決於當已知乘法 n 時，找出此 2 個因數的難度。此稱為因式分解問題。事實證明，若公開金鑰足夠長，即使強大之電腦亦無法找出此 2 個因數。

備考：量子電腦之出現可能改變此點。參照 B.9。

關於 RSA 演算法使用之最小金鑰長度有不同建議。常用之參考資料包括 NIST SP 800-57 第 1 部 [57] 及德國 BSI TR 02102-1 [58] 建議的可接受金鑰長度。依德國 BSI TR 02102-1，至少至 2023 年，2048 位元金鑰大小係視為足夠。宜依組織之安全政策謹慎處理 2048 位元金鑰長度的使用。強烈建議切換至最小金鑰長度 3072 位元。

B.3.3 DSA 公開金鑰演算法

數位簽章演算法(DSA)演算法最初定義於 FIPS PUB 186 [63] 中。其係由美國國家安全局(NSA)所開發。然而，於 FIPS 186-5 [64] 中，NIST 不容許該演算法用以產

生數位簽章，僅容許其用以查證數位簽章。

B.3.4 ECDSA 公開金鑰演算法

B.3.4.1 一般

橢圓曲線數位演算法(ECDSA)係 1 組依橢圓曲線密碼學(ECC)之密碼學安全公開金鑰演算法。ECC 加密技術優於 RSA 加密系統，因 ECC 針對相同等級之安全使用較 RSA 為小之金鑰及簽章，並容許快速金鑰產生、快速金鑰協議及快速簽章處理。

ECDSA 係依一般橢圓曲線方程式之 1 組演算法的規格，亦稱為 Weierstrass 曲線：

$$y^2 = x^3 + ax + b$$

此曲線係於質數域 p 上，其中 p 為大奇質數。此將產生：

$$y^2 \equiv x^3 + ax + b \pmod{P}$$

此公式產生具整數座標之曲線點群組。B.8.2 中之討論之循環群(cyclic group)概念亦可套用於曲線點上。其能證明，定義點之子群組形成循環群。其亦能證明，曲線上之點數目除以此種子群組中點“ n ”的點數目恆為整數，稱為共因數(cofactor)“ h ”。若共因數為“1”，則曲線上之所有點形成循環群。精心選擇之曲線的共因數為“1”。

特定曲線規定為 1 組參數，稱為域參數(domain parameter)。上述方程式中之曲線參數“ a ”、“ b ”及“ p ”即為 3 個此種域參數。其他參數為子群組中點“ n ”之數量及共因數 h 。曲線上用作定義子群組基礎的之點稱為生成元(generator)點“ G ”，亦屬域參數。此域參數係由曲線設計者所精心選擇。

針對某些 a 及 b 值，滿足上述方程式之座標 (x,y) ，且其中 x 及 y 係等於或大於 0 且小於 p 的整數，形成與 ECDSA 演算法規格相關之座標群組。

曲線之 1 組域參數係指派物件識別符，然後其識別特定之 ECDSA 演算法。

NIST FIPS 186-5 [64]為 ECDSA 公開金鑰演算法提供補充資訊。

ECDSA 係依 IETF RFC 3279 [81]正式規定為：

```
ecPublicKey ALGORITHM ::= {
    PARMS          OBJECT IDENTIFIER
```

```
IDENTIFIED BY id-ecPublicKey }
id-ecPublicKey OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-x962(10045) keyType(2) ecPublicKey(1) }
```

所有 ECDSA 曲線係由此資訊物件所識別，而 PARMS 欄位則藉由指派之物件識別符識別個別曲線。

B.3.4.2 定義曲線

本標準認可下列 Weierstrass 橢圓曲線：

(a) secp256r1 (NIST 稱為 P-256)係 256 位元質數域上之橢圓曲線。假設具 128 位元安全等級。

SEC 2 2.0 版中提供質數及其他參數的建議值。

(b) BrainPoolP256r1 亦為 256 位元質數域上之橢圓曲線。其亦假設具 128 位元安全等級。

IETF RFC 5639 中提供質數及其他參數之建議值。

依 IETF RFC 5480 [82]，下列物件識別符指派予 secp256r1：

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
ansi-x9-62(10045) curve(3) prime(1) 7 }
```

依 IETF RFC 5639 [37]，下列物件識別符係配置予 brainpoolP256r1：

```
brainpoolP256r1 OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) teletrust(36) algorithm(3) signature-algorithm(3)
ecSign(2) ecStdCurvesAndGeneration(8) ellipticCurve(1)
versionOne(1) brainpoolP256r1(7) }
```

B.3.4.3 金鑰產生

針對上面討論之 2 條曲線，私密金鑰係產生為 256 位元隨機位元串。

對應之公開金鑰係橢圓曲線上點之座標，亦即公開金鑰係由 2 個部分作成，x 值及 y 值。其係採取曲線上之點(稱為生成元) G，並使用橢圓曲線的特殊乘法規則將該點與私密金鑰相乘所計算。G 針對特定曲線係固定，且為曲線參數之一。

公開金鑰可表示為：

$$P = k \circ G$$

其中 P 為公開金鑰，k 為私密金鑰， \circ 為特殊乘號。

$$P = k \circ G$$

曲線上之點可能以未壓縮形式給定，亦即 x 座標及 y 座標的序聯。亦可能以壓縮形式給定點，其中僅給定 x 座標，然後可自曲線方程式計算 y 座標。

其中 y 可取正值 y_1 及負值 $-y_1$ 。作為模算術 $y_2 \equiv (-y_1 + p)$ 於 $\{0, \dots, p-1\}$ 範圍內取值之結果，得出 y 座標之 2 個值 y_1 及 y_2 。必然地，若 1 個值為偶數，則另一值為奇數，反之亦然。

若 $P = k \circ G$ 產生偶數 y 值，則 x 座標以 0x02 八位元組為前綴，若其產生奇數 y 值，則 x 值以 0x03 八位元組為前綴。

若使用未壓縮的形式，結果將以 0x04 八位元位元組為前綴。

B.3.4.4 安全議題

B.3.4.4 Security issues

依前文所指示，公開金鑰之計算方式為：

$$P = k \circ G$$

當私密金鑰 k 已知時計算公開金鑰 P 係快速運算。知悉公開金鑰 P 並嘗試發現私密金鑰 k 以滿足上述方程式並無有效因應方案(針對精心選擇之有限域及橢圓曲線)。此稱為橢圓曲線離散對數問題(ECDLP)。

備考：量子計算機之出現可能變更此。參照 B.9。

B.3.5 EdDSA 公開金鑰演算法

B.3.5.1 一般

Edwards 曲線數位簽章演算法(EdDSA)亦為加密安全之公開金鑰演算法。其與 ECDSA 大不相同。而為 ECDSA 定義之 det 曲線係 B.3.4.1 中所提及 Weierstrass 曲線的變異。

EdDSA 係依一般扭曲之 Edwards 曲線：

$$ax^2 + y^2 = 1 + dx^2y^2$$

使用此一般方程式僅定義 2 種曲線。曲線型式背後之數學原理不同用於 Weierstrass 曲線者，導致產生公開金鑰及數位簽章的技術不同。

扭曲 Edwards 曲線為一般 Montgomery 曲線(雙有理等價)之變異。

$$By^2 = x^3 + Ax^2 + x \bmod p$$

Montgomery 曲線係用於標記為 X25519 及 X448 之 2 個金鑰協議(Diffie Hellman) 演算法。

用於 EdDSA 之 2 種曲線稱為 Edwards15519 及 Edwards448。

用於金鑰協議之 2 種曲線稱為 Curve15519 及 Curve448。

相較於其他型式數位簽章演算法，2 種所定義曲線以相關聯雜湊演算法作為參數，SHA512 規定用於 Curve25519/Edwards25519 曲線，且 SHAKE256 規定用於 Curve448/Edwards448 曲線。

EdDSA 較 ECDSA 具某些優勢：

- (a) 具較佳性能。
- (b) 針對各調用，無須唯一隨機數。
- (c) 對側通道攻擊更具韌性。
- (d) 小的公開金鑰及簽章。

NIST FIPS 186-5 [64]提供有關 EdDSA 公開金鑰演算法的補充資訊。

B.3.5.2 定義之曲線

下列曲線係與本標準相關。

- (a) Ed25519：其依具 $p = 2^{255} - 19$ 之下層質數域。其私密金鑰大小為 256 位元。

假設具 128 位元安全等級。

- (b) Ed448：其依具 $p = 2^{448} - 2^{224} - 1$ 之下的質數域。其私密金鑰大小為 256 位元。假設具 224 位元安全等級。

IETF RFC 7748 [43]規定上述曲線的參數。

依 IETF RFC 8410 [79]，針對 Ed25519 及 Ed448 指派下列物件識別符：

```
id-Ed25519 OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
thawte(101) 112 }
```

```
id-Ed448 OBJECT IDENTIFIER ::= { iso(1) identified-organization(3)
thawte(101) 113 }
```

B.3.5.3 金鑰產生

IETF RFC 8032 [77]於 5.1.5 及 5.2.5 中規定 2 種曲線之金鑰產生。

針對 Ed25519 曲線，私密金鑰產生為 256 位元隨機位元串，而 Ed448 曲線則產生 456 位元隨機位元串。

公開金鑰之產生極不同於 ECDSA。針對 2 種曲線，涉及私密金鑰之雜湊。此意指雜湊演算法為 2 種曲線之域組件的一部分。針對 Ed25519，使用 SHA512，針對 Ed448，使用 SHAKE256。

如 B.3.4.3 中針對 ECDSA 所討論，公開金鑰之計算方式為曲線點乘以私密金鑰，且私密金鑰政策上可由對手透過求解 ECDLP 衍生。針對 EdDSA，公開金鑰係產生自私密金鑰之雜湊值，可表示為：

$$P = 'HASH'(k) \circ G$$

然而，由於私密金鑰之雜湊產生的摘要大小為私密金鑰 2 倍，因此僅使用摘要前半部分進行上述計算。

B.3.5.4 安全議題

自 B.3.5.3 可看出，求解 ECDLP (參照 B.3.4.4) 將不產生私密金鑰，而是私密金鑰之半雜湊。然而，可證明，此足以讓對手產生驗證者將接受之簽章。

IETF RFC 8032 [77] 之安全考量部分提供關於安全議題的細節。

B.3.5.5 簽章演算法及查證

IETF RFC 8032 [77] 提供關於簽章產生及查證之細節。

B.3.6 數位簽章演算法

B.3.6.1 一般

私密金鑰及對應之公開金鑰係數學上相關，亦即由私密金鑰所進行之某些運算可由公開金鑰解開，且於某些情況下反之亦然。因此，可使用私密金鑰產生數位簽章，並可藉由公開金鑰以查證數位簽章。

數位簽章涉及雜湊演算法。某些公開金鑰演算法容許於多種雜湊演算法間選擇。RSA 及 ECDSA 公開金鑰演算法即為此情況。當用作數位簽章演算法時，此種組合需其自有識別資訊以供參考。

某些公開金鑰演算法具特定雜湊演算法作為其參數一部分，其法亦用於數位簽章的產生及查證。針對此種公開金鑰演算法，當用作數位簽章演算法時，無需不同

之識別。

B.3.6.2 RSA 數位簽章演算法

B.3.6.2.1 一般

RSA 公開金鑰演算法可連同所選擇之雜湊演算法構成 1 組數位簽章演算法。

有 2 種產生及查證數位簽章之方案：

(a) RSA PKCS#1 v1.5。

(b) RSA-PSS

兩方案使用相同基本技術。由發送者使用安全雜湊演算法雜湊處理待使用 RSA 數位簽章演算法簽署之資料，然後使用私密金鑰加密摘要以產生簽章。接收者使用對應之公開金鑰解密所接收之加密摘要，並於所接收資料上產生自有摘要。若 2 個摘要相同，則數位簽章得以查證。

所產生摘要之加密極簡單。若 d 為私密金鑰指數， n 為模組(參照 B.3.2.2)， m 為待加密訊息轉換為整數後之摘要，則加密摘要 c 為：

$$c = m^d \pmod{n}$$

解密亦同樣簡單。若 e 係公開金鑰指數，則解密後之 m 係由下式所給定：

$$m = c^e \pmod{n}$$

B.3.6.2.2 RSA PKCS#1 v1.5 方案

IETF RFC 8017 附錄 A 中列出多種 RSA PKCS#1 數位簽章演算法。本標準之相關數位簽章演算法為：

(a) sha256WithRSAEncryptionAlgorithm.

(b) sha512WithRSAEncryptionAlgorithm.

此 2 種數位簽章演算法具下列正式規格：

```
sha256WithRSAEncryption ALGORITHM ::= {  
  PARMS NULL  
  IDENTIFIED BY { pkcs-1 sha256WithRSAEncryption(11) };  
sha512WithRSAEncryption ALGORITHM ::= {  
  PARMS NULL  
  IDENTIFIED BY { pkcs-1 sha512WithRSAEncryption(13) };  
pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)  
  rsadsi(113549) pkcs(1) }
```

B.3.6.2.3 RSA PSS 方案

RSA-PSS 數位簽章演算法正式規定為

```

rSASSA-PSS ALGORITHM ::= {
  PArms      RSASSA-PSS-params
  IDENTIFIED BY {pkcs-1 10} }
RSASSA-PSS-params ::= SEQUENCE {
  hashAlgorithm      [0] AlgorithmIdentifier DEFAULT sha-1,
  maskGenAlgorithms  [1] AlgorithmIdentifier DEFAULT mgf1SHA1,
  saltLength          [2] INTEGER              DEFAULT 20,
  trailerField        [3] TrailerField          DEFAULT trailerFieldBC,
  ... }

```

僅規定 1 種演算法，因其使用雜湊演算法作為參數之一。

亦有某些其他參數指示該演算法較 B.3.6.1 中討論者更複雜。細節超出本標準範圍。有關細節，參照 IETF RFC 8017。

B.3.6.3 ECDSA 數位簽章演算法

B.3.6.3.1 一般

相同於 RSA 公開金鑰演算法，ECDSA 公開金鑰演算法可連同所選擇之雜湊演算法構成數位簽章演算法系列。

針對相同等級之安全，ECDSA 的數位簽章大小較 RSA 為小。

針對簽章產生，對待簽署之資料進行雜湊。由於 ECDSA 未支援加密/解密，因此採用另一方式使用私密金鑰產生簽章。查證依循使用 NIST FIPS 186-5 [64]中所述公開金鑰之相同規則。

B.3.6.3.2 ECDSA 簽章演算法之正式規格

IETF RFC 5758 [80]中列出多種 ECDSA 數位簽章演算法。本標準相關之數位簽章演算法為：

- (a) ecdsa-with-SHA256-Algorithm.
- (b) ecdsa-with-SHA512-Algorithm.

此 2 種演算法具下列正式規格：

```

ecdsa-with-SHA256-Algorithm ALGORITHM ::= { - IETF RFC 5758
  IDENTIFIED BY { iso(1) member-body(2) us(840) ansi-x962(10045)
    signatures(4) ecdsa-with-SHA2(3) 2 }}
ecdsa-with-SHA512-Algorithm ALGORITHM ::= { - IETF RFC 5758
  IDENTIFIED BY { iso(1) member-body(2) us(840) ansi-x962(10045)
    signatures(4) ecdsa-with-SHA2(3) 4 }}

```

B.3.6.3.3 數位簽章產生及查證

待簽署之訊息經雜湊處理，然後轉換為整數，作為數位簽章產生及查證的第一步。

數位簽章的產生係依：

- (a) 私密金鑰。
- (b) 橢圓曲線上之 1 組曲線點(元素)的生成元點。
- (c) 群組中元素之數量。
- (d) 由安全隨機數產生器產生之安全隨機數。或者，可依待簽署之訊息及稱為確定性 ECDSA 的私密金鑰產生秘密數字。

數位簽章的驗證係依：

- (a) 數位簽章。
- (b) 公開金鑰。
- (c) 群組中之元素數。

B.4 對稱金鑰演算法

B.4.1 串流加密相對於區塊加密

對稱金鑰係用於 2 種主要型式之加密，亦即區塊加密(block cipher)及串流加密(stream cipher)。

區塊加密一次處理具固定區塊大小之資料區塊。若待加密資料之長度並非區塊大小的倍數，則將資料填墊，亦即於加密前新增虛擬八位元組以形成加密區塊大小之倍數。此等八位元組隨後於解密階段剝離。

串流加密一次處理 1 個小單元資料(通常為八位元組甚至位元)。此容許加密處理任意數量之資料而無需填墊。

B.4.3 至 B.4.4 中僅考量區塊加密。

B.4.2 先進加密標準

AES 係屬區塊加密，區塊大小為 128 位元(16 個八位元組區塊大小)。因此，待加密資料係分割為 128 位元區塊，且此等區塊係逐一加密/解密。定義 3 種金鑰大小：128 位元大小、192 位元大小及 256 位元大小。

NIST FIPS 197 係 AES 區塊如何加密/解密的基本規格。

針對不同之 AES 模式，分別規定如何組合區塊以實作完整的加密/訊息加密。下列討論與本標準相關之 2 種模式。

區塊的加密/解密會經歷某些步驟，然後依對稱金鑰的大小再次重複幾輪。

B.4.3 先進加密標準 - 加密區塊鏈接(AES-CBC)

先進加密標準 - 加密區塊鏈接(AES-CBC)對稱金鑰演算法已廣泛使用。有 3 種 AES-CBC 對稱金鑰演算法之金鑰大小變異(128 位元、192 位元及 256 位元)。僅 128 位元變異及 256 位元變異與本標準相關。

於加密區塊鏈接中，明文(plain text)之第 1 個區塊係藉由將其與區塊大小相同之隨機產生的位元串“XOR”所修改，稱為初始化向量。使用對稱金鑰加密該結果，其產生密文(cipher text)之區塊。然後使用該密文區塊修改(“XOR”)的第 2 個明文區塊，並加密該結果。然後，使用第 2 個所得出之密文區塊修改第 3 個明文區塊，依此類推，直至所有區塊以序連之密文區塊加密為最終結果。

當訊息並非區塊大小倍數時，將填墊訊息。IETF RFC 2315 中定義之 PKCS#7 規定最常用之填墊技術。基本想法為填墊之最後八位元組告知容許接收者於解密後刪除填墊的長度。為避免歧義，即使訊息為區塊大小之精確倍數，亦對其填墊。初始化向量係使用隨機數產生器所產生，且針對演算法的各調用產生新值。然而，初始化向量並非秘密值。其亦用於解密，且以明文形式傳送予接收者。

先於 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)·B.2.1 中列出之 ALGORITHM 資訊物件類別並無 DYN_PARMS 欄位，但依 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)，AES 演算法現須此欄位。此要求重新定義演算法並配置新的物件識別符。新定義係由 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)所定義。

ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)已針對密碼演算法配置下列物件識別符分支弧：

id-algo OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) ds(5) algo(44)

2 種 AES-CBC 演算法之正式定義為：

```
aes-cbc128 ALGORITHM ::= {
    DYN-PARMS  AES-InitializationVector
```

```
IDENTIFIED BY {id-algo aes(2) 1 } }

aes-cbc256 ALGORITHM::= {
  DYN-PARMS AES-InitializationVector
  IDENTIFIED BY {id-algo aes(2) 3 } }
AES-InitializationVector::= OCTET STRING (SIZE (16))
```

B.4.4 先進加密標準 - 計數器模式(AES-CTR)

先進加密標準 - 計數器模式(AES CTR)使用計數器模式技術，其中 128 位元計數器區塊由 2 個欄位組成，亦即單次隨機數欄位與計數器欄位序連。

初始計數器值係用於明文之第 1 區塊。產生之計數器區塊係 AES 所加密，並將結果與第 1 個明文區塊 XOR 以建立第 1 個密文區塊。後續明文區塊以相同方式處理，針對各所處理之區塊，不同處在於計數器將增加固定值。整個過程使用相同單次隨機數。然而，重要的是針對各待加密訊息產生新的單次隨機數。

如 B.4.3，有必要使用 ISO/IEC 9595-11 | Rec. ITU-T X.510 所定義之新定義。

2 種 AES-CTR 演算法之正式定義為：

```
aes-ctr128 ALGORITHM::= {
  DYN-PARMS CtrNonce
  IDENTIFIED BY {id-algo aes(2) 13 } }

aes-ctr256 ALGORITHM::= {
  DYN-PARMS CtrNonce
  IDENTIFIED BY {id-algo aes(2) 15 } }

CtrNonce::= OCTET STRING (SIZE (8))
```

此處選定之初始計數器區塊結構係 NIST SP 800-38A 之 B.2 中規定的第 2 種作法。

計數器區塊之大小為 16 個八位元組。最左邊(最顯著)之 8 個八位元組持有單次隨機數，而其餘 8 個八位元組則用作計數器欄位。訊息第 1 個區塊之計數器欄位應具十六進位值 0x0000 0000 0000 0001。針對訊息之各後續區塊，計數器應增加 `1`。

B.5 雜湊演算法

雜湊演算法係關於如何取得任意訊息(位元串)，並產生稱為摘要之固定長度雜湊值的規範。好的雜湊演算法係設計為滿足下列性質：

- (a) 其係單向演算法，意指其於計算上無法反轉該演算法以發現對映於特定摘要之訊息。
- (b) 於不變更摘要之情況下修改訊息係屬不可行。
- (c) 具抗重複性(collision resistant)，意指於計算上無法發現對映於相同摘要之任意 2 個不同訊息。
- (d) 即使輸入位元串發生小變動，亦會致輸出摘要發生不可預測之變動。

雜湊演算法之應用可用於不同目的，包括：

- (a) 完整性保護。
- (b) 數位簽章過程之一部分。
- (c) 用以產生特徵。
- (d) 產生金鑰雜湊訊息鑑別碼(HMAC)。
- (e) 金鑰衍生函數，亦即自共享秘密值(諸如密碼)衍生 1 或多個對稱金鑰之函數。
- (f) 隨機數產生。

NIST 於 FIPS PUB 180-4 [66]中發布針對所謂安全雜湊演算法(SHA)之規格，以取代先前視為不夠安全的雜湊演算法。此規格定義 SHA-1、SHA-224、SHA-256、SHA-512、SHA-512/224 及 SHA-512/256。SHA-1 現遭視為不安全，因此不再進一步考量。為確保互通，本標準僅考量 SHA-256 及 SHA-512。

適用於少於 264 位元訊息之 SHA-256 產生 256 位元(32 個八位元組)的摘要，並假設具 128 位元之安全等級。

SHA-512 適用於少於 2^{128} 位元之訊息產生 512 位元(64 個八位元組)的摘要，並假設安全等級為 256 位元。

產生摘要時，SHA-256 於 64 個八位元組的區塊大小進行運算，而 SHA-512 使用 128 個八位元組的區塊大小。

B.6 完整性核對值(ICV)演算法

B.6.1 一般

完整性核對值(ICV)，亦稱為訊息鑑別碼(MAC)，係依 ICV 演算法所產生或查證，其將待保護之資料及對稱金鑰作為輸入。僅當 2 個通訊個體共享相同之對稱金鑰

時才可使用。ICV 於傳送前新增至待保護之訊息中。ICV 與數位簽章具某些相似之處，但計算速度更快。

資料發送者依 ICV 演算法產生 ICV。接收者使用相的演算法產生 ICV。若此 2 個值相等，則接收者可一定程度上保證發送者之完整性及真確性。

ICV 演算法具下層雜湊演算法，因此 ICV 演算法確保受保護資料之完整性，亦即，受保護資料的接收者可肯定地假設若 ICV 經查證，則資料自 ICV 由發送者新增起即未遭變更。此外，若 ICV 已查證，則接收者亦可於一定程度上假設 ICV 係與查證所使用對稱金鑰相同的對稱金鑰所產生。因此，假設共享對稱金鑰係獨立於用於其他成對通訊之金鑰產生，接收者對發送者的鑑別具某些保證。

當加密及 ICV 產生係分離之過程時，則：

- (a) 2 個過程宜使用不同對稱金鑰。
- (b) 建議先加密，然後於加密資料上產生 ICV。

B.6.2 金鑰雜湊訊息鑑別碼(HMAC)演算法

HMAC 演算法係屬 ICV 演算法，涉及加密雜湊函數及秘密對稱金鑰。其定義於 FIPS PUB 198-1 [67]。

HMAC 可與任何加密雜湊函數結合使用，但此處僅考量下列各項：

- (a) hmacWithSHA256，其係依 SHA-256 雜湊演算法。
- (b) hmacWithSHA512，其係依 SHA-512 雜湊演算法。

建議使用相同於所用雜湊演算法區塊長度之共享對稱金鑰大小，亦即 hmacWithSHA256 為 64 個八位元組(512 位元)，hmacWithSHA512 為 128 個八位元組(1024 位元)。

IETF RFC 4231 [85]提供此等 HMAC 演算法的正式定義：

```
digestAlgorithm OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
  rsadsi(113549) 2 }
```

```
hmacWithSHA256 ALGORITHM ::= {
  PARMS NULL
  IDENTIFIED BY { digestAlgorithm 9 } }
```

```
hmacWithSHA512 ALGORITHM ::= {
  PARMS NULL
```



```
IDENTIFIED BY { digestAlgorithm 11 } }
```

B.6.3 先進加密標準(AES) - Galois 訊息鑑別碼(GMAC)演算法

GMAC 係依 B.7.2 中規定之 Galois/計數器模式(GCM)運作。其使用 GCM 規格產生標籤(ICV)，但未對明文加密。

定義對應於 AES 所定義 3 種金鑰大小之 3 種 AES-GMAC: aes128-GMAC、aes192-GMAC 及 aes256-GMAC。本標準僅認可 aes128-GMAC 及 aes256-GMAC。

IETF RFC 9044 [86]中提供用於 CMS 之 AES-GMAC 演算法的正式定義。然而，此等演算法具動態參數，因此由 ISO/IEC 9594-11 | Rec. ITU-T X.510 重新定義。

```
aes128-GMAC ALGORITHM ::= {
    PARMS MACLength
    DYN-PARMS GMAC-nonce
    IDENTIFIED BY { id-algo aes(2) 29 } }

aes256-GMAC ALGORITHM ::= {
    PARMS MACLength
    DYN-PARMS GMAC-nonce
    IDENTIFIED BY { id-algo aes(2) 31 } }

MACLength ::= INTEGER (12 | 13 | 14 | 15 | 16)
GMAC-nonce ::= OCTET STRING (SIZE (12))
```

ASN.1 值 id-algo 定義於 B.4.3。

B.7 具相關聯資料鑑別加密(AEAD)演算法

B.7.1 一般

下列各節所簡介之 AEAD 演算法係屬 AES 密碼的變異。

AEAD 演算法之輸入包括 4 個項目：

- (a) 對稱金鑰。
- (b) 將鑑別並加密之資料。
- (c) 將鑑別但不加密之相關聯資料。
- (d) 單次隨機數。

就 AEAD 演算法之各調用會產生新的單次隨機數，對 AEAD 演算法之安全至關重要。

加密過程之輸出相同於待加密的明文及標籤長度之密文序連。解密過程之輸出為

明文及相關標籤查證是否正確的指示。

B.7.2 先進加密標準(AES) - Galois/計數器模式(GCM)

採用 Galois/計數器模式之先進加密標準(AES-GCM)係屬高效率相關聯資料鑑別加密(AEAD)演算法。特別是當以硬體實作時，其可高速且低延遲地運作。

加密部分類似於 AES-CTR 演算法。其使用 16 個八位元組計數器區塊，其中包含與計數器欄位序連之初始化向量(IV)欄位。

IV 欄位宜由 12 個八位元組(96 位元)組成，以獲得最佳效能及更高等級之可運作性。訊息第 1 個區塊之計數器欄位值為 0x0000 0001 並遞增。

若多次使用相同 IV 及對稱金鑰群組合，則該實作容易遭受攻擊。NIST SP 800-38D 第 8 節指出：「於 2 個(或更多)不同之輸入資料集上使用相同 IV 及相同的金鑰調用經鑑別的加密函數之機率不應大於 2^{-32} 」。藉由良好之隨機數產生器(RNG)及/或定期替換對稱金鑰可將風險降至最低。

定義對應於 AES 所定義 3 種金鑰大小之 3 種 AES-GCM 演算法：aes128-GCM、aes192-GCM 及 aes256-GCM。本標準僅認可 aes128-GCM 及 aes256-GCM。

IETF RFC 5084 中提供用於 CMS 之 AES-GCM 演算法之正式定義。然而，此等演算法具動態參數，因此由 ISO/IEC 9594-11 | Rec. ITU-T X.510 重新定義。

```
aes128-GCM ALGORITHM ::= {  
    PARMS GCM-ICVlen  
    DYN-PARMS GCM-nonce  
    IDENTIFIED BY { id-algo aes(2) 17 } }
```

```
aes256-GCM ALGORITHM ::= {  
    PARMS GCM-ICVlen  
    DYN-PARMS GCM-nonce  
    IDENTIFIED BY { id-algo aes(2) 19 } }
```

```
GCM-ICVlen ::= INTEGER (16)  
GCM-nonce ::= OCTET STRING (SIZE (12))
```

ASN.1 值 id-algo 定義於 B.4.3 中。

有關 GCM 之更多資訊，參照 NIST SP 800-38D [68]。

B.7.3 先進加密標準(AES) - 具 CBC-MAC 之計數器(CCM)

CCM 代表具 CBC-MAC 之計數器，其中 CBC-MAC 代表加密區塊鏈訊息鑑別碼。

CCM 使用計數器模式對稱金鑰演算法進行加密及解密(參照 B.4.4)。其使用 CBC-MAC 演算法產生並查證鑑別標籤。

CBC-MAC 演算法規定不使用雜湊之 ICV 產生及查證技術，而是以極相似於加密區塊鏈接的方式加密，不同之處在於其無須初始化向量，且最後加密區塊係用作標籤而非所有加密區塊的序連。

定義對應於 AES 所定義 3 種金鑰大小之 3 種 AES-CCM 演算法：aes128-CCM、aes192-CCM 及 aes256-CCM。本標準僅認可 aes128-CCM 及 aes256-CCM。

IETF RFC 5084 中提供用於 CMS 之 AES-CCM 演算法的正式定義。然而，此等演算法具動態參數，因此由 ISO/IEC 9594-11 | Rec. ITU-T X.510 重新定義。

```

aes128-CCM ALGORITHM ::= {
    PARMS CCM-ICVlen
    DYN-PARMS CCM-nonce
    IDENTIFIED BY { id-algo aes(2) 25 } }

aes256-CCM ALGORITHM ::= {
    PARMS CCM-ICVlen
    DYN-PARMS CCM-nonce
    IDENTIFIED BY { id-algo aes(2) 27 } }

CCM-ICVlen ::= INTEGER (16)
CCM-nonce ::= OCTET STRING (SIZE (12))

```

ASN.1 值 id-algo 定義於 B.4.3 中。

關於 CCM 之更多資訊，參照 NIST SP 800-38C [69]。

B.8 Diffie-Hellman 金鑰協議

B.8.1 一般

Diffie-Hellman 金鑰協議方法容許須交換所謂 Diffie-Hellman 公開金鑰之雙方，以不容許竊聽者獲悉關於此共享秘密的方式，共同達到共享秘密。然後，此共享秘密可用以衍生 1 或多個對稱金鑰(參照 B.9)。NIST SP 800-56A 修訂版 3 [72] 提供此方法之詳細規格。

Diffie-Hellman 演算法亦使用公開金鑰演算法之變異。金鑰對可為臨時性，亦即其通常依需產生，然後僅使用 1 次，亦可為靜態者，其中 CA 已驗證金鑰對且於公開金鑰憑證中提供公開金鑰。有 3 種可能之運作模式：

- (a) 靜態-靜態，其中雙方擁有靜態金鑰對。
- (b) 臨時-臨時：其中雙方依需產生臨時金鑰對。
- (c) 暫時-靜態，其中一側依需產生金鑰對，而另一側擁有靜態金鑰對。

B.8.2 循環群簡介

為理解 Diffie-Hellman 金鑰交換如何與離散對數問題相關，有必要簡介群論。

“群”定義為連同群運算符之元素集。此處僅考量由 1 至 $p-1$ 之整數組成之群，其中 p 係質數。此可寫成：

$$\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$$

作為群運算符，使用特殊乘法方式：

$$a \circ b == a \times b \bmod p$$

其中 \circ 為群運算符， \times 是經典乘號。

循環群為其中 1 或多個元素係所謂生成元之群。生成元 g 具下列特性： $\{g, g^2, \dots, g^{p-1}\} \pmod{p}$ 之集合與 $\{1, 2, \dots, p-1\}$ 具相同元素集，僅順序不同。

Diffie-Hellman 金鑰協議係於循環群上所定義。

Alice 將群組內之任意元素 x_a 作為其 Diffie-Hellman (DH) 私密金鑰，並將其 DH 公開金鑰計算為 $y_a = g^{x_a}$ 。Bob 亦將組內之任意元素 x_b 作為其 DH 私密金鑰，併計算出其 DH 公開金鑰為 $y_b = g^{x_b}$ 。

B.8.3 有限域上之 Diffie-Hellman 方法

此方法規定於 IETF RFC 2631 中，並使用離散對數加密技術。於該方法中，2 個夥伴(此處稱為 Alice 及 Bob)想要交換訊息。Alice 產生或擁有與公開金鑰相關之私密金鑰 x_a ，由 $y_a = g^{x_a} \bmod p$ 所給定，

其中 g (稱為生成元)為所議定參數之一，而質數 p 係另一議定的參數。同樣，Bob 產生或擁有與另一公開金鑰 $y_b = g^{x_b} \bmod p$ 相關聯的私密金鑰 x_b 。

然後雙方交換公開金鑰。Alice 計算：

$$ZZ = y_b^{x_a} \bmod p = (g^{x_b} \bmod p)^{x_a} \bmod p = g^{x_b x_a}$$

而 Bob 則計算：

$$ZZ = y_a^{x_b} \bmod p = (g^{x_a} \bmod p)^{x_b} \bmod p = g^{x_a x_b}$$

其中 ZZ 係共享秘密。

B.8.4 離散對數問題

可看出，DH 私密金鑰與對應之 DH 公開金鑰間存在關係。當知悉 Alice 之 $g^{x_a} = y_a$ 之 y_a 及 g 值時，對手可藉由解方程式 $y_b = g^{x_b}$ 或 $\log_g y_a = x_a$ 。若可能的話，對手將能計算共享秘密。此稱為離散對數問題。

目前亦無已知之有效方法以因應此問題，但蠻力方法可能計算 g^2, g^3, \dots ，直至結果為 y_a 。針對大質數，例：2048 位元質數，即使就快速計算機而言亦不可行。

備考：量子電腦之出現可能改變此點。參照 B.9。

IETF RFC 3526 定義具不同長度的質數 p 及所定義生成元 g 之循環群清單。各組別皆配送 1 個組別號碼。透過透過議定一個群，參數 p 及 g 於通訊夥伴間建立。

B.8.5 橢圓曲線 Diffie-Hellman 金鑰協議

橢圓曲線 Diffie-Hellman (ECDH) 金鑰交換係依橢圓曲線乘法之關聯性規則。

B.3.4.3 中顯示 ECC 公開金鑰為生成元點 G 乘以私密金鑰 a 。於不安全通道上交換公開金鑰 $(a_x \cdot G)$ 與 $(a_y \cdot G)$ ，其中 a_x 係 Alice 之私密金鑰， a_y 係 Bob 之私密金鑰。

然後，Alice 將計算 $(a_y \cdot G) \cdot a_x$ ，Bob 將計算 $(a_x \cdot G) \cdot a_y$ 。依上述關聯性規則，計算出之值係相同，因此表示共享秘密。

另一表述方式為，Alice 之公開金鑰乘以 Bob 之私密金鑰等於 Bob 之公開金鑰乘以 Alice 之私密金鑰，其再次等於共享秘密。

B.8.6 金鑰建立演算法

B.8.6.1 一般

ISO/IEC 9594-11:2020 | Rec. ITU-T X.510 (2020) 針對 Diffie-Hellman 方法與金鑰衍生函數之組合，定義金鑰建立演算法。未來，可能之量子安全金鑰建立方法亦可表示為金鑰建立演算法。目的為容許類似於其他型式密碼演算法之協商及移轉技術。

B.8.6.2 具 HKDF-256 之 Diffie-Hellman 群 14 演算法

下列係依 Diffie-Hellman 金鑰協議方法及 B.9 中規定之金鑰衍生方法的金鑰建立演算法之規格。

```
dhModpGr14Hkdf256Algo ALGORITHM::= {  
    PARMS Group14  
    DYN-PARMS Payload14  
    IDENTIFIED BY id-algo-dhModpGr14Hkdf256Algo }
```

```
Group14::= INTEGER (14)
```

```
Payload14::= SEQUENCE {  
    dhPublicKey OCTET STRING (SIZE (256)),  
    nonce OCTET STRING (SIZE (32)) OPTIONAL,  
    ... }
```

依 IETF RFC 3526 中所規定，PARMS 符記規定固定參數應為 2048 位元組 MODP 群組編號 14 之該等參數。

DYN-PARMS 符記規定動態參數應為 Payload14 資料型式所規定之參數。

Payload14 資料型式具下列組件：

- (a) dhPublicKey 組件應規定發送者所使用 Diffie-Hellman 公開金鑰之八位元組長度。針對所使用群組，大小恆為 256 個八位元組。
- (b) nonce 組件應規定 B.9 中所規定共享金鑰衍生所使用之隨機值的長度(以八位元組為單位)。若單次隨機數可以另一方法產生，則應不出現。否則，其應出現。

B.8.6.3 具 HKDF-256 之 Diffie-Hellman 群組 23 演算法

下列為依 Diffie-Hellman 金鑰協議方法及 B.9 中所規定金鑰衍生方法的金鑰建立演算法之規格。

```
dhModpGr23Hkdf256Algo ALGORITHM::= {  
    PARMS Group23  
    DYN-PARMS Payload23  
    IDENTIFIED BY id-algo-dhModpGr23Hkdf256Algo }
```

```
Group23::= INTEGER (23)
```

```
Payload23::= SEQUENCE {  
    dhPublicKey OCTET STRING (SIZE (65)),  
    nonce OCTET STRING (SIZE (32)),  
    ... }
```

依 IETF RFC 5114 中所規定之 ECDH 曲線 secp256r1，PARMS 符記規定固定參

數應為群組編號 23 所規定之參數。

DYN-PARMS 符記表示動態參數應為 Payload23 資料型式所規定之參數。

除 dhPublicKey 之長度應為 65 個八位元組外，Payload23 資料型式具相同於 Payload14 資料型式之組件。

B.8.6.4 具 HKDF-256 之 Diffie-Hellman 群組 28 演算法

下列為依 Diffie-Hellman 金鑰協議方法及 B.9 中所規定金鑰衍生方法之金鑰建立演算法的規格。

```
dhModpGr28Hkdf256Algo ALGORITHM ::= {
    PARMS          Group28
    DYN-PARMS      Payload28
    IDENTIFIED BY id-algo-dhModpGr28Hkdf256Algo }

Group28 ::= INTEGER (28)

Payload28 ::= SEQUENCE {
    dhPublicKey  OCTET STRING (SIZE (65)),
    nonce        OCTET STRING (SIZE (32)),
    ... }

```

針對 IETF RFC 6932 中規定之 ECDH 曲線 BrainpoolP256r1，PARMS 符記規定固定參數應為群組編號 28 規定的參數。

DYN-PARMS 欄位規定動態參數應為 Payload28 資料型式所規定之參數。

除 dhPublicKey 之長度應為 65 個八位元組外，Payload28 資料型式具相同於 Payload14 資料型式的組件。

B.9 金鑰衍生

B.9.1 一般

當金鑰協議方法之結果為共享秘密時，藉由使用金鑰衍生函數延伸該共享秘密，以針對所須對稱金鑰提供足夠資料。

B.9.2 HMAC 式抽取及延伸金鑰衍生函數

雜湊式金鑰衍生函數(HKDF)規定於 IETF RFC 5869 中。其要求使用 IETF RFC 2104 中所規定之金鑰雜湊訊息鑑別碼(HMAC)演算法。

HKDF 依循“抽取然後延伸”典範，其中 KDF 於邏輯上由 2 個模組組成：階段

1 取得輸入建鑰材料(IKM)並從中“抽取”固定長度之擬隨機金鑰(PRK)，然後階段 2 將此金鑰“延伸”為幾個額外的輸出擬隨機金鑰(OKM)。

HKDF 抽取可表示如下

$PRK = \text{HMAC-Hash}(\text{salt}, \text{IKM})$ ，其中：

(a) salt 係非秘密隨機值 - 其採用須使用 HKDF 之討論中金鑰建立演算法實例的單次隨機數組件的值。

(b) IKM 代表輸入建鑰材料 - 其係 DH 金鑰協定產生的共享秘密。

(c) OKM 定義為：

$OKM = \text{HKDF-expand}(PRK, \text{info}, L)$ ，其中：

PRK 為上述 HKDF 延伸所產生之 PRK，

info 係選項全景及應用特定資訊，可能為 0 長度字串(自 RFC 5869 起)，

L 係待產生金鑰的組合長度。

B.10 密碼演算法之移轉

事實證明，跨個體之密碼演算法移轉甚為困難，因並非所有個體能或將同時移轉，導致互作問題。Rec. ITU-T X.509 | ISO/IEC 9594-8 提供容許移轉公開金鑰憑證、屬性憑證、憑證撤銷清單(CRL)，以及授權及驗核清單(AVL)之密碼演算法的規格。Rec. ITU-T X.510 | ISO/IEC 9594-11 提供關於如何移轉協定規格所使用之密碼演算法的建議。

移轉期間之一般技術係包括特定型式之 2 種演算法，稱為原生演算法(**native algorithm**)，其係待移轉的演算法及想要移轉至之替代演算法。提供替代演算法之方式使得尚未移轉的個體將忽略該演算法。移轉期結束後，替代演算法將成為新的原生演算法。若相關，亦可依循相同政策包括替代數位簽章或 ICV。

備考：若不升級系統，則某些加密移轉可能無法完成。

B.11 後量子運算密碼學

由於適用金鑰管理之電力系統組件通常於現場停留較長時間，因此需考量其下密碼演算法之密碼敏捷性，以因應密碼學的最新發展，例：特別是於後量子密碼學領域。此適用於所使用之憑證格式，亦適用於憑證管理中所使用的安全協定。

目前流行之非對稱演算法的問題在於其安全依賴於 3 個數學難題之一：

- (a) 整數分解問題，如 B.3.2.35 中所討論。
- (b) 離散對數問題，如 B.8.4 中所討論。
- (c) 橢圓曲線離散對數問題，如 B.3.4.4 中所討論。

眾所周知，量子電腦於因應此等數學問題方面極有效，此使得非對稱性易於遭量子電腦攻擊。

對稱密碼演算法不易受量子電腦影響。建議將對稱金鑰之大小加倍。針對雜湊演算法，建議將摘要大小乘以 2.5。

Alexandra 研究所發布關於後量子密碼學之白皮書[78]。

NIST 有分析及選擇待標準化之量子安全密碼演算法的過程。NISTIR 8309, *Status Report on the Second Round of NIST Post-Quantum Cryptographic Standardization Process* 提供預期為何之良好景像[83]。

NIST 亦發表關於“為後量子密碼學做好準備”之論文[84]。

作為第 1 步，協定規格宜提供 B.9 中討論之移轉功能，為後量子演算法做好準備。

B.12 隨機數產生(RNG)

B.12.1 隨機數產生型式

隨機數產生器(random number generator, RNG)係以安全方式產生隨機性及金鑰之先決條件。雜湊及對稱金鑰演算法之所述安全強度，假設使用尚屬完美的隨機數產生器。

不同裝置可使用不同演算法用以產生隨機數。實作者可針對其裝置及應用選擇適切之隨機數產生機制。

下列係常用隨機數產生方法之簡單概觀。美國國家標準與技術研究院特別出版物 800-90A 修訂版 1 [61]，以及 ISO/IEC 18031 [87]及 ISO/IEC 20543 [88]中深入討論隨機數產生。

產生隨機數之 1 種方式係由使用過程其中產生隨機位元，其中位元輸出(熵)源自不可預測的實體機制。此等稱為非確定性隨機位元產生器(NRBG)。通常，實體機制產生隨機二進數字之速度受限制。因此，有政策可使用延伸演算法自熵

中快速計算出擬隨機資料位元；此類別 RBG 稱為確定性隨機位元產生器 (DRBG)。

B.12.2 確定性隨機位元產生器

DRBG 機制使用實體機制提供熵輸入。此稱為種子。然後，DRBG 演算法自種子中產生快速之位元序列。DRBG 輸出擬隨機位元，而並非隨機位元，速度通常大幅提升。DRBG 之熵輸入須保證隨機性。只要種子保密，DRBG 將係不可預測的，取決於種子的強度。DRBG 演算法須為良好演算法，否則種子強度並不重要。

使用 DRBG 機制之 RBG 安全係屬實作議題。實作者須提供足夠強大之熵來源及良好 DRBG 演算法。

良好 DRBG 可提供回溯阻力。換言之，於未知悉種子的情況下，不可能猜測先前之隨機輸出。良好 DRBG 演算法亦提供無偏差輸出及預測阻力。於未知悉種子之情況下，不可能預測下個擬隨機數。最後，良好 DRBG 使用條件熵 (conditioned entropy) 來源。熵調節 (Entropy conditioning) 包括隨機性及非重複性之連續測試，此將捕捉熵來源失常，諸如 11111、00000 或 010101 等。

針對實作，選定 DRBG 演算法，然後與條件熵輸入耦合。選擇種子大小及種子壽命以提供對預測攻擊之適切抵抗。由於種子壽命與其產生之擬隨機資料量相關，因此 DRBG 之速度最終受限於熵來源可支援的重選種子速率。

許多主機裝置並無一直有良好之熵輸入來源。因此，當 DRBG 實際上可存取某些可靠熵輸入來源時，須實例化 DRBG。熵輸入之來源可能僅偶爾可用。DRBG 可能以能累積源自應用之額外熵作為額外輸入的方式以實作。DRBG 實作宜盡可能接受額外輸入。可能有權存取某些熵 (諸如源自其他裝置之時戳或單次隨機數) 的應用，宜應將此等值作為額外輸入提供予 DRBG。

B.12.3 非確定性隨機數產生

此基本上與使用密碼金鑰之本系列標準各部 (第 3 部至第 6 部及第 8 部) 有關。

非確定性隨機數產生器及熵來源係唯一不受標準化限制之加密基元。

ISO/IEC 18031 或 NIST SP 800-90 提供假設之雜訊二極體示例。然而，建立良

好之二極體式隨機數產生器並不容易。該作法的問題之一為廉價 A/D 轉換器的低品質，另一問題則為電力線嗡嗡聲及其他電磁雜訊易於進入電路，另一問題則某些二極體可能隨著時間推移而損壞。

針對電腦化賭博及加密用途，有幾種現成硬體式隨機位元產生器出售。其實作方式多種多樣，自雜訊二極體及未鎖定振盪器(**unlocked oscillator**)設計至商用量子光學設計。

宜持續監視硬體隨機數產生器是否正常運作。RFC 4086 及 FIPS Pub 140-2 包括可用於此目的之測試。

存在許多雜訊源。由於其輸出大多數係可預測，因此須避免將此等來源用於加密用途。應避免之示例：

- 粉紅雜訊(**pink noise**)產生電路。雖價格便宜，但不幸的是，其產生擬隨機數字雜訊，因此不適合加密使用。
- 麥克風及收音機：其可能遭攻擊者操控外部輸入。
- 1955 年 RAND 表及其他已發布之類似隨機數來源。此等係是眾所周知之來源，且於加密設定中無前向或回溯安全。

B.12.4 熵來源

熵係於某些小過程或裝置中無序之度量，其為封閉系統，但可自外部量測。量測過程產生隨機位元串。具完全熵(**full entropy**)之位元串的各位元係不可預測，具均勻分布且獨立於其他位元。為使熵來源可用於隨機數產生，該過程始於雜訊來源，諸如熱雜訊、數位化過程、評鑑過程、選項調節過程，以及健全狀態測試。源自網路介面或電力線之輸入雜訊通常不可接受，因其不可靠。須考量側通道攻擊。例：為安靜熱雜訊源而進行之極端溫度攻擊降低其隨機性，並可能大幅降低其產生的隨機數之真實隨機性。為考量可能之攻擊，熵來源宜由其最壞情境或其提供之最小熵量測。

附錄 C

(參考)

憑證登錄及更新流程圖

C.1 憑證登錄

憑證登錄之可能流程，參照圖 C.1。

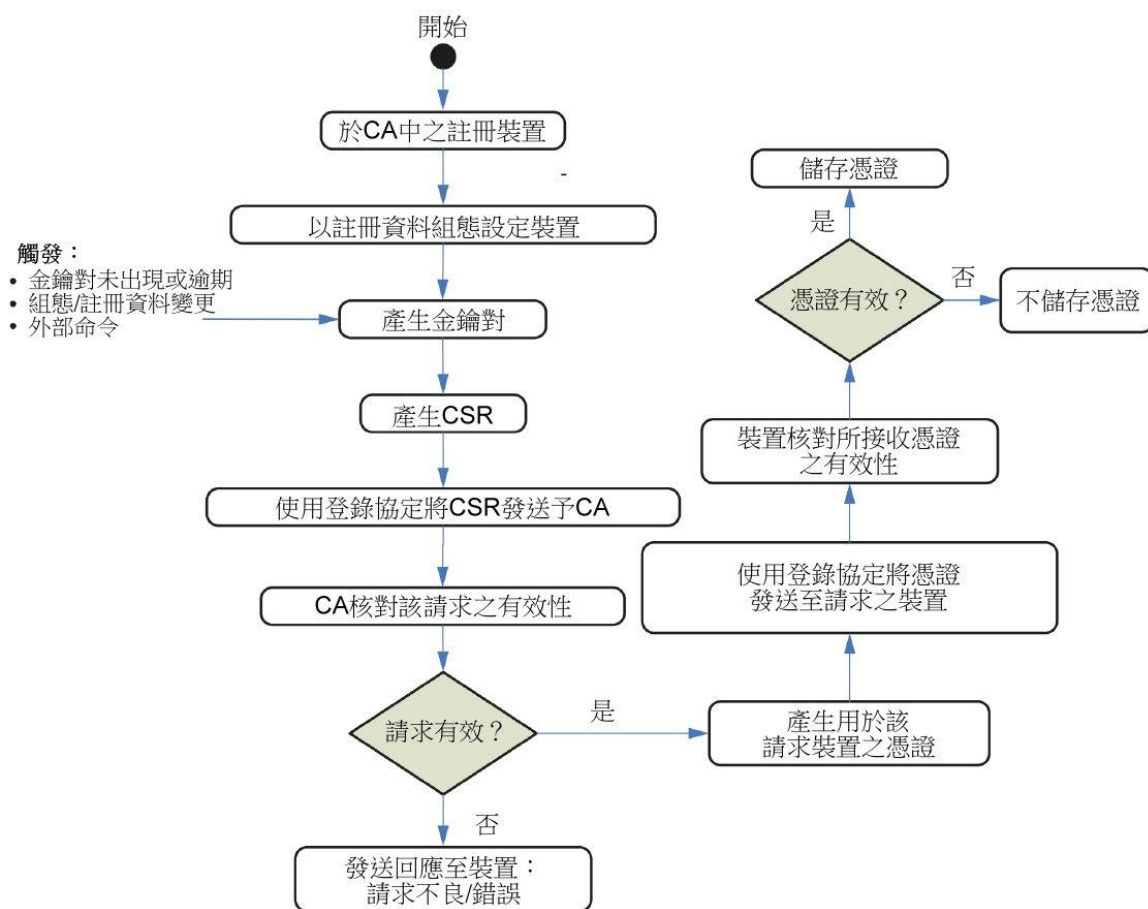


圖 C.1 憑證登錄(一般)

C.2 憑證更新

憑證更新之狀態機，參照圖 C.2：

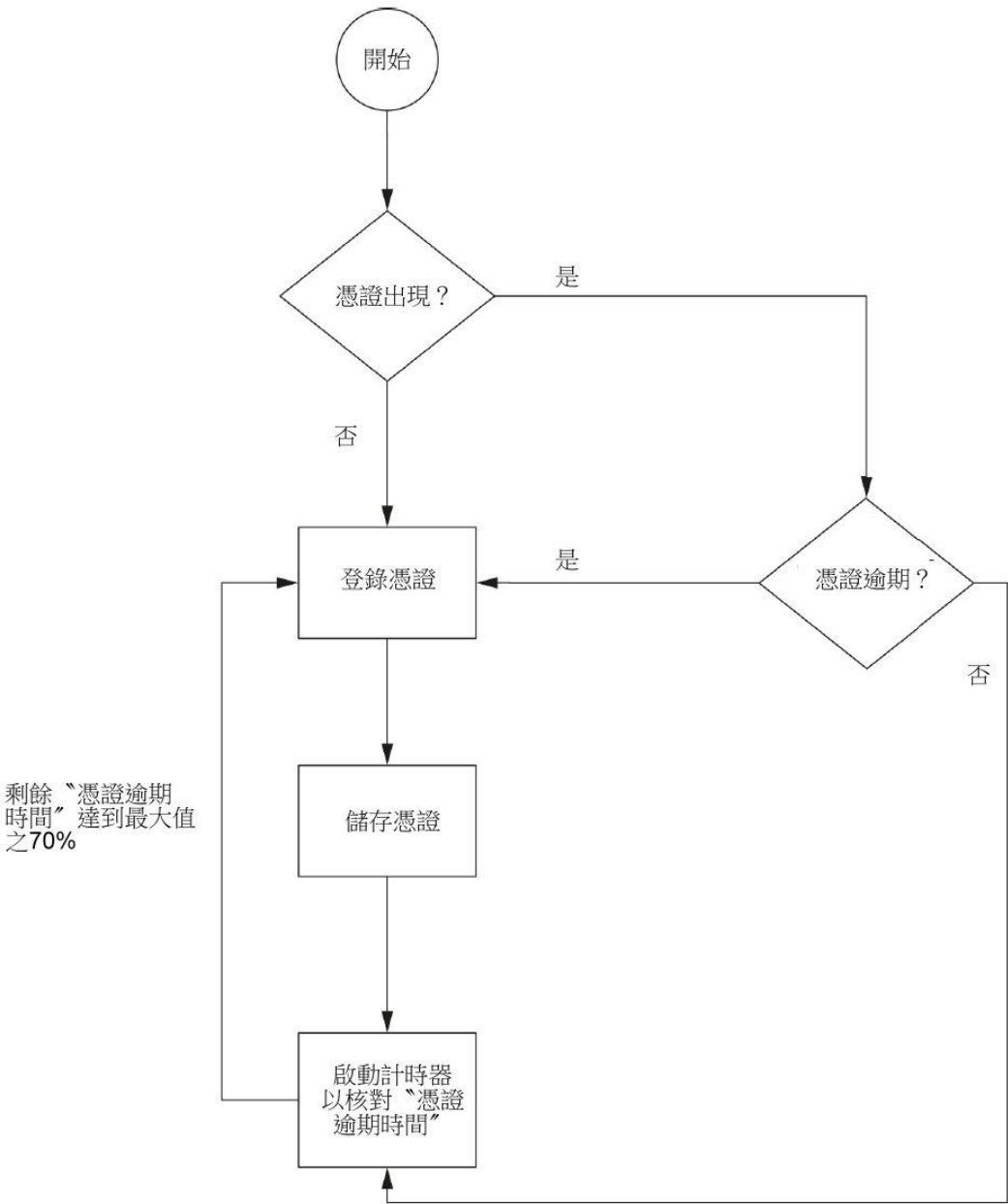


圖 C.2 憑證更新狀態機

附錄 D

(參考)

對映本系列標準第 14 部之安全事件

D.1 一般

本附錄包含本標準中所定義安全事件與本系列標準第 14 部中所規定格式之對映。

有關安全事件之資訊以及額外資訊欄中包含的可能細節，僅能由個體依此資訊透過其下平台或所利用之組件的可用性提供。

所有安全事件之 IEC 版本應設定為“1”。針對安全事件，使用下列分群：

- 值“1”與公開金鑰憑證傳送相關事件相關，包括登錄協定錯誤。
- 值“2”公開金鑰憑證查證特定安全事件。
- 值“3”與屬性憑證查證特定安全事件相關。
- 值“4”與憑證撤銷狀態事件相關(對公開金鑰憑證及屬性憑證有效)。
- 值“5”與 GDOI 特定安全事件相關。

D.2 信符傳送及登錄之安全事件日誌紀錄

表 D.1 包含與信符傳送及登錄相關之事件。

表 D.1 對映本系列標準第 14 部之信符傳送及憑證登錄的安全事件日誌

安全事件	本標準節次	助憶符	嚴重性	事件識別符	文字	額外資訊
金鑰傳送: PKCS #12 格式錯誤	7.3.2	CRED_PKCS12_FORMAT	警告	IEC 62351-9:1.1	PKCS #12 格式未匹配。	
金鑰傳送: PKCS #8 格式錯誤	7.3.2	CRED_PKCS8_FORMAT	警告	IEC 62351-9:1.2	PKCS #8 格式未匹配。	
SCEP 登錄已成功執行	7.3.7.2	CRED_ENR_SCEP_SUCC	通知	IEC 62351-9:1.3	使用成功執行之 SCEP 登錄。	核發之公開金鑰憑證
SCEP 登錄因不成功而中止	7.3.7.2	CRED_ENR_SCEP_FAIL	錯誤	IEC 62351-9:1.4	因 SCEP 不成功，使用 SCEP 之登錄遭中止。	

安全事件	本標準節次	助憶符	嚴重性	事件識別符	文字	額外資訊
EST 登錄已成功執行	7.3.7.2	CRED_ENR_EST_SUCC	通知	IEC 62351-9:1.5	使用成功執行之 EST 登錄。	核發之公開金鑰憑證
EST 登錄因不成功而中止	7.3.7.2	CRED_ENR_EST_FAIL	錯誤	IEC 62351-9:1.6	因 SCEP 不成功，使用 EST 之登錄遭中止。	

D.3 用於公開金鑰憑證查證之安全事件日誌紀錄

表 D.2 包含與公開金鑰憑證查證相關之事件。

表 D.2 針對對映本系列標準第 14 部之公開金鑰憑證查證所定義的安全事件日誌

安全事件	本標準節次	助憶符	嚴重性	事件識別符	文字	額外資訊
憑證編碼錯誤	7.4.2	CERT_V_FOR_MAT	警告	IEC 62351-9:2.1	憑證格式未匹配。不成功之查證。	
公開憑證簽章查證不成功。	7.4.3	CERT_V_PK_SIG_WRONG	告警	IEC 62351-9:2.2	無法查證公開金鑰憑證簽章。	
X.509 憑證之版本未與預期版本匹配	7.4.4.2	CERT_V_PK_VERSION	錯誤	IEC 62351-9:2.3	錯誤之公開金鑰憑證版本。	
核發者未與已知且受信任核發者匹配	7.4.4.3	CERT_V_PC_ISSUER	錯誤	IEC 62351-9:2.4	公開金鑰憑證核發者未受信任。	
未支援簽章演算法	7.4.4.4	CERT_PK_SIG_ALG	錯誤	IEC 62351-9:2.5	未支援之簽章演算法。	
公開金鑰憑證有效性：逾期	7.4.4.5	CERT_V_PK_EXPIRED	錯誤	IEC 62351-9:2.6	公開金鑰憑證逾期。	

安全事件	本標準 節次	助憶符	嚴重性	事件識別符	文字	額外資 訊
公開金鑰憑證有效性： 未曾有效	7.4.4.5	CERT_V_PK_ E ARLY	錯誤	IEC 62351-9:2.7	公開金鑰憑證未曾有效。	
主體未納入公開金鑰憑證	7.4.4.6	CERT_V_PK_ SUBJECT	警告	IEC 62351-9:2.8	主體未納入公開金鑰憑證。	
未支援公開金鑰憑證中之演算法	7.4.4.7	CERT_V_PK_ ALG_MISMA TCH	錯誤	IEC 62351-9:2.9	未支援公開金鑰憑證中之本機公開金鑰演算法。	
路徑驗核錯誤，因未支援信任錨	7.4.4.8	CERT_V_PK_ TA	錯誤	IEC 62351-9:2.10	未支援信任錨。	
憑證路徑驗核錯誤	7.4.4.8	CERT_V_PK_ PATH	錯誤	IEC 62351-9:2.11	無法查證憑證路徑。	
未知之關鍵延伸	7.4.4.10.1	CERT_V_PKC E_CEXT	錯誤	IEC 62351-9:2.12	公開金鑰憑證中未知之關鍵延伸。	
未知之關鍵延伸值	7.4.4.10.1	CERT_V_PKC E_EXT_VAL UE	錯誤	IEC 62351-9:2.13	關鍵延伸中之未知資訊。	
機構金鑰識別符未納入公開金鑰憑證	7.4.4.10.2	CERT_V_PK_ AKID	錯誤	IEC 62351-9:2.14	機構金鑰識別符未納入公開金鑰憑證。	
主體金鑰識別符未納入公開金鑰憑證	7.4.4.10.3	CERT_V_PKC E_SKID	錯誤	IEC 62351-9:2.15	主體金鑰識別符未納入公開金鑰憑證。	
主體替代名稱未納入 TLS 伺服器憑證	7.4.4.10.4	CERT_V_PKC E_SA	錯誤	IEC 62351-9:2.16	主體替代名稱未納入 TLS 伺服器憑證。	
BC 未納入 CA 憑證	7.4.4.10.5	CERT_V_PKC E_BC	錯誤	IEC 62351-9:2.17	基本限制事項未納入 CA 憑證。	

安全事件	本標準 節次	助憶符	嚴重性	事件識別符	文字	額外資 訊
違反 CA 憑證中路徑長度限制事項	7.4.4.10.5	CERT_V_PKCE_PL	錯誤	IEC 62351-9:2.18	違反 CA 憑證中路徑長度限制事項。	
數位簽章金鑰使用未納入 TLS 憑證中	7.4.4.10.6	CERT_KU_DIGSIG	錯誤	IEC 62351-9:2.19	數位簽章金鑰使用未納入 TLS 憑證。	
當使用與金鑰加密一起使用之 TLS 密碼時，金鑰加密的金鑰使用未納入	7.4.4.10.6	CERT_PKCE_KU	錯誤	IEC 62351-9:2.20	當使用與金鑰加密一起使用之 TLS 密碼時，金鑰加密的金鑰使用未納入。	
用以簽署憑證之金鑰使用未納入	7.4.4.10.6	CERT_PKCE_KU_KCS	錯誤	IEC 62351-9:2.21	用以簽署憑證之金鑰使用未納入。	
CRL 簽章憑證中未包括用以簽署 CRL 之金鑰使用	7.4.4.10.6	CERT_PKCE_KU_CRLS	錯誤	IEC 62351-9:2.22	CRL 簽章憑證中未包括用以簽署 CRL 之金鑰使用。	
伺服器鑑別之延伸金鑰使用未納入 TLS 伺服器憑證	7.4.4.10.7	CERT_PKCE_EKU_TLS_SA	錯誤	IEC 62351-9:2.23	伺服器鑑別之延伸金鑰使用未納入 TLS 伺服器憑證。	
伺服器鑑別之延伸金鑰使用未納入 TLS 客戶端憑證	7.4.4.10.7	CERT_PKCE_EKU_TLS_CA	錯誤	IEC 62351-9:2.24	伺服器鑑別之延伸金鑰使用未納入 TLS 客戶端憑證。	

安全事件	本標準節次	助憶符	嚴重性	事件識別符	文字	額外資訊
OCSP 回應者憑證中未包括用於 OCSP 簽章之延伸金鑰使用	7.4.4.10.7	CERT_PKCE_EKU_OCSPS	錯誤	IEC 62351-9:2.25	OCSP 回應者憑證中未包括用於 OCSP 簽章之延伸金鑰使用。	OCSP 回應者憑證
公鑰憑證中未包含 CRL 配送點	7.4.4.10.9	CERT_V_PKCE_NCDP	警告	IEC 62351-9:2.26	公鑰憑證中未包含 CRL 配送點。	
公開金鑰憑證中未包含 OCSP 回應者資訊	7.4.4.10.10	CERT_V_PKCE_NOCSP	警告	IEC 62351-9:2.27	公開金鑰憑證中未包含 OCSP 回應者資訊。	

D.4 用於屬性憑證查證之安全事件日誌紀錄

表 D.3 包含與屬性憑證驗證相關之事件：

表 D.3 針對對映本系列標準第 14 部之屬性憑證查證所定義的安全事件日誌

安全事件	本標準節次	助憶符	嚴重性	事件識別符	文字	額外資訊
憑證編碼錯誤	7.4.2	CERT_V_AC_FORMAT	警告	IEC 62351-9:3.1	憑證格式未匹配。不成功之查證。	
屬性憑證簽章查證不成功	7.4.3	CERT_V_AC_S_IG_WRONG	警告	IEC 62351-9:3.2	無法查證公開金鑰憑證簽章。	
屬性憑證版本資訊未匹配	7.4.5.2	CERT_V_AC_VERSION	錯誤	IEC 62351-9:3.3	錯誤之屬性憑證版本。	
無法依公開金鑰憑證查證屬性憑證之持有者	7.4.5.3	CERT_V_AC_HOLDER_PK	警告	IEC 62351-9:3.4	無法依公開金鑰憑證查證屬性憑證之持有者	

安全事件	本標準節次	助憶符	嚴重性	事件識別符	文字	額外資訊
無法依替代鑑別查證屬性憑證之持有者	7.4.5.3	CERT_V_AC_HOLDER_NPK	警告	IEC 62351-9:3.5	無法依替代鑑別查證屬性憑證之持有者。	
組態設定之屬性憑證核發者不受信任	7.4.5.4	CERT_V_AC_ISSUER_CONFIG	錯誤	IEC 62351-9:3.6	屬性憑證核發者不受信任(未組態設定)。	
依受信任之CA，屬性憑證核發者不受信任	7.4.5.4	CERT_V_AC_ISSUER_TCA	錯誤	IEC 62351-9:3.7	屬性憑證核發者不受信任(藉由受信任之CA)。	
屬性憑證逾期	7.4.5.7	CERT_V-AC_EXPIRED	錯誤	IEC 62351-9:3.8	屬性憑證逾期。	
屬性憑證未曾有效	7.4.5.7	CERT_V_AC_EARLY	錯誤	IEC 62351-9:3.9	屬性憑證未曾有效。	
屬性憑證中未知之關鍵延伸	7.4.5.8.1	CERT_V_AC_E_EXT	錯誤	IEC 62351-9:3.10	屬性憑證中未知之關鍵延伸。	
屬性憑證關鍵延伸中無法辨識之資訊	7.4.5.8.1	CERT_V_AC_E_EXT_VALUE	錯誤	IEC 62351-9:3.11	屬性憑證關鍵延伸中無法辨識之資訊。	
屬性憑證之未知延伸	7.4.5.8.1	CERT_V_AC_CE_EXT	警告	IEC 62351-9:3.12	屬性憑證之未知延伸。	
無法查證屬性憑證中之機構金鑰識別符	7.4.5.8.2	CERT_V_AC_E_AKID	錯誤	IEC 62351-9:3.13	無法查證屬性憑證中之機構金鑰識別符。	
屬性憑證中無預期之撤銷資訊	7.4.5.8.3	CERT_V_AC_E_NRII	通知	IEC 62351-9:3.14	屬性憑證中無預期之撤銷資訊。	
屬性憑證中未包含CRL配送點	7.4.5.8.3	CERT_V_AC_E_NCDPCRL	警告	IEC 62351-9:3.15	屬性憑證中未包含CRL配送點。	

安全事件	本標準節次	助憶符	嚴重性	事件識別符	文字	額外資訊
屬性憑證中未包含 OCSP 回應者資訊	7.4.5.8.3	CERT_V_AC E_NOCS	警告	IEC 62351- 9:3.16	屬性憑證中未包含 OCSP 回應者資訊。	

D.5 憑證撤銷狀態之安全事件紀錄

表 D.4 包含與憑證撤銷狀態相關之事件：

表 D.4 針對對映本系列標準第 14 部之憑證撤銷狀態所定義的安全事件日誌

安全事件	本標準節次	助憶符	嚴重性	事件識別符	文字	額外資訊
憑證遭撤銷	7.4.6	CERT_V_ REV OKED	告警	IEC 62351- 9:4.1	憑證遭撤銷。	撤銷原因
CRL 配送點不可存取	7.4.6	CERT_V_ R_NR_CR L	警告	IEC 62351- 9:4.2	CRL 配送點不可存取。	CRLDP URL
CRL 逾期	7.4.6	CERT_V_ CRL_EXP	警告	IEC 62351- 9:4.3	CRL 逾期。	
CRL 簽章查證不成功	7.4.6	CERT_V_ CRL_SIG _FAIL	警告	IEC 62351- 9:4.4	CRL 簽章查證不成功。	
OCSP 回應者不可存取	7.4.6	CERT_V_ R_N R_OCSP	警告	IEC 62351- 9:4.5	OCSP 回應者不可存取。	OCSP 回 應者 URL
OCSP 回應者連接逾時	7.4.6	CERT_V_ R_TO_OC SP	警告	IEC 62351- 9:4.6	OCSP 回應者連接逾時。	
OCSP 回應者不知憑證	7.4.6	CERT_V_ R_C U_OCSP	警告	IEC 62351- 9:4.7	OCSP 回應者不知憑證。	
OCSP 回應逾期	7.4.6	CERT_V_ R_O CSP_EXP	警告	IEC 62351- 9:4.8	OCSP 回應逾期。	
OCSP 回應訊息簽章查證不成功	7.4.6	CERT_V_ OCSP_SI G_FAIL	警告	IEC 62351- 9:4.9	OCSP 回應簽章查證不成功。	

D.6 用於具 GDOI 之群組式金鑰管理的安全事件日誌紀錄

表 D.5 包含與 GDOI 相關之事件。

表 D.5 對映本系列標準第 14 部之 GDOI 安全事件日誌

安全事件	本標準 節次	助憶符	嚴重性	事件識別 符	文字	額外資訊
未支援 GDOI 密碼演算法	8.2	IKEv1_C ALG_MISM ATCH	錯誤	IEC 62351- 9:5.1	未支援密碼演 算法之提議。	
GDOI 填墊錯誤	8.2	IKEv1_PA DDING	錯誤	IEC 62351- 9:5.2	IKEv1 訊息解密 期間出現填充 錯誤。	
GDOI-PULL 逾 期 SA 之使用	8.5.11	GROUP_P ULL_EXPI RED_SA	警告	IEC 62351- 9:5.3	請求使用逾期 之 SA。	
GDOI-PULL 階 段 2 解密議題	8.5.11	GROUP_P ULL_PHA SE2_DEC RYPTION	警告	IEC 62351- 9:5.4	無法解密階段 2 訊息。	
GROUPKEY- PULL 請求未知 群組之金鑰	8.5.11	GROUP_P ULL_PHA SE2_GRO UP_NONE XISTENT	警告	IEC 62351- 9:5.5	請求未知群組 之金鑰。	
GROUPKEY- PULL 無法同意 PHASE 1 金鑰	8.5.11	GROUP_P ULL_PHA SE1_KEY_ NEGOTIA TION	通知	IEC 62351- 9:5.6	無法協商 GDOI PHASE 1。	
GROUPKEY- PUSH 無法抵達 之目的地	8.6.2	GROUP_P USH_UNR EACHABL E_DESTIN ATION	錯誤	IEC 62351- 9:5.7	嘗試發送予無 法抵達之群組 成員。	
KDA 不成功	8.6.3	KDA_FAI LURE	通知	IEC 62351- 9:5.8	無法將 KDA 提 供予發布者。	

參考資料

- [1] RFC 2631, Diffie Hellman Key Exchange, June 1999.
<https://tools.ietf.org/html/rfc2631>
- [2] Ecommerce PKI Glossary, <http://www.ecommercepki.com/cps/glossary.htm>
- [3] CNS TS 62351-1, Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues, January 2007
- [4] IEEE 1588, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, Version 2.1, 11/2019
- [5] IEEE 1686:2022, IEEE Standard for Substation Intelligent Electronic Devices Cyber Security Capabilities, 2013 (currently under revision)
- [6] ISO/IEC 11770-1:2009, Information technology – Security techniques – Key management Part 1: Framework, December 2009
- [7] ISO/IEC 11770-2:2008, Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques
- [8] ISO/IEC 11770-3:2008, Information technology – Security techniques – Key management – Part 3: Mechanisms Using Asymmetric Techniques
- [9] ISO/IEC 19790:2012, Information technology – Security techniques – Security requirements for cryptographic modules
- [10] ISO/IEC 8802-3-2000, Telecommunications and information exchange between systems, October 2006
- [11] NIST SP 800-130, A Framework for Designing Cryptographic Key Management Systems, Elaine Barker, Miles Smid, Dennis Branstad, Santosh Chokhani, April 2012
- [12] NIST SP 800-133, Recommendation for Cryptographic Key Generation, Elaine Barker and Allen Roginsky, July 2012
- [13] NIST SP 800-57, Recommendation for Key Management – Part 1: General (Revision 5), May 2020
- [14] NIST SP 800-90 A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Elaine Barker and John Kelsey, January 2012
- [15] NIST SP 800-90 B, Recommendation for the Entropy Sources Used for Random Bit Generation, Elaine Barker and John Kelsey, August 2012
- [16] NIST SP 800-90 C, Recommendation for Random Bit Generator (RBG) Constructions, Elaine Barker and John Kelsey, August 2012
- [17] NIST SP 800-97, Establishing Wireless Robust Security Networks, Sheila Frankel, Bernard Eydt, Les Owens, Karen Scarfone, February 2007
- [18] IETF RFC 2986:2000, PKCS #10: Certification request Syntax Specification Version 1.7 [19] IETF RFC 2985:2000, PKCS #9: Selected Object Classes and Attribute Types Version 2.0, <https://tools.ietf.org/html/rfc2985>

- [20] IETF RFC 4211:2005, Internet X.509 Public Key Infrastructure – Certificate Request Message Format (CRMF), <https://tools.ietf.org/html/rfc4211>
- [21] PKCS #11, Cryptographic Token Interface Standard – Version 2.4, RSA Laboratories, June 2003
- [22] R. Kissel, Glossary of Key Information Security Terms, NIST IR 7298, April 2006. http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf
- [23] RFC 2407, Internet Security Association and Key Management Protocol (ISAKMP), November 1998, <http://www.ietf.org/rfc/rfc3647.txt>
- [24] RFC 2818, HTTP Over TLS, E. Rescorla, May 2000 <http://www.ietf.org/rfc/rfc2818.txt>
- [25] RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, February 2003 <https://www.rfc-editor.org/pdf/rfc/rfc3447.txt.pdf>
- [26] RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu, November 2003, <https://tools.ietf.org/html/rfc3647>
- [27] RFC 3740, The Multicast Group Security Architecture, T. Hardjono, B. Weis, March 2004, <https://tools.ietf.org/html/rfc3740>
- [28] RFC 4082, Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction, June 2005, <https://tools.ietf.org/html/rfc4082>
- [29] RFC 4120, The Kerberos Network Authentication Service (V5), July 2005, <https://tools.ietf.org/html/rfc4120>
- [30] RFC 4210, Internet X.509 Public Key Infrastructure Certificate Management Protocols, September 2005, <https://tools.ietf.org/html/rfc4210>
- [31] RFC 4476, Attribute Certificate (AC) Policies Extension, May 2006, <https://tools.ietf.org/html/rfc4476>
- [32] RFC 4754, IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA), January 2007
- [33] RFC 4949, Internet Security Glossary, Version 2, August 2007. <https://tools.ietf.org/html/rfc4949>
- [34] RFC 5055, Server-Based Certificate Validation Protocol (SCVP), December 2007 <https://tools.ietf.org/html/rfc5055>
- RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2, August 2008 <https://tools.ietf.org/html/rfc5246>
- RFC 5272, Certificate Management over CMS (CMC), June 2008, <https://tools.ietf.org/html/rfc5272>
- [35] RFC 5273, Certificate Management over CMS (CMC): Transport Protocols, June 2008, <https://tools.ietf.org/html/rfc5273>
- [36] RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate

- Revocation List (CRL) Profile, May 2008, <https://tools.ietf.org/html/rfc5280>
- [37] RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010, <https://tools.ietf.org/html/rfc5639>
- [38] RFC 5905, Network Time Protocol Version 4: Protocol and Algorithms Specification, June 2010, <https://tools.ietf.org/html/rfc5905>
- [39] RFC 5996, Internet Key Exchange Protocol Version 2 (IKEv2), September 2010, <https://tools.ietf.org/html/rfc5996>
- [40] RFC 5998, An Extension for EAP-Only Authentication in IKEv2, September 2010, <https://tools.ietf.org/html/rfc5998>
- [41] RFC 6066, Transport Layer Security (TLS) Extensions: Extension Definitions, D. Eastlake 3rd, January 2011, <https://tools.ietf.org/html/rfc6066>
- [42] RFC 6712, Internet X.509 Public Key Infrastructure – HTTP Transfer for the Certificate Management Protocol (CMP), September 2012, <https://tools.ietf.org/html/rfc6712>
- [43] RFC 7748, Elliptic Curves for Security, January 2016 <https://tools.ietf.org/html/rfc7748>
- [44] RFC 8366, A Voucher Artifact for Bootstrapping Protocols, May 2018, <https://tools.ietf.org/html/rfc8366>
- [45] RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3, August 2018 <https://tools.ietf.org/html/rfc8446>
- [46] RFC 8520, Manufacturer Usage Description Specification, March 2019, <https://tools.ietf.org/html/rfc8520>
- [47] RFC 8995, Bootstrapping Remote Secure Key Infrastructures (BRSKI), May 2021, <https://tools.ietf.org/html/rfc8995>
- RFC 8951, Clarification of Enrollment over Secure Transport (EST): transfer encodings and ASN.1, November 2020, tools.ietf.org/html/rfc8951
- [48] IETF Draft, Lightweight CMP Profile, <https://datatracker.ietf.org/doc/draft-ietf-lamps-lightweight-cmp-profile/>
- [49] BSI/AIS31, A proposal for: Functionality classes for random number generators, September 2011 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Zertifierung/Interpretation/AIS31_Functionality_classes_for_random_number_generators.pdf
- [50] FIPS PUB 201-1, Personal Identity Verification, March 2006
- [51] IANA Service Name and Transport Protocol Port Number Registry, <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>
- [52] IANA Assignments for GDOI Payloads, <https://www.iana.org/assignments/gdoi-payloads/gdoi-payloads.xhtml>
- [53] FIPS PUB 140-2, Security requirements for cryptographic modules, May 2001 <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
- [54] IEC 62351-12, Power systems management and associated information exchange –

- Data and communications security – Part 12: Resilience and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems
- [55] IEC 62351-1, Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues
 - [56] IEC 62351-8, Power systems management and associated information exchange – Data and communications security – Part 8: Role-based access control
 - [57] NIST Special Publication 800-57 Part 1 Rev. 5, Recommendation for Key Management, 05/2020, <https://doi.org/10.6028/NIST.SP.800-57pt1r5>
 - [58] TR-02102-1, BSI Technical Guideline: Cryptographic Mechanisms: Recommendations and Key Lengths, 02/2022, <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf>
 - [59] RFC 8915, Network Time Security for the Network Time Protocol, September 2020, tools.ietf.org/html/rfc8915/
 - [60] Standards for Efficient Cryptography, <http://www.secg.org/sec2-v2.pdf>
 - [61] NIST SP 800-90A, Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators
 - [62] RFC 4086, Randomness Requirements for Security, June 2005, <https://tools.ietf.org/html/rfc4086>
 - [63] FIPS PUB 186, Digital Signature Standard (DSS), 1994
 - [64] FIPS PUB 186-5, Digital Signature Standard (DSS), 2023, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf>
 - [65] FIPS PUB 186-4, Digital Signature Standard (DSS), 2013, <https://doi.org/10.6028/NIST.FIPS.186-4>
 - [66] FIPS PUB 180-4, Secure Hash Standard (SHS), 2015, <https://doi.org/10.6028/NIST.FIPS.180-4>
 - [67] FIPS PUB 198-1, The Keyed-Hash Message Authentication code (HMAC), 2008, <https://doi.org/10.6028/NIST.FIPS.198-1>
 - [68] NIST SP 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, 2007, <https://doi.org/10.6028/NIST.SP.800-38D>
 - [69] NIST SP 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, 2007, <https://doi.org/10.6028/NIST.SP.800-38C>
 - [70] FIPS 140-3, Security Requirements for Cryptographic Modules, 2019, <https://doi.org/10.6028/NIST.FIPS.140-3>
 - [71] ISO/IEC 19790, Information technology – Security techniques – Security requirements for cryptographic modules, 2012
 - [72] NIST SP 800-56A Rev.3, Recommendation for Pair-Wise Key-Establishment

- Schemes Using Discrete Logarithm Cryptography, 2018,
<https://doi.org/10.6028/NIST.SP.800-56Ar3>
- [73] IEC 62443-3-3, Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels, 2013
- [74] IEC 62443-4-2, Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components, 2019
- [75] IEEE c37.240, IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems, 2015 (currently under revision)
- [76] RFC 8572, Secure Zero Touch Provisioning (SZTP),
<https://datatracker.ietf.org/doc/html/rfc8572>
- [77] RFC 8032, Edwards-Curve Digital Signature Algorithm (EdDSA), January 2017,
<https://tools.ietf.org/html/rfc8032>
- [78] Alexandra Institute, Post-Quantum Cryptography, [Alexandra-Institutet-Whitepaper-Post-Quantum-Cryptography.pdf](#)
- [79] RFC 8410, Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure, August 2018,
<https://datatracker.ietf.org/doc/html/rfc8410>
- [80] RFC 5758, Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA, January 2010,
<https://datatracker.ietf.org/doc/html/rfc5758>
- [81] RFC 3279, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, April 2002, <https://datatracker.ietf.org/doc/html/rfc3279>
- [82] RFC 5480, Elliptic Curve Cryptography Subject Public Key Information, March 2009, <https://datatracker.ietf.org/doc/html/rfc5480>
- [83] NISTIR 8309, Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process, July 2020,
<https://doi.org/10.6028/NIST.IR.8309>
- [84] NIST White Paper, Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, April 2021, <https://doi.org/10.6028/NIST.CSWP.04282021>
- [85] RFC 4231, Identifiers and Test Vectors for HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512, December 2005,
<https://datatracker.ietf.org/doc/html/rfc4231>
- [86] RFC 9044, Using the AES-GMAC Algorithm with the Cryptographic Message Syntax (CMS), June 2021, <https://datatracker.ietf.org/doc/html/rfc9044>
- [87] ISO/IEC 18031, Information technology – Security techniques – Random bit generation, 2011
- [88] ISO/IEC 20543, Information technology – Security techniques – Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408, 2019

- [89] NIST SP 800-131A Rev.2, Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019, <https://doi.org/10.6028/NIST.SP.800-131Ar2>
- [90] Draft ISO/IEC 9594-12 | Rec. ITU-T X.508, Information technology – Open systems interconnection – Part 12: The Directory: Key management and public-key infrastructure establishment and maintenance

名詞對照

- A -

advance encryption standard, AES	先進加密標準
asymmetric key	非對稱金鑰
authenticated encryption with associated data, AEAD	具關聯資料之鑑別加密
authorization and validation list, AVL	授權及驗核清單
authorizer	授權者

- C -

certification authority, CA	憑證機構
certification path	驗證路徑
certification request	驗證請求
cipher block chaining	密碼區塊鏈接
cipher suite	密碼套組
cofactor	共因數
controllership	控制權
cookie	訊錄
credential	信符
cross certification	跨域憑證
cryptographic algorithm	密碼演算法
cryptographic key	密碼金鑰
cyclic group	循環群

- D -

deactivated	停用
digital signature	數位簽章
distinguished encoding rule, DER	區別編碼規則
distinguished name, DN	區別名稱
domain of interest, DOI	關注領域

- E -

end entity	終端個體
end point	端點
enrolment	登錄
enrolment over secure transport	透過安全傳送登錄

- F -

fingerprint	特徵;指紋
-------------	-------

- G -

generator	產生器;生成元
group domain of interpretation, GDOI	解譯之群域
group member, GM	群組成員

- H -

hash message authentication code, HMAC	雜湊訊息鑑別碼
--	---------

- I -

identity, ID	識別資訊
individual identity	個別身分
integrity check value, ICV	完整性核對值

- K -

key derivation function, KDF	金鑰衍生函數
key distribution centre, KDC	金鑰配送中心
key download, KD	金鑰下載
keyed-hash message authentication code, HMAC	金鑰雜湊訊息鑑別碼

- L -

legal ownership	合法所有權
-----------------	-------

- M -

message authentication code, MAC 訊息鑑別碼

- N -

native 原生

nonce 單次隨機數

- O -

object 物件；客體

object identifier, OID 物件識別符

one-time-password 單次通行碼

online certificate status protocol, OCSP 線上憑證狀態協定

- P -

plain text 明文

precision time protocol, PTP 精密時間協定

pre-shared key, PSK 預先共享金鑰

private key 私密金鑰

public-key cryptography standards, PKCS 公開金鑰密碼標準

- R -

random number generation, RNG 隨機數產生

registration authority, RA 註冊機構

relying party 依賴方

renewal 更新

- S -

secure hash algorithm, SHA 安全雜湊演算法

security association, SA 安全關聯

security parameter index, SPI 安全參數指標

session key 會期金鑰

signatory	簽署者
simple certificate enrolment protocol, SCEP	簡單憑證登錄協定
subject	主體
symmetric key	對稱金鑰
- T -	
traffic-encrypting key, TEK	訊務加密金鑰
transport layer security, TLS	傳送層安全
trust anchor	信任錨
- V -	
validation	驗核
verification	查證

相對應國際標準

IEC 62351-9:2023 Power systems management and associated information exchange
– data and communications security – part 9: cyber security key
management for power system equipment