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 3 部：通訊網路及系統安全－含 TCP/IP 之剖繪

Power systems management and associated information exchange − Data and communications security − Part 3: Communication network and system security - Profiles including TCP/IP

CNS 62351-3(草-制1150157):2026

中華民國　年　月　日制定公布
Date of Promulgation:　-　-

中華民國　年　月　日修訂公布
Date of Amendment:　-　-

※

目錄

前言

本標準係依據 2023 年發行之 IEC TR 62351-3，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與健康作業，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。

簡介(INTRODUCTION)

本標準係獨立文件，剖繪 TLS 之使用供安全電力系統通訊。建議參考本版標準，而非任何先前版本，因本版更新所使用之密碼演算法(密碼套組)，強化功能，且涵蓋不同 TLS 版本。與先前版本相比，本標準明確規定所有必要之 TLS 特定設定，並未要求參引標準以對 TLS 定義特定設定。

要注意到對使用本版標準之建議，亦可能具有較舊版之參引標準，要求採本版標準中所規定之 TLS 設定，實作技術支援。

1. 適用範圍

1.1 適用範圍

本標準規定對使用 TCP/IP 作為訊息傳送層，並在要求網宇安全時採用傳送層安全(TLS)之協定，如何提供機密性、完整性保護及訊息層鑑別。此可關係到 SCADA/遠端控制、保護、自動化及控制協定。

本標準規定如何經由傳送層安全協定(TLS)(定義於 RFC 5246 之 TLSv1.2，定義於 RFC 8446 之 TLSv1.3)之訊息、程序及演算法規格上的限制條件，保護依 TCP/IP 之協定的安全。在特定子節中，將包含用於說明不同目標 TLS 版本在應用中之差異及共通性子節。外部安全裝置(例如〝線間碰撞(bump-in-the-wire〞)之使用及規格，不在本標準討論範圍。

與前幾版相比，本標準係獨立完整定義 TLS 之剖繪。故可直接適用而無需規定更多 TLS 參數(於其上進行通訊之連接埠除外)。因此，本標準其可直接運用自參引標準，並可與其他層之安全措施合併。提供 TLS 之剖繪無規定更多 TLS 參數之需要，容許宣稱符合所述功能性無需引用其他本系列標準。

本標準旨在作為其他需要在類似邊界條件下，保障基於 TCP/IP 協定交換安全性之 CNS 標準之規範性組成部分加以引用。然而，仍由個別協定安全自行決定係否參引本標準。。

本標準亦對支援錯誤處置、安全稽核存底、入侵偵測及符合性測試之特定條件，定義安全性事件。組織在為回應本標準所述錯誤條件所採取之所有行動，均超出本標準範圍，係期望由組織安全政策定義。

本標準反映 CNS 電力系統管理協定之安全要求事項。若其他標準提出新要求事項，則本標準可能需修訂。

1.2 預期讀者(intended audience)

本標準之預期初始讀者係電力系統管理及相關聯資訊交換場域中，開發或使用協定的專家。為使本標準所述措施有效，必須由應用 TLS 技術採用 TCP/IP 安全性之協定的規所格接受及參引。本標準之編撰係用以啟用該過程。

本標準預期之後續讀者係實作此等協議之產品開發者。

本標準部分內容亦有助於管理者及主管了解工作之目的及要求事項。

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 62351-1　電力系統管理及關聯資訊交換－資料及通訊安全－第 1 部：通訊網路及系統安全－安全議題簡介

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

ISO/IEC 9594-8 :2020 | Rec. ITU-T X.509 (2019)　*Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks*

RFC 5246 :2008　*The TLS Protocol Version 1.2*[1]

RFC 5280:2008　*Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

RFC 5288 :2008　*AES Galois Counter Mode (GCM) Cipher Suites for TLS*

RFC 5289:2008　*TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*

RFC 5746 :2010　*Transport Layer Security (TLS) Renegotiation Indication Extension*

RFC 6066:2011　*Transport Layer Security Extensions*

RFC 6176:2011　*Prohibiting Secure Sockets Layer (SSL) Version 2.0*

RFC 8422:2018　*ECC Cipher Suites for TLSv1.2 and earlier*

RFC 8446:2018　*The TLS Protocol Version 1.3*

RFC 9150:2021　*TLS* 1.3 *Authentication and Integrity only Cipher Suites*

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。

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

ISO 及 IEC 所維護用於標準化工作之用語資料庫，網址如下：

- IEC 電子百科：可自 http://www.electropedia.org/取得
- ISO 線上瀏覽平台：可自 http ://www.iso .org/obp 取得

3.2 縮寫

下列縮寫適用於本標準。

ACSE	關聯控制服務元件(Association Contro l Service Element)
AEAD	以相關聯資料鑑別加密(Authenticated Encryption with Associated Data)
BCP	最佳現行實務(Best Current Practice)
CRL	憑證註銷表列(Certificate Revocation List)
DER	區別編碼規則(Distinguished Encoding Rules)
DH(E)	Diffie-Hellman(暫時性)金鑰協議(亦參閱 CNS 62351-9)(Diffie Hellman(Ephemeral) Key Agreement (see also IEC 62351-9))
ECDH(E)	橢圓曲線 Diffie-Hellman(暫時性)金鑰協議(亦參閱 CNS 62351-9) Elliptic Curve based Diffie Hellman (Ephemeral) Key Agreement (see also IEC 62351-9))
ECDSA	橢圓曲線數位簽章演算法(Elliptic Curve Digital Signature Algorithm)
IV	初始化向量(Initialization Vector)
MAC	訊息鑑別碼(Message Authentication Code)
MitM	中間人(攻擊之形式)(Man-in-the-Middle (type of attack))
OCSP	線上憑證狀態協定(參閱 RFC 6960)(Online Certificate Status Protocol (see RFC 6960))
PICS	協定實作符合性陳述(Protocol Implementation Conformance Statement)
PIXIT	測試用協定實作額外資訊(Protocol Implementation eXtra Information for Testing)
PSK	預先共享金鑰(Pre-shared key)
TLS	傳送層安全(Transport Layer Security)

4. 本標準所應處之安全議題

4.1 一般

CNS 電力系統環境具有之運作要求事項，與許多使用 TLS 保護 TCP/IP 連線上資訊傳輸之資訊科技(IT)應用系統不同。此一方面要求用於鑑別實體之憑證之管理，其係於\CNS 62351-9 中處置。另一方面，需要定義特定 TLS 相關安全參數，諸如選定之密碼套組、會期管理參數及利用之延伸事項，此係本標準之焦點。於電力系統域，TLS 係指需要維護安全性之 TCP/IP 連線之持續時間。此外，亦必須考量到電力系統自動化中之設備係經久耐用。此可能亦要求支援舊版之 TLS 或密碼套組，以保持向後相容性(backward compatibility)。

許多 IT 協定具有短連線持續時間，其容許在連線重新建立時重新協商加密演算法。然而，遠端控制環境中之連線往往持續時間較長，通常係〝永久性(permanent)〞。其為電力系統管理域及相關聯資訊交換中連線之長期性，此引發特殊考量之需要。為此，欲能對〝永久性〞連線提供保護，本標準選擇了一種依既有 TLS 特徵之會期金鑰更新機制。要注意到 TLSv1.2 及 TLSv1.3 對重設金鑰(rekying)支援不同作法。

TLS 容許多樣化設置，諸如選定密碼套組用以保護交握過程及紀錄層協定，其係於連線建立期間協商。其亦支援會期管理機制，用以設立新會期或更新現存會期。為確保不同實作之間之互運性，本標準規定由符合實作所要支援之一組共通 TLS 特徵。

TLS 已發展至 1.3 版。於 1.3 版，協定之若干部件已完成重工，其在功能上與 TLSv1.2 不向後相容。由於首次訊息交換係以向後相容之途徑定義，TLS 伺服器可能依安全性政策切換到此 2 版本其中之一。

此外，本標準規定特殊 TLS 能力之使用，其顧及所要反制之特定安全威脅(亦參閱 4.2 節)。具體而言，TLS 容許對協定延伸之定義，以緩解潛在之協定脆弱性或去強化協定功能性。本標準妥善利用已定義之延伸事項。

要注意到 TLS 運用 X.509 憑證(另參閱 ISO/IEC 9594-8 或 RFC 5280)供鑑別及金鑰協議。於本標準，用語〝憑證〞始終指公開金鑰憑證(與屬性憑證相比)。

註：假定運作 TLS 所必要之憑證管理係按照 CNS 62351-9 應處。

4.2 安全威脅反制

安全威脅及攻擊方法之討論，參閱 CNS 62351-1。

本標準中之 TCP/IP 及安全規格僅涵蓋通訊傳送層(OSI 第 4 層及以下)。具體而言，TLS 以透明之方式保護來自 OSI 第 5 層及以上傳送之訊息。本標準不涵蓋通訊應用層(OSI 第 5 層及以上)或應用程式間安全之特定安全功能性。此等內容在 CNS 62351 之其他部定義，例如，CNS 62351-4 對 MMS，CNS 62351-5 對串列通訊及遠端控制，而 CNS 62351-6 對(R)GOOSE 及(R)SV。

註：本標準中所剖繪 TLS 之應用程式，支援在 TLS 所保護的連線上所發送之資訊的保護。

本標準所對抗傳輸層之特定威脅包括：

- 竄改(未經授權之修改或插入訊息)係藉由通訊參與者間之相互、依憑證之鑑別以及 TLS 封包層完整性保護來應處。

此外，當資訊已識別要求保密保護時：

- 透過訊息之 TLS 封包層加密，未經授權存取資訊。

4.3 所反制之攻擊方法

下列安全攻擊方法，係透過適切實作本標準中之規格及建議事項加以反制。

- 冒充：本項威脅係透過在 TLS 交握期間，使用依 X.509 憑證之相互鑑別，以及數位簽章資訊作為註銷資訊來應處。
- 中間人(MitM)：TLS 紀錄層係透過使用依會期金鑰之相互鑑別協商之密碼式核對合(MAC)來反制本項威脅。此等金鑰係於 TLS 交握期間設定。在 TLS 交握階段本身，係由 Finish 訊息提供對 MitM 攻擊之保護以結束交握階段。此訊息係經加密，並內含交握中所交換之所有訊息的雜湊值。此外，TLSv1.3 已直接提供交握訊息(ClientHello 訊息除外)之密碼式保護。
- 重演：透過應用 MAG 提供完整性保護，按封包包括序號以偵測實際重演來反制本項威脅。
- 竊聽：在協商 TLS 紀錄層安全性時，使用加密密碼套組來反制本項威脅。

註：宣稱符合本標準之實作的實際績效特性，非屬本標準範圍。

4.4 安全性事件之處置

終本標準，皆在定義安全性事件。此等安全性事件旨在支援錯誤處置，從而提升系統彈性。實作宜提供用以向評估系統通告安全性事件之機制。建議之標準係 CNS 62351-4。

關於安全性事件及潛在細部資訊之資訊，僅能由實體透過底層平台或所採用的組件，依資訊之可用性提供。

建議將本標準中所定義之安全性事件，由 IEC 62351-14 所規定之網路安全性事件，或 CNS 62351-7 中所規定的監控對象，提供給運作基礎設施。附件 A 提供本標準所定義之事件與 IEC 62351-14 概念之對映。

要注意到通知(notice)、警告(warning)、錯誤(error)及告警(alarm)係用於從安全之視點，指示事件之嚴重性。下列觀念係引用自 IEC 62351-14：

- 通知係指實體之日常使用或維護過程期間與網宇安全相關之活動。不涉及網宇安全漏洞或攻擊或實體偏離正常運作情況。

- 警告係實體偏離正常運作情況，但非必然係網宇攻擊。
- 錯誤描述未預見之情況，其可能指出未經授權之活動。其可能不要求立即採取行動。
- 告警係嚴重問題之指示，其可能指出未經授權之活動。

無論如何，可預期組織之安全政策依運作環境判定事件之最終處置。例如，1 或多個告警之評鑑可能升級成事故。建議立即採取行動。

5. TLS 版本差異概述

5.1 一般

本節簡短概述 TLS 1.2 版與 TLS 1.3 版間之主要差異。經具體應處者為密碼套組之命名、向後相容性及延伸，其已在本標準之先前版本中使用。

5.2 TLSv1.2 與 TLSv1.3 間之主要差異

以下列出 TLSv1.2 及 TLSv1.3 於不同子協定(TLS 交握、TLS 紀錄層)間之主要差異(注意，RFG 8446 提供自 TLSv1.2 至 TLSv1.3 之完整變更表列)，其與 CNS 62351-3 中 TLSv1.2 所使用之特徵有關：

- TLSv1.3 交握往返次數較少(單邊鑑別會期一次往返，雙邊鑑別會期 1.5 次往返)。
- TLSv1.3 交握訊息係經加密，除了 ClientHello 及部分 ServerHello 以明文發送。要注意到，IETF 中有正持續之工作以定義延伸事項，容許對部分 ClientHello 加密，如 Server Name Indication (SNI)產生經加密的 SNI(ESNI)，或將整個 ClientHello 加密成為經加密之 ClientHello(ECH)。
- — TLSv1.3 移除對過時而脆弱之密碼學演算法之支援：輸出級加密法(Export cipher)、DES、3DES、AES-CBC、RC4、MD5 及 SHA-1 均不再予以支援。
- TLSv1.3 改變金鑰建立
  - 移除任意 Diffie-Hellman 群組
  - 金鑰建立係依短暫性 Diffie-Hellman
  - 不支援 RSA 金鑰加密
- TLSv1.3 移除會期重新協商，但對金鑰及 IV 更新以及客戶端鑑別(client authentication)提供交握後訊息(post-handshake message)。
- TLSv1.3 藉由使用 PSK 及會期權證(session ticket)簡化會期恢復。
- TLSv1.3 引入交握後訊息供
  - 會期權證
  - 客戶端鑑別
  - 金鑰及 IV 更新
- 依據 RFC 6961 (status_request_v2)，TLSv1.3 移除對 OCSP 回應之多重裝訂支援。而係以一種直接變體取代，容許由 CertificateEntry 之延伸，將 OCSP 回應，裝訂到憑證鏈中之憑證上。
- TLSv1.3 對客戶端憑證引入 OCSP 裝訂，其對行業使用案例可能特別重要，於其中伺服器通常位於查核所接收憑證之註銷狀態之能力可能有限之現場裝置上。
- TLSv1.3 移除供 TLS 紀錄層保護之非 AEAD 密碼套組。要注意到僅供完整性保護之密碼套組已定義在 RFC 9051。
- TLSv1.3 提供在首次往返(O-RTT)中具已加密應用程式資料，但安全性會隨之降低(給由攻擊者重播之選項)。要注意到本標準明確未使用此選項。
- 要注意到 ChangeCipherSpec 係獨立之 TLSv1.2 協定內容型式，並非 TLS 交握訊息。ChangeCipherSpec 已於 TLSv1.3 中移除。

5.3 密碼套組命名法

TLSv1.3 中之 TLS 交握及紀錄層處置之變更事項，亦反映在密碼套組定義中。

TLSv1.2 及先前版本中之密碼套組合併了 TLS 交握期間供鑑別及金鑰協議之演算法，以及供紀錄層之加密及訊息鑑別(完整性)之演算法，如圖 1 所示。因此，密碼套組兼具考量 TLS 交握及紀錄層二者。通常，各密碼套組皆有名稱，其係由底線分隔之助憶符(mnemonic)組成，格式如圖 1 所示。

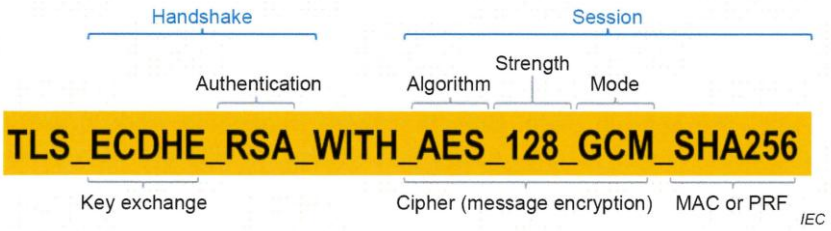
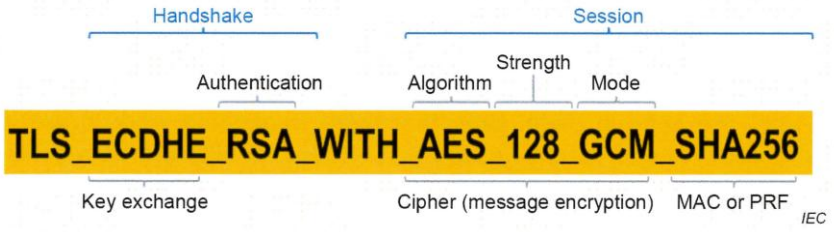


圖 1 依據 TLSv1.2 (RFC 5246)定義之密碼套組

Handshake	交握
Session	會期
Authenticaion	鑑別
Algorithm	演算法
Strength	強度
Mode	模式
Key exchange	金鑰交換
Cipher(message encryption)	密碼法(訊息加密)
MAC or PRF	MAC 或 PRF



於 TLSv1.3，密碼套組之命名法變更成僅與紀錄層相關。因此，其包含關於所採用之加密方案(始終為經鑑別加密)以及依雜湊之金鑰衍生函數中所採用之雜湊值之資訊，如圖 2 所示。

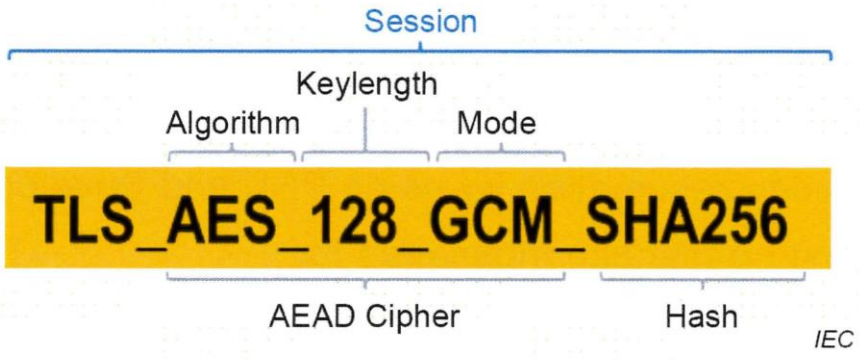
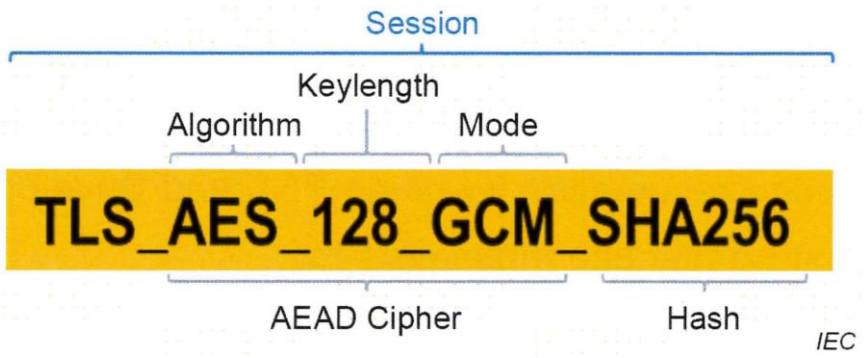


圖 2 – 依據 TLSv1.3 (RFC 8446) 定義之密碼套組

Session	會期
Algorithm	演算法
Strength	強度
Mode	模式
AEAD Cipher	AEAD 密碼法
Hash	雜湊值



於 TLS 交握所使用之演算法係經明確標示，作為 ClientHello 及 ServerHello 交換之一部分。

5.4 向後相容性

TLS 藉由在與 1.x 版本訊息完全相容之 Client.Hello 訊息中標示 TLS 版本資訊，以確保向後相容性。要注意到已不同意 TLSv1.2 版協商機制，而係以在延伸中使用版本表列取代。具體言之，能在 Client.Hello 訊息中優先使用 supported_versions 延伸協商欲使用之 TLS 版本，而非 Client.Hello 訊息中之 legacy_version 欄位。此係旨在提升與現有伺服器(其所實作版本協商不正確)之相容性。

5.5 延伸事項

延伸事項提供在 TLS 之某些交握訊息中包括額外資訊的選項。如 5.2 節所述，TLSv1.2 中可用之某些特徵係在 TLSv1.3 不受支援或處置不同。因此，某些延伸事項在 TLSv1.3 中係不適用或無支援必要。

IEC 62351-1 版次 1(2007 年)規定性使用之延伸事項包括：

- renegotiation_info：重新協商延伸事項定義在 RFC 5746，將所重新協商之會期綁定至先前會期。
- trusted_ca_keys：容許客戶端出示本機有效之 CA 憑證，其能用於驗核所接收到之伺服器憑證(定義在 RFC 6066)。
- signature algorithms:容許客戶端標示其支援之簽章演算法(作為雜湊演算法及簽章演算法之組合) (定義在 RFC 5426 (TLSv1.2)及 RFC 8446 (TLSv1.3)二者)。

於此等延伸事項，僅 signature_algorithm 延伸在 2 個 TLS 版本皆有支援。TLSv1.3 規定任一端皆能用於標示所支援之 CA 供接收端指引之〝certificate_authorities〞延伸取代 trust_ca_keys。TLSv1.3 不支援 renegotiation_info 延伸，因不支援會期重新協商。

此外，TLSv1.3 規範本標準所頗繪之支援延伸事項。不同 TLS 版本之特定子節中將提供所支援之延伸事項表列。

6 一般性要求

6.1 一般

本節定義適用於本標準中所考量之所有 TLS 版本之要求事項。

若設立 TLS 會期之交握執行成功(滿足第 6 節、對 TLSv1.2 之第 7 節或 TLSv1.3 之第 8 節中概述之要求事項)，應引發安全性事件(〝通知：TLS 交握成功執行〞【/〝notice: TLS handshake successfully performed〞？翻譯成中文或保留原文？】)。若於 TLS 通道建立期間發生錯誤而無法建立 TLS 會期，則第 6 節、TLSv1.2 第 7 節或 TLSv1.3 第 8 節中所定義之安全性事件將提供細部資訊。

本標準之參引標準應規定供執行 TLS 所保護的通訊之埠號。

6.2 所支援 TLS 版本之標示

RFC 5246 所定義之 TLSv1.2 係預設版本，應予以支援。TLSv1.3 係 TLS 之最新版本，建議予以支援。

建議發起 TLS 連線之 TLS 客戶端在 TLS 交握的 ClientHello 訊息中指出所支援之最高 TLS 版本。若功能性支援且作業環境之安全政策容許，接收 TLS 伺服器可接受較高版本。

TLSv1.2 及 TLSv1.3 對版本訊標示處置不同。於 TLSv1.2，版本編號係以 ClientHello 訊息中 ProtocolVersion 之一部分提供，並標示由客戶端所支援的最高 TLS 版本。

客戶端應在 ProtocolVersion 中包括 TLSv1.2 識別符 0x0303 以標示其支援 TLSv1.2。若用戶端亦支援 TLSv1.3，在 ClientHello 訊息之 supported_versions 延伸中指出其版本偏好。於此情況，supported_versions 延伸中之 ProtocolVersion 應依據 RFC 8446 設為 TLSv1.3 識別碼 0x0304。要注意到支援 TLSv1.3 之伺服器於接收到具 supported_versions 延伸的 ClientHello 訊息時，將不使用 ClientHello 訊息之 ProtocolVersion 欄位中所標示的 TLSv1.2 版本。

為確保向後相容性，實作可選項支援 TLS 版本 1.0 及 1.1(有時亦稱為 SSL v3.1 與 3.2)。TLS 交握提供支援版本協商所應使用之內建機制。發起 TLS 連線之對等方(peer)，應全程於 TLS 交握訊息期間指出所支援之最高 TLS 版本。非 v1.2 之 TLS 版本的應用，係本機安全性政策之事務。版本早於 TLS v1.0 之提案，應導致無安全連線建立(亦參閱 RFC 6176)。

註 1：TLSv1.0 及 TLSv1.1 之某些脆弱性係已知。再者，IETF 於 RFC 8996 中發布 BCP，不同意 TLSv1.0 及 TLSv1.1。可選用支援係旨在僅供向後相容。

僅支援 TLSv1.0 或僅支援 TLSv1.1 或僅此二者，應予預設停用，並要求由組織之安全性政策授權才能單獨啟用。若停用此支援，則僅有 TLSv1.0 或僅有 TLSv1.1 或僅有此二者之提案，應引發安全性事件(〝告警：不安全之通訊：所提之 TLS 版本不同意〞/〝alarm: unsecure communication: deprecated TLS version proposed〞)，而接收方應終止會期建立。若啟用支援，TLSv1.0 或 TLSv1.1 版本之提案，應引發安全性事件(〝警告：不安全之 TLS 版本〞/〝warning : insecure TLS version〞)。

不應使用 TLSv1.0 前之版本。TLSv1.0 前之版本或僅有 SSLv3.1 之提案，應引發安全性事件(〝告警：不安全通訊：所提之 TLS 版本不容許〞 / 〝alarm: unsecure communication: disallowed TLS version proposed〞)，且接收者應終止會期建立。

註 2：IETF 已在 RFC 7568 不同意 SSLv3.0。

若所協商之 TLS 版本變更自初始 TLS 交握，則應終止 TLS 會期：

如圖 3 所示，安全係不斷演進之過程，而非靜止不動。採行持續工作及教育，以協助安全過程跟得上處於系統上之需要式項。安全將會是公司安全政策/安全基礎建設與敵對實體間之持續競爭。安全過程及系統於未來亦將持續演進。按定義，無 100%安全之通訊連線系統，裝備亦非絕對萬無一失。總是會有宜納入考量及管理之殘餘風險。因此，為維護安全，需要保持持續警覺及監控，並適應整體環境之變更。

- TLSv1.2 及較低版本：於 TLS 會期重新協商或會期恢復交握期間；
- TLSv1.3：依 TLSv1.3 中雙方提供之 PSK 身分的會期恢復。

會期終止，應引發安全性事件(〝告警：偵測到正進行之通訊中所申請的 TLS 版本變更(可能降級〞 / 〝alarm : requested TLS Version change (potential downgrade) in ongoing communication detected〞)。

註 3 RFC 8446 明確禁止在 TLSv1.2 重新協商期間進行版本變更以升級至 TLSv1.3。

6.3 非加密密碼套組之用法

若不能保證以其他手段加密此通訊連接，則所有規定 NULL 為加密值之密碼套組不應用於管理域以外的通訊。

註 1：本標準不排除透過使用密碼式 VPN 通道使用加密通訊。此類 VPN 之使用超出本標準範圍。

於管理域內，可能容許使用非加密式密碼套組，其使用係運作者之職責。

註 2：容許使用非加密式密碼套組供訊務檢驗，同時仍維持訊務之端對端鑑別及完整性保護。

若通訊連線係僅旨在堅固涉及所傳輸資訊之完整性，則下列密碼套組可與 TLSv1.2 及較低版本搭配使用：

– TLS_RSA_WITH_NULL_SHA256(定義於 RFC 5246)

註 3：CNS 62351-3 支援此密碼套組

TLS_RSA_WITH_NULL_SHA。由於 SHA-1 不同意，此可選用支援已移除。

TLS_SHA256_SHA256 (RFC 9150)

TLS_SHA384_SHA384 (RFC 9150)

容許 TLS 密碼套組搭配宣稱符合本標準 NULL 加密之實作事項，應提供明確啟用該等 TLS 密碼套組之機制。於預設情況，非加密 TLS 密碼套組應予停用。

6.4 憑證支援

6.4.1 多信任錨之支援

CA 相關之信任錨提供憑證驗核(尤其憑證路徑驗證)的基礎。由於預期到實體與屬不同領域之實體互動，需支援不同的信任錨。實際數量取決於目標使用案例。

宣稱符合本標準之實作應支援至少 5 個信任錨(通常稱為根 CA 憑證)作為最低數量。

CA 之準則及選擇超出本標準討論範圍。

於 IED 上有超過 1 個 X.509 憑證(及對應私密金鑰)可用之情景，可能期待啟用申請者於伺服器端，選擇與申請者端的可用受信任錨(根 CA)憑證相符之憑證。

6.4.2 憑證長度

宣稱符合本標準之實作，應能處理最大長度至少為 8192 位元組之憑證。實際支援之憑證長度應予記錄。

註 1：憑證亦可依據 CNS 62351-8 載送會影響其最終長度(final size)之角色資訊。

註 2 憑證長度可能會受到核發者之謹慎選擇及主題與支援的延伸等之影響。

TLS 交握期間，若長度超過憑證之最大支援長度，應引發安全性事件(〝告警：TLS 憑證長度超限〞 / 〝alarm : TLS certificate size exceeded〞)，並終止 TLS 會期建立。

要注意到憑證長度之限制關係到來自上層協定(例如 MMS)之潛在要求事項。對於 MMS，為達成公開金鑰憑證之互運性，有必要為由 ACSE 交換的公開金鑰憑證設定最大容許長度。

本項長度限制描述於 CNS 62351-4。若相同憑證用於 MMS 及 TLS 之全景，則需遵守此邊界條件。

若憑證不在更高憑證長度限制條件之下，製造商可支援更大的 TLS 憑證長度。

6.4.3 憑證交換

憑證交換及驗核應係雙向以達成相互鑑別。若任一實體未提供其憑證，則連接應予終止。

註：伺服器憑證係於 ServerHello 訊息中載送。客戶端憑證係於 Certificate 訊息中載送。

TLS 交握期間因缺少對等方憑證所導致之連線終止，應引發安全性事件(〝告警：對等方憑證不可用〞 / 〝alarm: peer certificate unavailable〞)。

無能力存取本機端點憑證及對應私密金鑰，應引發安全性事件(〝告警：端點憑證不可用〞/〝alarm: endpoint certificate unavailable〞)。

6.4.4 公開金鑰憑證驗核

6.4.4.1一般

憑證應由呼叫方及被呼叫方雙方查證。此外，使用憑證前，各方均應依照本節所概述驗核各自之憑證，而更具體亦涉及按照定義於 CNS 62351-9 所包括的憑證延伸事項。

應有兩種可組態機制供憑證驗核。

– 接受來自獲授權 CA 之所有憑證

– 接受來自獲授權 CA 之個別憑證(發行 CA 之限制範圍)

6.4.4.2依所選定之發行 CA 查證

宣稱符合本標準之實作，應能組態成為接受來自 1 或更多憑證機構之憑證，無需個別憑證之組態。

TLS 交握期間尋找匹配 CA 憑證失敗，應引發安全性事件(〝告警：憑證驗核：CA 憑證不可用〞

/〝alarm：certificate val idation: CA certificate not available〞)，並終止 TLS 會期建立。

6.4.4.3 依來自所選定之發行 CA 之個別憑證查證

宣稱符合本標準之實作，應能組成為接受來自 1 或更多憑證機構之個別憑證(受信賴憑證表列)。個別憑證之組態，可能為依憑證的主體名稱或序號加上發行 CA 之資訊。

註 1：依個別憑證之查證，可能受自動化憑證更新程序影響，通常會變更憑證序號。

註 2 依個別憑證之查證，可能由 CNS 62351-9 中所概述之憑證機構及驗核表列提供支援。

TLS 交握期間尋找匹配之個別憑證失敗，應引發安全性事件(〝告警：憑證驗核：來自獲獲授權 CA 之受信賴個別憑證不可用〞/〝alarm: certificate validation: trusted individual certificate from authorized CA not available〞)，並終止 TLS 會期建立。

6.4.4.4 憑證註銷查核

6.4.4.4.1 一般

憑證註銷應依循 ISO/IEC 9594-8 所規定之規定性參數及程序。CRL 之管理係本機實作議題。對於 CRL 管理問題之討論，能在 CNS 62351-1 找到。CRL 之應用，係於 CNS 62351-9 概述。

或者，對於本機 CRL，OCSP 可能用於查核所適用憑證之註銷狀態。OCSP 與 OCSP 回應器互動之應用，係概述於 CNS 62351-9。

若應用 OCSP，TLS 提供對傳輸 OCSP 回應訊息之支援，即所謂 OCSP 裝訂。對在 TLSv1.2 之伺服器憑證，此係可能，並於 7.5.5 節描述。TLSv1.3 對客戶端憑證及伺服器憑證支援 OCSP 回應之裝訂，如 8.8.10 節所描述。

宣稱符合本標準之實作，應能夠在可組態的時間區間，查核所接收憑證之註銷狀態。

憑證註銷查核可能依 TLS 協定特徵(像是對 TLSv1.2 會期重新協商)，或由監控所利用之憑證的應用程式調用。

於應用程式監控所利用之 TLS 憑證的情況，要求應用程式保持追蹤 TLS 會期建立所使用之對等方憑證，並依可組態的時間調用憑證註銷查核。為容許在憑證註銷之情況下的操作行動(例如，提供有效信符或對執行相關 IED 之安全性查核)，應用程式可提供一個寬限期(以小時為單位)，此期間可執行此等行動而無需立即終止當前會期。若未提供寬限期，則要求應用程式終止相關聯之連線。寬限期之預設值為 0 小時(即無寬限期)。要注意到對應用程式之寬限期組態係本機實作議題，且可能按照組織之安全政策，須獲得核可。

已註銷之憑證不應用於建立 TLS 會期(TLSv1.2 及 TLSv1.3)。實體於會期建立期間收到已註銷憑證應拒絕連線。實體於 TLSv1.2 會期重新協商過程中收到已註銷之憑證，應終止連線。

於會期建立或會期重新協商期間偵測到已註銷之憑證，應引發安全性事件(〝告警：憑證驗核：已註銷之憑證〞 /〝alarm: certificate validation: revoked certificate〞)。

已註銷之憑證造成 TLS 連線的終止，應引發安全性事件(〝告警：已註銷之憑證造成會期終止〞/〝alarm：session terminated due to revoked certificate〞)。

要注意到已註銷之憑證可能導致 TLS 會期終止。因此，系統管理者宜制定憑證管理程序以緩解此情況(亦參閱 CNS 62351-9)。再者，期望設立安全管理過程，在分發 CRL 或 OCSP 回應之前評估，以避免通訊連線的意外切斷而可能影響到系統之可靠性。實作事項亦支援各裝置使用多個憑證以動態切換至另一(有效)憑證。要注意到後者之選項係本機實作議題。

6.4.4.4.2 憑證註銷查核使用 CRL

查核 CRL 之過程不應導致已建立之會期終止。

對於 TLSv1.2，肇因於已註銷之憑證的 TLS 會期切斷，將隨下次會期重新協商而生效，如 7.4.5 節所概述。此處可保留一段寬限期(憑證註銷及偵測到正在使用之已註銷之憑證間)，供運作者處置已註銷的憑證。另一選擇係由應用程式處置憑證註銷查核，如 6.4.4.4.1 節所概述。

註 1：因 TLSv1.2 容許會期重新協商，其通常由 TLS 協定堆疊執行，且能調用應用程式來執行憑證驗核，尤其是註銷查核。

由於 TLSv1.3 不支援會期重新協商，其為應用程式之職責，發動憑證驗核並對偵測到之已註銷憑證採取相應措施，尤其係在長時間會期中。此要求應用程式在連線建立期間保持追蹤所使用之憑證。此係概述於 6.4.4.4.1 節。

建議本機 CRL 之刷新週期為 24 小時。CRL 本身亦於 nextUpdate 欄位中包含 CRL 將於何時更新之資訊。CRL 之刷新宜以先到者為準。如欲取得新 CRL，宜聯絡發行 CA 之分發點。無法存取 CRL 分發點不應導致會期終止。本機 CRL 不可用，應引發安全性事件(〝警告：本機 CRL 無法存取〞 / 〝warn ing : local CRL not accessible〞)。無法存取本機 CRL 不應造成會期終止。

註 2 CRL 可以透過不同途徑分發(手動以檔案形式分發、自 CRL 分發點取得等)。

註 3 若沒有已註銷之憑證，則 CRL 為表列空，但仍然可用。

本機 CRL 逾期，應引發安全性事件(〝警告：CRL 逾期〞 / 〝warning: CRL expired〞)，但不應造成會期終止。

6.4.4.4.3 憑證註銷查核使用 OCSP

宣稱符合本標準之實作，宜能夠與 OCSP 回應程式互動以取得註銷資訊。

當以裝訂之 OCSP 作為 TLS 交握的一部分回應提供時，宣稱符合本標準之實作，應能處理 OCSP 回應訊息。

註：與 OSCP 回應者互動，亦提供 OCSP 回應訊息。

OCSP 回應逾期，應引發安全性事件(〝警告：OCSP 回應已逾期〞 / 〝warning: OCSP response expired〞)。

OCSP 回應具有由 nextUpdate 值指示之逾期時間。本項容許快取 OCSP 回應。若 OCSP 適用，則 OCSP 回應之快取，應以最長 24 小時支援。

若 OCSP 係用於憑證註銷查核，則 OCSP 回應者之不可存取性應引發安全性事件(〝警告：OCSP 回應者不可存取〞 / 〝warning : OCSP responder not accessible〞)。

對於 TLSv1.2 及伺服器憑證訊息之憑證表列中所包含之中間 CA 憑證，RFC 6066 定義了憑證狀態請求(status_request)及回應延伸。7.5.5 提供更多細節。

TLSv1.3 提供支援供請求及裝訂 OCSP 回應，依 RFC 6066 中所述(由客戶端或伺服器端所提供憑證表列中)之所有憑證。8.8.10 提供更多細節。

6.4.4.5 逾期憑證

逾期憑證不應用於 TLS 會期之建立(TLSv1.2 及 TLSv1.3)或重新協商(僅限 TLSv1.2)。實體於會期建立其間收到逾期憑證，應拒絕連線(TLSv1.2 及 TLSv1.3)。實體於 TLSv1.2 會期重新協商期間收到逾期憑證，應終止連線。

要注意到安全管理過程已就緒，以及時發起憑證延期程序(亦參閱 CNS 62351-9)。例如，時框可能為一個月。

各個裝置亦可能支援多個憑證，以榮許切換至另一(有效)憑證。

肇因於憑證逾期所致之拒絕建立初始會期或重新協商會期，應引發安全性事件(〝警報：憑證驗核：憑證逾期〞 / 〝alarm : certificate validation: expired certificate〞)。

6.4.4.6 簽章演算法

金鑰交換期間對簽章加密演算法之支援，係定義給 7.4 節中的 TLSv1.2 及 8.3 中之 TLSv1.3。

於 TLS 交握期間找尋與憑證元件相符之簽章演算法失敗，應引發安全性事件(〝告警：憑證驗核：無支援之簽章演算法〞/〝alarm: certificate validation : signature algorithms not supported〞)。

於 TLS 交握期間驗核所接收憑證之簽章失敗，應引發安全性事件(〝告警：憑證驗核：無法驗證憑證簽章〞 / 〝alarm : certificate validation : certificate signature could not be verified〞)。

要注意到對所支援簽章演算法之指示，必須對定義在 7.5.4 中的 TLSv1.2 及 8.8.4 (簽章演算法)與 8.8.4.2(簽章演算法憑證)中之 TLSv1.3 使用適切延伸。

6.5 與非安全協定訊務共存

參引標準要求對非安全協定訊務之支援，可規定如何處理安全及非安全通訊的共存。此可藉由

對 TLS 安全訊務提供單獨之 TGP/IP 做到。

7 TLSv1.2 特定要求事項

7.1 一般

IEC62351-3 之早期版本要求對 TLS 處置或 TLS 協定特徵支援提供附加定義之參引標準。

本標準已將此等定義已整合。此外，對 TLSv1.2 之描述，已與參引標準 lEC 62351-3:2014+AMD1:2018+AMD2:2020 中提供的 TLS 相關參數規格(即 IEC 62351-4:2018+ AMD1 :2018+AMD2:2020，其係 lEC 62351-4:2018+ AMD1 及 CNS 62351-8)保持一致。

7.2 所支援之密碼套組

於表 1 中，本標準規定對 TLSv1.2(及以下版本)強制支援及可選支援之密碼套組。

表 1-對 TLSv1.2 密碼套組之支援

金鑰交換		加密	雜湊	IANA 值	來源	支援
演算法	簽章					
TLS_RSA -		WITH_NULL	SHA256	0x00,0x3B	RFC 5246	c1
TLS_RSA -		WITH_AES_128_CBC_	SHA256	0x00,0x3C	RFC 5246	m
TLS_DHE	RSA	WITH_AES_128_GCM_	SHA256	0xC0,0x9E	RFC 5288	m
TLS_DHE	RSA	WITH_AES_256_GCM_	SHA384	0x00,0xA1	RFC 5288	o
TLS_ECDHE	RSA	WITH_AES_128_GCM_	SHA256	0xC0,0x2F	RFC 5289	m
TLS_ECDHE	RSA	WITH_AES_256_GCM_	SHA384	0xC0,0x30	RFC 5289	o
TLS_ECDHE	ECDSA	WITH_AES_128_GCM_	SHA256	0xC0,0x2B	RFC 5289	m
TLS_ECDHE	ECDSA	WITH_AES_256_GCM_	SHA384	0xC0,0x2C	RFC 5289	o
c1: 若僅要完整性保護，可予以支援。此等密碼套件應預設應停用，並要求經組織之安全性政策授權才能單獨啟用。						

可能支援其他密碼套組。為選定此等密碼套組，宜依循 IETF 之建議。對其他密碼套組之互運性，取決於此等密碼套組之對等方支援(peer support)。

運作環境中最終選定之密碼套組，取決於組織之安全政策。由於本標準支援多種規定性密碼套組，因此，若不想要向後相容性，運作者可以選擇不使用未提供 PFS 之密碼套組。

支援 NULL 供加密之密碼套組的處置，細說明於 6.3。

7.3 不容許之密碼套組

不容許之密碼套組表列包括但不限於：

- TLS NULL WITH NULL NULL
- 含 TLS_*_ *_MD5 之密碼套組(不容許 MD5 對所有組合鑑別)
- 含 TLS_*_DES_*之密碼套組(不容許 DES 對所有組合加密)

在 TLS 交握期間，客戶端及服務端對不容許之密碼套組的標示方式不同：

若不容許之密碼套組僅於 ClientHello 提案，則應在 TLS 伺服器引發安全性事件(〝告警：所提出之 TLSv1.2 密碼法套件不容許〞 / 〝alarm: disallowed TLSv1.2 cipher suite proposed〞)。

若在 ServerHello 訊息標示出不容許之密碼套組，TLS 用戶端應引發安全性事件(〝告警：所提出之 TLSv1.2 密碼法套件不容許〞 / 〝alarm: disallowed TLSv1.2 cipher suite proposed〞)。

若在密碼套組中，於 ClientHello 提出不容許之密碼套組，則 TLS 伺服器應忽略此不容許之提案。

只要任何一方標示不容許之密碼套組，應終止會期建立。

期望 TLS 客戶端/伺服器運用表 1 所列示之 TLS 密碼套組。除不容許之套組外，容許利用其他密碼套組，但不保證互運性。宜依運作者之風險評鑑使用其他密碼套組。

若密碼套組表列排除 7.2 所陳述之密碼套組，且由本機安全性政策覆蓋，將導致不符合第 3 部【IEC TS 62351-100-3？？】(100-3 PIXIT 中之負面測試個案)。

7.4 金鑰交換

7.4.1 一般

金鑰交換機制係由所支援之密碼套組判定，如 7.2 所述。

7.4.2 金鑰交換機制

所要支援之金鑰交換機制，係與列示於 7.2 所支援之密碼套組一致，包括：

- 公鑰加密使用 RSA
- 短暫性 Diffie-Hellman 金鑰協議
- 依橢圓曲線之短暫性 Diffie-Hellman 金鑰協議

註：對 TLSv1.2 所定義之密碼套組，亦支援依 RSA 簽章及橢圓曲線 Diffie-Hellman 的混合。

7.4.3 密碼式演算法

透過使用 RSA 及 ECDSA 演算法之簽署，應予支援。

對於依 RSA 之簽章，下列金鑰長度，應予支援：

- 規定性：簽章操作：RSA，金鑰長度至少為 2048 位元。

金鑰長度為 2048 位元之 RSA 演算法，應予支援。2048 位元係對 RSA 簽章所支援之最小金鑰長度。依 NIST SP800-57 或 BSI TR01202-1 之建議，強烈建議同時支援金鑰長度為 3072 位元及以上之 RSA 演算法，以應處密碼學之進步。簽章演算法之選擇取決於組織之安全性政策。

不同意對 1024 位元 RSA 金鑰之支援。其係僅限於向後相容使用。對 1024 位元 RSA 金鑰之支援應預設停用，並要求係由組織之安全性政策授權單獨啟用。若停用 1024 位元 RSA 金鑰，則偵測到長度小於 2048 位元之 RSA 金鑰時，應引發安全性事件(〝告警：RSA 金鑰長度不足 << 2048 位元〞 / 〝alarm : insufficient RSA key length «2048 bit〞)，且接收者應終止會期建立。若啟用 1024 位元 RSA 金鑰，則偵測到長度在 1024 <= RSA 金鑰長度 < 2048 位元範圍內之 RSA 金鑰，應引發安全性事件(〝警告：金鑰長度不足〞 / 〝warning: minimum key length〞)。

若無法使用大於 1024 位元之金鑰，建議採取額外之安全措施。

不應使用小於 1024 位元之 RSA 金鑰。偵測到小於 1024 位元之 RSA 金鑰，應引發安全性事件(〝告警：金鑰長度不足〞 / 〝alarm: insufficient key length〞)，接收者應終止會期建立。

應以下列金鑰長度，支援 ECDSA 公鑰演算法：

- 規定性：簽章操作：ECDSA 金鑰長度至少為 256 位元

註 1：關於簽章演算法所要求金鑰長度之建議，係持續接受審查，可在 NIST SP800-57、BSI TR 02102-1 或 NSA Suite B 中找到。

對於依定義在有限質數體上採用 ECDSA 簽名演算法之橢圓曲線的簽章，最小金鑰長度為 256 位元(結合 SHA-256)。對所要使用之 ecdsa-with-SHA256，OID 係：iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)。

宣稱符合本標準之實作，應支援具以下曲線之 ECDSA：

{OID}

seep256r1: {iso(1) member-body(2) us(840) ansi-X9-62(10045) curves(3) prime(1) prime256v1(7)}.

Implementations claiming conformance to this standard shall support ECDSA with the curve :

對 ECDSA，可選擇支援以下曲線{OID}：

- seep384r1: {iso(1) identified-organization(3) certicom(132) curve(O) ansip384r1(34)}
- seep521r1: {iso(1) identified-organization(3) certicom(132) curve(O) ansip521r1(35)}
- brainpoo1P256r1: {iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecStdCurvesAndGeneration(8) ellipticCurve(1) versionOne(1) brainpoolP256r1(7)}
- brainpoo1P384r1: {iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecStdCurvesAndGeneration(8) ellipticCurve(1) versionOne(1) brainpoolP384r1(11)}
- brainpoo1P512r1: {iso(1) identified-organization(3) teletrust(36) algorithm(3)

signatureAlgorithm(3) ecSign(2) ecStdCurvesAndGeneration(8) ellipticCurve(1) versionOne(1) brainpoolP512r1(13)}

SHA-256 應予支援，且係首選擬使用之雜湊演算法。

不同意 SHA-1 之支援，其僅限於向後相容使用。已不再承認 SHA-1 對抗碰撞性係安全，因此強烈建議使用此演算法前執行風險評鑑。若不能使用 SHA-256，亦建議採取額外安全措施。

註 2：IETF 發布了 RFC 9155，不同意 TLSv1.2 中之 MD5 及 SHA-1 簽章雜湊。

偵測到 SHA-1 之使用，應引發安全性事件(〝警告：使用不同意之雜湊演算法〞 / 〝warning: deprecated hash algorithm used〞)。

實體之安全政策，應能夠不容許或阻止對所有可選雜湊演算法之支援。

註 3：有關簽章演算法之建議，係持續接受審查，可在 NIST SP800-57、BSI TR 02102-1 或 NSA Suite B 中找到。

欲標示所支援之簽章演算法，應使用 7.5.4 中描述之〝signature_algorithm〞延伸。

7.4.4 會期恢復

於 TLSv1.2 中之會期恢復功能，容許依會造成新會期金鑰、與專用(既有)預主秘密(pre-master secret)連結的 sessionID，將會期恢復或重設金鑰。此極小化非對稱交握之效能衝擊，且能在會期運轉期間或已定義之會期結束後一段時期內做到。

TLS 在 RFC 5246 中建議給 sessionID 之存活時間不超過 24 小時。本標準遵循此建議。主動式會期應定期執行會期恢復。對結束之會期，會期可不遲於 24 小時(取決於 sessionID 存活時間)恢復。實際參數宜由運作者依風險評鑑予以定義。

若會期恢復係依會期識別符(如 RFC 5246 中所述)執行，且 sessionID 已逾期，則 TLS 客戶端及伺服器執行 RFC 5246 段落 7.3 的全部逐項交握。於此情況，應引發安全性事件(〝通知：會期無法恢復，sessionID 存活時間期已逾期。改為執行全部 TLS 交握〞 / 〝notice: Session could not be resumed session_ID lifetime expired. Performing a full TLS handshake instead〞)。

預期到主動式會期之恢復而更新會期金鑰，將比會期重新協商頻繁。為此理由，會期恢復時間間隔應小於會期重新協商間隔。以下公式提供對設定各自值之建議：0<會期恢復間隔<會期重新協商間隔<= 24 小時。

宣稱符合本標準之實作，應對主動式會期，支援會期恢復間隔之組態。對會期恢復間隔之預設值宜為 6 小時。

註 1：對預設值之理由說明，亦參閱 7.4.5 中的資訊性範例。

客戶端應使用 ClientHello 訊息發起會期恢復。

註 2：IEC62351-3 之前期版本容許伺服器發送 HelloRequest 訊息來觸發 TLSv1.2 中的伺服器所發起之會期恢復。但根據 RFC 5246，由於 HelloRequest 係僅用於觸發會期重新協商，因而已予刪除。

只要客戶端及伺服器二者之安全性政策皆容許，可由客戶端發起會期恢復。設若恢復會期失敗，應遵循 TLSv1.2 中所述之失敗處置機制。或者，會期恢復可依會期識別符(按照 RFC 5246 之原生 TLS)做到，亦可依會期權證(RFC 5077)做到。後者選項，容許避免能恢復之會期處於伺服器端狀態。本選項可適用於資源受限裝置，以避免較大之會期快取(session cache)。

在權證式 TLS 會期(ticket-based TLS)恢復作法中，TLS 伺服器產生會期權證。此權證以經加密之形式包含會期全景資訊，容許 TLS 伺服器重建先前關閉之會期，或依既有會期的金鑰材料建立新會期。會期全景係在僅有 TLS 伺服器知悉之權證金鑰下加密。此權證金鑰宜依組織之安全性政策定期換新。此係與操作相關之建議，其不會影響互運性。為與所容許之會期恢復時間保持一致，所發行權證的最大存活時間應係 24 小時。

註 3：會期權證之應用，避免在伺服器端上的會期特定儲存，提供於連線中斷並在特定時間後重新連線之環境中的優勢。若會期恢復係用於更新正進行中會期之會期金鑰，則可能沒有優勢。若對同一 TLS 連線利用 TLS 會期恢復，則應按 7.5.2 之概述，使用 TLS 會期重新協商延伸。

要注意到若係為了重新建立先前已關閉之 TLS 會期而執行會期恢復，則在會期恢復期間不會驗核用於建立原始會期的憑證。本項處置係類似於 6.4.4 所概述，在所定義之週期後的憑證定期驗核之作法。要注意到為了能做憑證驗核，實作可需要儲存對等方憑證。

7.4.5 會期重新協商

於 TLSv1.2，會期重新協商發起完整之 TLS 交握，其中金鑰交換期間之所有非對稱式運作都必須執行，包括憑證驗核。如 6.4.4.4 及 6.4.4.5 所概述，已註銷或逾期之憑證不應用於會期重新協商。

註 1：若應用程式在會期進行期間驗證憑證之結果，偵測到憑證已逾期或註銷，則到下次 TLS 會期重新協商之時間可提供一段寬限期，以便採取措施(例如，提供有效憑證或執行相關 IED 之安全查核)。本項通常由組織之安全政策處置。

會期重新協商將依全新協商之主金鑰及新會期金鑰的結果，建立新會期。由於此點具體涉及憑證驗核，供會期重新協商之時框，宜按照 6.4.4.4 所述的註銷狀態資訊(CRL)之刷新週期擇定。會期重新協商間隔應係可組態，只要其係位於指定之最大時間週期內，且應與 CRL 更新週期保持一致。若 OCSP 係用於憑證註銷查核，則會期重新協商應係與 OCSP 回應快取時間保持一致。無論如何，對於長時間連線，應至少每 24 小時執行重新協商，強制執行憑證有效期限查核。較短間隔可由參引標準定義。

註 2：對齊之例係〝*Y*〞，1/2 CRL 刷新時間或〝*Y*〞，1/2 OCSP 回應快取時間以限制未偵測到已註銷憑證之可能性。

宣稱符合本標準之實作，應支援會期重新協商間隔之組態。TLS 會期重新協商應於最多 24 小時時間週期內完成。供會期重新協商之預設值宜為 12 小時。

由實作對會期重新協商之支援，下限應至少為 10 分鐘。

註 3：本項要求藉由防止過多全部 TLS 交握及相關聯之公開金鑰憑證驗核，保護客戶及伺服器效能。

只要 TLS 客戶及 TLS 伺服器二者之安全性政策都容許使用此特徵，會期重新協商可由任一方發起。於會期重新協商失敗之情況，應遵循 TLSv1.2 中所述的失敗處置。

呼叫實體(TLS 客戶端)及被呼叫實體(TLS 伺服器)，係負責驗證在預期的間隔所發生的 TLS 會期重新協商。若呼叫實體於所預期間隔內未收到被呼叫實體之 TLS 會期重新協商請求(HelloRequest)，則呼叫實體應使用 ClientHello 自行發起 TLS 會期重新協商。若被呼叫實體未收到對 HelloRequest 之回應(ClientHello)，則被呼叫實體應終止連線。由錯過 TLS 會期重新協商所導致之連線終止，宜引發安全性事件(〝告警：會期重新協商間隔逾期〞/〝alarm: session renegotiation interval expired〞)。

宣稱符合本標準之實作，應支援 HelloRequest 之處理。

註 4：根據 RFC 5246，HelloRequest 係伺服器可發送給客戶端之選項訊息。

註 5：期待客戶端及伺服器係以相同之 TLS 安全性政策設定組態。

為避免會期重新協商中之安全漏洞，應使用 7.5.1 所概述，定義於 RFC 5746 的會期重新協商延伸。

註：以下資訊性範例係提供予組態會期重新協商及會期恢復：

- 假定之 CRL 刷新時間(或 OCSP 回應有效期限)為 24 小時。
- 會期重新協商涉及對等方憑證之驗核，含註銷查核。涉及供鑑別用的對等方憑證會期重新協商，可能至少每 12 小時執行一次。
- 為容許在 12 小時之會期重新協商間隔期間更新會期金鑰，會期期間係每 6 小時執行會期恢復。用以恢復先前已結束之會期的最長時間為 24 小時。

7.5 延伸事項之支援

7.5.1 一般

本子節定義對 TLS 交握之延伸，其係規定性或可選，由符合的實作事項支援。各子節對所考量之延伸參引此規格。

7.5.2 TLS 會期重新協商延伸

TLSv1.2 及較低版之定義，並未考慮於初始會期重新協商的會期之間，提供密碼式綁定。本項所缺少之綁定，可能容許攻擊者於正進行中的 TLS 連線建立中注入內容(亦稱為三重交握攻擊)。為應處此攻擊，RFC 5746 定義重新協商延伸，其將重新協商之 TLS 會期，綁定到執行重新協商之 TLS 會期。符合之實作事項，必須支援此會期重新協商延伸。

根據 RFC 5746，TLS 客戶端在初始 ClientHello 訊息中包括〝renegotiation_info〞延伸。於初始交握期間，本項延伸為空，且將標示客戶端對安全重新協商之支援。同樣，若 TLS 伺服器自客戶端偵測到此資訊且其支援會期重新協商，則在 ServerHello 訊息中會包括空的〝renegotiation_info〞延伸。於本標準全景，支援本項延伸係規定性。若任何一方偵測到初始交握中缺少〝renegotiation_info”，則應引發安全性事件(〝警告：不支援之安全會期重新協商(初始交握)〞 / 〝warning：secure session renegotiation not supported (initial handshake〞))。未使用本項延伸之會期重新協商，必須不予執行。

根據 RFC 5746，TLS 客戶端將前次交握之 Finish 訊息中發送的客戶端查證資料〝client_verify_data〞包括在重新協商之 ClientHello 訊息中的 renegotiation_info 延伸中。當發送對應之 ServerHello 訊息時，TLS 伺服器端將會在此延伸中包括〝client_verify_data〞並加上〝server_verify_data〞。若任何一方偵測到重新協商之交握中缺少 renegotiation_info 或其任何組成部分，而此支援係已標示在初始交握中，則應引發安全性事件(〝告警：不支援安全會期重新協商(重新協商之交握)〞 / 〝alarm: secure session renegotiation not supported (renegotiated handshake)〞)。會期應予中止。宣稱符合本規格之實作，應依據 RFC 5746 支援本項延伸。

依據 RFC 5746 段落 3.1，會期重新協商延伸係適用於同一 TLS 連線中之全部交握及已恢復的交握。因此，參數 client_verify_data 及 server_verify_data 係特定連線，並非 TLS 會期快取之一部分。若 TLS 會期恢復係對不同之 TLS 連線而做，則不能使用 TLS 會期重新協商延伸。對同一 TLS 連線之 TLS 會期恢復，應予使用。

註：通常係由 TLS 協定堆疊做到延伸之使用。

7.5.3 透過 Trusted CA 對客戶端所支援之 CA 憑證的標示

RFC 6066(段落 6)中所規定之 Trusted CA Indication 延伸，容許 TLS 客戶端提供有關本機所支援之 CA 憑證的資訊，因公用程式之根 CA 可能不公開。本項延伸容許請求方去影響在 IED 端 X.509 憑證之選擇，以供伺服器端鑑別，從而在請求者方啟用查證所使用之 X.509 憑證。

Trusted CA Indication 係包含在 ClientHello 訊息中。本延伸之〝extension_data〞欄位應為空。

接收 Trusted CA Indication 之 TLS 伺服器可使用本資訊指導其回給客戶端之適切憑證鏈的選擇。於本事件，根據 RFC 6066，伺服器應在(所延伸之)ServerHello 訊息中包括型式〝trusted_ca_keys〞之延伸。

宣稱符合本標準之實作，宜支援本延伸。

本延伸之支援，可能適用於 IED 係由不同管理域存取之情節，例如，具獨立公鑰基礎設施之 2 公用程式。若所擬支援者係不同管理域，則宜使用 TLS Trusted CA Indication 延伸。

使用本延伸並宣稱符合本標準之實作，可在 TLS 伺服器端規定所請求之 CA 所發行的憑證。

若選擇匹配之 CA 所發行的憑證失敗，則應引發安全性事件(〝告警：未找到 TLSv1.2 客戶端上所支援匹配之 CA 憑證〞 / 〝alarm: matching CA certificate supported on TLSv1.2 client not found〞)。

7.5.4 所支援簽章演算法之標示

RFC 5246 定義簽章演算法延伸，以容許客戶端指出哪些雜湊及簽章組合可用於憑證及 TLS 交握運作之數位簽章。

使用 TLSv1.2 之客戶端，應在 ClientHello 訊息中包括至少具：{SHA-1, RSAi SHA-256, RSAi

SHA-256, ECDSA}的組合之 signature_algorithm 延伸。SHA-1 及 RSA 之組合，係僅供向後相容(參閱下文)，且取決於組織之安全政策(亦參閱 7.4.3)。可支援其他組合。

註：若未包括 signature_algorithm，TLSv1.2 伺服器將落回預設值，其導致始終套用 SHA-1 雜湊。

偵測到缺少 signature_algorithm 延伸時，應引發安全性事件(〝警告：缺少簽章演算法延伸〞 / 〝warning: Signature algorithm extension missing〞)。

SHA-256 應予支援，且係擬使用之首選雜湊演算法。

已不同意 SHA-1。其使用係僅限於向後相容。已不再承認 SHA-1 對抗碰撞性係安全，故強烈建議使用此演算法之前執行風險評鑑。若不能使用 SHA-256，亦建議採取額外之安全措施。本標準之下一版本將禁止使用 SHA-1。

偵測到 signature_algorithm 組合 {SHA-1, RSA}，應引發安全性事件(〝警告：不同意之簽章演算法標示〞 / 〝warning：deprecated signature algorithm signalled〞)。

實體之安全政策，應能夠禁止或阻止正在支援的所有可選雜湊演算法。

附註：涉及雜湊簽章演算法之建議事項係持續審查，且可在 NIST SP800-57、BSI TR 02102-1 或 NSA Suite B 找到。

宣稱符合本標準之實作，應根據 RFC 6066 支援本項延伸。

7.5.5 OCSP 回應訊息之裝訂

7.5.5.1一般

OCSP 回應裝訂，容許伺服器將伺服器端憑證之註銷資訊，以 TLS 交握之一部分提供客戶端。若客戶端不能透過 CRL 或 OCSP 檢索註銷資訊，此機制之使用可能很有幫助。

TLSv1.2 存在有 2 種不同延伸事項，其可選項予以支援，且概述於 7.5.5.2 及 7.5.5.3。對此機制之規格，參引相對應之文件。

7.5.5.2OCSP 裝訂

RFC 6066(段落 8)對伺服器端憑證，定義 OCSP 回應之裝訂。

若 TLS 客戶端欲接收 OCSP 回應，可將〝status_request〞延伸包括在 ClientHello 訊息之 ExtensionType 中。此延伸中之資料係“CertificateStatusRequest”，含狀態型式“OCSPStatusRequest”及客戶端信任的 OCSP 回應者表列。若此表列為空，則伺服器隱含知曉 OCSP 回應者。亦有更多選項給 TLS 客戶端，像是在延伸中包括臨時數字(nonce)，其係由 OCSP 客戶端使用，用以查詢憑證註銷狀態。

TLS 伺服器收到帶有〝status_request〞延伸之 ClientHello 訊息，可在 CertificateStatus 訊息(其係由 RFC 6066 定義之一種新交握訊息)中以〝OCSPResponse〞回傳 OCSP 回應。本訊息緊緊跟隨由 TLS 伺服器所發送之〝Certificate〞訊息。

宣稱符合本標準之實作，應依據 RFC 6066 支援 status_request_v2 延伸。

要注意到本項未必要求 OCSP 與 OCSP 回應方互動之支援。

7.5.5.3OCSP 多重裝訂

定義在 RFC 6066 中之 OCSP 裝訂，對伺服器憑證提供 OCSP 回應提供選項，RFC 6961 定義 OCSP 回應之多重裝訂。此處亦支援對憑證鏈中之中間 CA 提供 OCSP 回應。此係透過提供更多資訊結構，以及強化原始定義於 RFC 6066 中之 ExtensionTypes 及 CertificateStatusTypes 而達成。

若 TLS 客戶端欲接收多個 OCSP 回應，其可在 ClientHello 訊息之 ExtensionType 中包括〝status_request_v2〞延伸。延伸中之資料係〝CertificateStatusRequestItemV2〞，包含狀態型式如〝OCSPStatusRequest〞及客戶端信任之 OCSP 回應者的表列。若此表列為空，則隱含伺服器係知曉 OCSP 回應者。亦有更多選項給客戶端，像是在延伸中包括臨時數字，其係由 OCSP 客戶端使用，以查詢憑證註銷狀態。

TLS 伺服器收到帶有〝status_request_v2〞延伸之 ClientHello 訊息，可在 CertificateStatus 訊息

(其係由 RFC 6066 定義之一種新交握訊息)中以〝OCSPResponseList〞回傳 OCSP 回應。此訊息緊緊跟隨由 TLS 伺服器所發送之〝Certificate〞訊息。

實作宜根據 RFC 6961 支援本項延伸。

要注意到本項未必要求 OCSP 與 OCSP 回應方互動之支援。

7.5.6 透過 Server Name Indication 對所擬定目標 TLS 伺服器之標示

RFC 6066(段落 3)定義〝server_name〞延伸，其能由 TLS 客戶端使用在 ClientHello 訊息中。本項延伸可由 TLS 客戶端使用以簡化情況，於其中多個(虛擬)TLS 伺服器係寄駐(host)在單一網路位址上。

標示所擬定目標伺服器名稱，容許伺服器選擇適切憑證以回應客戶端，或處置由安全性政策所關切之其他層面。

宣稱符合本標準之實作，宜根據 RFC 6066 支援本項延伸。

7.5.7 鑑別前加密之支援

在 TLSv1.2 中，預設供紀錄層安全之作法，係先 MAC 再加密(MAC-then-encrypt)。由於 CBC 密碼套組上之攻擊係已知(例如 LUCKY13、POODLE)，其巧妙運用操作順序，已定義用於反轉先加密再鑑別的順序之延伸。

RFC 7366 定義了〝encrypt_then_mac〞延伸，其能由 TLS 客戶端在 ClientHello 訊息中使用，以標示此支援。同樣，TLS 伺服器亦將此延伸包括在 ServerHello 訊息內。

由於本標準亦在 7.2 規定依 CBC 密碼套組之支援，實作應如 RFC 7366 所規定，支援本項延伸。若〝encrypt_then_mac〞延伸未包括在 ClientHello 或 ServerHello 訊息中，而密碼套組(CipherSuite)在 CBC 模式包含加密演算法，係在所支援之 CipherSuite(ClientHello)或所選定之 TLS 密碼套組(CipherSuite)標示，則應提供安全性事件(〝告警：偵測到使用先 MAC 再加密的 TLS 會期。〞/〝alarm: TLS session with MAC-then-encrypt detected.〞)會期應予終止。

8 TLSv1.3 特定要求事項

8.1 一般

本節描述對支援密碼套組、金鑰交換作法及設定事項之規定性，作為對 TLSv1.3 的剖繪，用以保護電力系統自動化通訊安全。

8.2 所支援之密碼套組

對於 TLSv1.3，本標準規定表 2 中規定性及選項性支援之密碼套組的支援。

表 2 -密碼套組對 TLSv1.3 之支援

密碼套組	IANA 值	來源	支援 (客戶端/伺服器端)
TLS_AES_128_GCM_SHA256	0x13,0x01	RFC 8446	m
TLS_AES_256_GCM_SHA384	0x13,0x02	RFC 8446	m
TLS_CHACHA20_POLY1305_SHA384	0x13,0x03	RFC 8446	o
TLS_AES_128_CCM_SHA256	0x13,0x04	RFC 8446	m
TLS_AES_128_CCM_8_SHA256	0x13,0x05	RFC 8446	o
SHA256_SHA256	0x13,0xB4	RFC 9150	c1
SHA384_ SHA384	0x13,0xB5	RFC 9150	c1
c1:若僅期待完整性，可能予以支援。此等密碼套組應預設停用，並要求係由組織之安全性政策授權單獨啟用。			

任何未指定使用 AEAD 密碼供加密之密碼套組，若無法透過其他方式確保通訊連線之加密，則不應用於管理域以外之通訊。若由其他方式不能保證本項通訊連線之加密，未規定 AEAD 密碼法供加密的所有密碼套組，不應用於對管理域以外連線。

註 1：本標準未排除經由使用密碼式 VPN 通道加密之通訊。此類 VPN 之使用，超出本標準範圍。

在管理域內，可容許使用非加密密碼套組，但其使用由運作者負責。

註 2：應用非加密式密碼套組，容許供訊務查核，同時仍維持端對端鑑別及訊務之完整性保護。容許使用無加密之 TLS 密碼套組的實作宣稱符合本標準，應提供明確啟用該等 TLS 密碼套組之機制。應預設停用非加密 TLS 密碼套組。

8.3 金鑰交換

8.3.1 一般

來自 RFG 8446 之要求事項，此處已遵循涉及簽章演算法對交握訊息及憑證的規定性支援。本項具體關係到：

- 數位簽署，具備 rsa_pkcs1_sha256(用於憑證)、rsa_pss_rsae_sha256(用於 CertificateVerify 訊息及憑證)以及 ecdsa_secp256r1_sha256 之規定性支援。
- 金鑰交換依橢圓曲線 secp256r1 之規定性支援。

欲換新會期金鑰，TLSv1.3 支援相較於 TLSv1.2 之不同新機制：

- 已定義新訊息 KeyUpdate 為交握後訊息，用於更新發送方之密碼金鑰材料(金鑰及初始化向量)。本項功能係用於會期期間自任一方更新會期金鑰。其係在 TLSv1.2 使用會期恢復(僅更新會期金鑰)及會期重新協商(更新會期金鑰並驗核雙方之憑證)實現。
- 新預先共享金鑰交握模式，容許利用前一次於 TLS 會期期間建立或透過外部方式提供之 PSK 協商新會期金鑰，而無需在會期建立之全景中包括憑證。此類似於 TLSv1.2 中(依權證)之無伺服器端狀態會期恢復。
- 根據 RFC 8446，係禁止會期重新協商。對於 TLSv1.2，CNS 62351-3 中使用會期重新協商，以便在一定時間後強制雙方依憑證之鑑別，其係擬與憑證註銷資訊之更新保持一致。與使用 TLSv1.2 相比，憑證驗核之調用必須由專供長持續時間之會期(超過 CRL 刷新週期)的應用程式處置，如 6.4.4.4 所概述。

8.3.2 交握模式

TLSv1.3 支援不同之交握模式。Diffie-Hellman 金鑰交換(DHE、ECDHE)係規定性支援，且係預設使用。

TLSv1.3 亦支援如表 3 中所表列之 PSK 模式，由支援並行 TLS 連線的會期恢復及/或建立，啟用更快之會期設置。

無關於所利用之交握模式，於 TLS 交握期間(直到 TLS 伺服器端收到 TLS 客戶端完成的訊息)不應提供經加密之應用程式資料。此亦與 RFC 8446 段落 2 一致。

要注意到對於 TLSv1.2，CNS 62351 利用會期恢復而強制實行會期金鑰更新或建立第二個 TLS 連線，其係綁定至初始連線之全部交握。於 TLSv1.3 中，存在顯然不同之機制用於會期期間更新會期金鑰，其能由任何一方發起。因此，TLSv1.3 中之會期恢復係旨在僅供建立另一安全連線，其係綁定至相同對等方間的初始 TLS 會期。

表 3 - TLSv1.3 對依 PSK 交握模式之支援

交握模式	參引	IANA 值	支援 (客戶端/伺服器端)
psk_ke	RFC 8446	0	x
psk_dhe_ke	RFC 8446	1	m
註：使用 psk_ke 時，不提供完美前向秘密性(forward secrecy)。			

依 PSK，TLSv1.3 啟用 O-RTT 交握，容許加密資料(由 early_data 延伸指示)隨同第一個訊息(ClientHello)傳輸。由於 PSK 如非以帶外(out-of-band)就是以先前會期結果方式提供，因此不能提供完美前向秘密性。於本標準全景中，不應使用 O-RTT。

為確保對所要建立之會期金鑰的完美前向秘密性，應由宣稱符合本標準的實作支援 psk_dhe_ke。僅使用 psk_ke 之選項，不要求伺服器端提供金鑰共享，並且不會對所協議之會期金鑰造成完美

前向秘密性。在本標準中，不應使用交握模式 psk_ke。

若 TLS 客戶端標示僅限 psk_ke 之支援，則應提供安全性事件(〝告警：僅限非短暫性 PSK 模式之支援〞 / 〝alarm : support of non-ephemeral PSK mode only〞)。會期應予終止。

8.3.3 Diffie-Hellman 群組

TLSv1.3 容許通訊對等方指定(EG)DHE 支援之使用者群組。在本標準中，表 4 中標記為規定性之 Diffie-Hellman 使用者群組應予以支援。選項群組可能予以支援。

表 4 - Diffie-Hellman 群組對 TLSv1.3 之支援

Diffie-Hellman 群組	參引	IANA 值	支援 (客戶端/伺服器端)
secp256r1	RFC 8422	23	m
secp384r1	RFC 8422	24	o
brainpoolP256r1	RFC 8734	31	o
brainpoolP384r1	RFC 8734	32	o
brainpoolP512r1	RFC 8734	33	o
ffdhe2048	RFC 7919	256	m
ffdhe3072	RFC 7919	257	o
ffdhe4096	RFC 7919	258	o

8.3.4 簽章演算法

8.3.4.1對交握訊息之簽章演算法

與 TLSv1.2 相比，TLSv1.3 容許更具體指示所期待之簽章演算法。此處提出 2 延伸事項(亦參閱 8.3.4.2)。signature_algorithm 延伸規定在 CertificateVerify 訊息中所要支援及使用之演算法。表 5 中所給之演算法係規定性予以支援，且在本標準的全景中可選項性與 signature_algorithm 一起使用。

表 5–在 TLSv1.3 中對交握支援之簽章演算法

簽章演算法	參引	IANA 值	支援 (客戶端/伺服器端)
rsa_pss_rsae_sha256	RFC 8446	0x0804	m
rsa_pss_rsae_sha384	RFC 8446	0x0805	o
rsa_pss_rsae_sha512	RFC 8446	0x0806	o
rsa_pss_pss_sha256	RFC 8446	0x0809	m
rsa_pss_pss_sha384	RFC 8446	0x080A	o
rsa_pss_pss_sha512	RFC 8446	0x080B	o
ecdsa_secp256r1_sha256	RFC 8446	0x0403	o
ecdsa_secp384r1_sha384	RFC 8446	0x0503	m
ecdsa_brainpool_P256r1_sha256	RFC 8734	0x081A	o
ecdsa_brainpool_P384r1_sha384	RFC 8734	0x081B	o
ecdsa_brainpool_P512r1_sha512	RFC 8734	0x081C	o

8.3.4.2對憑證之簽章演算法

TLS 1.3 容許在 signature_algorithms_cert 延伸中，指示擬用於憑證中簽章所期待的簽名演算法。根據 RFC 8446，若未包含 signature_algorithms_cert 延伸，則〝signature_algorthms〞延伸(參見 8.3.4.1)亦適用於在憑證中之簽署。表 6 中所列示之演算法應規定性予以支援，且可選項性與 signature_algorithms_cert 一起使用：

表 6–在 TLSv1.3 中對憑證所支援之簽章演算法

簽章演算法	參引	IANA 值	支援 (客戶端/伺服器端)
rsa_pkcs1_sha256	RFC 8446	0x0401	m
rsa_pkcs1_sha384	RFC 8446	0x0501	o
rsa_pkcs1_sha512	RFC 8446	0x0601	o

rsa_pss_rsae_sha256	RFC 8446	0x0804	m
rsa_pss_rsae_sha384	RFC 8446	0x0805	o
rsa_pss_rsae_sha512	RFC 8446	0x0806	o
rsa_pss_pss_sha256	RFC 8446	0x0809	m
rsa_pss_pss_sha384	RFC 8446	0x080A	o
rsa_pss_pss_sha512	RFC 8446	0x080B	o
ecdsa_secp256r1_sha256	RFC 8446	0x0403	m
ecdsa_secp384r1_sha384	RFC 8446	0x0503	o
ecdsa_brainpool_P256r1_sha256	RFC 8734	0x081A	o
ecdsa_brainpool_P384r1_sha384	RFC 8734	0x081B	o
ecdsa_brainpool_P512r1_sha512	RFC 8734	0x081C	o

子節 8.8.4 及 8.8.4.2 定義了相關延伸之使用。

8.4 會期金鑰更新(交握後訊息)

TLSv1.3 容許連線之任一方經由使用交握後訊息發送金鑰材料(金鑰及初始化向量)的更新。

宣稱符合本標準之實作，應支援對主動式會期金鑰更新間隔之組態。供金鑰更新間隔之預設值宜為 6 小時。

發送方之金鑰更新應使用 RFC 8446 中所述之交握後 KeyUpdate 訊息執行。由於本項僅限於更新發送方金鑰材料，發送者應在 KeyUpdate 結構中包括〝update_requested〞，以強迫接收者亦更新其發送金鑰材料。這將造成會期金鑰材料完全換新。KeyUpdate 之接收者應以相同方式換新其發送金鑰材料，並將〝update not requested〞包括在其 KeyUpdate 訊息中以避免發起者立即重設金鑰。

雙方實體(TLS 客戶端、TLS 伺服器)均負責查證 TLS 會期金鑰更新係依照安全性政策所定義執行。若任一方未接收到被呼叫方實體之 TLS Key_Update 以回應其自身的 Key_Update，呼叫方實體應終止連線。肇因於 TLS 會期金鑰更新失誤之連線終止，應引發安全性事件(〝告警：會期金鑰更新間隔已逾期〞 / 〝alarm: session key update interval expired〞)。

8.5 新會期權證(交握後訊息)

另一交握後訊息，NewSessionTicket(亦參閱 RFC 8446 段落 4.6.1)藉由提供會期權證支援會期恢復。

符合本標準之實作，應依 RFC 8446 所規定，支援交握後訊息 NewSessionTicket。

客戶端應藉由在恢復會期之 ClientHello 中將權證值納入 pre_shared_key 延伸(8.8.9)中，使用此會期權證供後續交握(參閱 8.6)。

在權證式 TLS 會期恢復作法中，TLS 伺服器產生會期權證，此處此權證包含加密形式之會期全景資訊，容許 TLS 伺服器重建先前已結束的會期。此會期全景係在使用僅 TLS 伺服器知曉之權證金鑰下加密。此權證金鑰宜依組織之安全性政策定期換新。此係與運作相關之建議，不影響互運性。

8.6 會期恢復

TLSv1.3 中之會期恢復機制，使用初始交握後用 NewSessionTicket 訊息(參閱 8.5)所建立的會期權證，恢復先前會期或在已連線實體間另外建立會期。會期恢復可在主動式會期期間執行，以建立其他連線。

註：根據 RFC 8446 段落 4.1.2，因 TLS 交握後，ClientHello 訊息將導致會期終止，主動式會期全景中不能執行會期恢復。

供會期恢復之會期權證，應以 24 小時之最大存活時間發行。

可依會期權證之有效期限時間，對已終止連線執行會期恢復。恢復已終止會期所使用的參數，應由運作者依風險評鑑定義。

符合本標準之實作，應支援會期恢復。

若使用會期恢復，應如 RFC 8446 段落 4.2.9 概述之 psk_dhe_ke 交握模式執行。

要注意到，若係執行會期恢復以重建先前已結束之 TLS 會期，則會期恢復期間不驗核用於建立原始會期之憑證。此如同 6.4.4 中所概述，於所定義之週期後定期驗核憑證的作法類似。要注意到，實作可能需要儲存對等方憑證，才能夠做憑證查證。

8.7 憑證驗核

TLSv1.3 禁止會期重新協商。RFC 8446 段落 4.1.2 明確陳述，若某伺服器在已建立之 TLSv1.3 連線中接收到 ClientHello 訊息，則必須終止此連線。會期重新協商係用於 TLSv1.2(亦參閱 7.4.5)中更新會期金鑰及調用雙方之憑證驗核。

如 6.4.4.4 所陳述，係要求支援在可組態之時間間隔，查核所接收憑證之註銷狀態。與使用 TLSv1.2 相比，憑證驗核之調用，必須由專供持續時間較長會期(較 CRL 刷新週期長)的應用程式處置。

8.8 延伸事項之支援

8.8.1 一般

本節定義對 TLS 交握之延伸事項。TLSv1.3 在段落 4.2 中規定，若無應用程式剖繪標準可用，則規定性實作延伸事項。CNS 62351-3 藉由採用 TLSv1.3 所要求之延伸事項，同時將其他延伸事項納入考量，規定此類 TLS 應用程式剖繪，並定義對支援延伸事項之規定性。

此係描述在 8.8.2、8.8.3、8.8.4、8.8.4.2、8.8.5、8.8.6、8.8.7、8.8.8、8.8.9 及 8.8.10 中對電力系統應用之全景。各子節參引此規格供所考量之延伸。

8.8.2 所支援 TLS 版本之標示

RFC 8446 段落 4.2.1 規定 ClientHello 訊息中之〝supported versions〞延伸，指示客戶端支援哪些 TLS 版本。在 ServerHello 訊息中指示伺服器端將使用何版本。此延伸包含依優先排序之支援 TLS 版本的表列。

宣稱符合本標準並支援 TLSv1.3 之實作，應在本項延伸中發送 TLSv1.3 識別符 0x0304。若安全性政策亦容許使用段落 6.2 所概述之 TLS 先前版本，其亦可包括較低 TLS 版本識別符。

根據 RFC 8446，所有 ClientHello、ServerHello 及 HelloRetryRequest 訊息皆要求〝supported_versions〞延伸。

8.8.3 訊錄(Cookie)

RFG 8446 段落 4.2.2 規定，當缺少應用程式剖繪時，係規定性由實作支援〝cookie〞延伸。其係由 TLS 伺服器在 HelloRetryRequest 訊息中使用，並由 TLS 客戶端在 ClientHello 訊息中反映。其係對 2 主要目的服務：

- 展現 TLS 客戶端在給定之網路位址下係可達成，其係有用於非連線導向傳送。
- 將狀態卸載到 TLS 客戶端之選項。

在本標準全景中，並未規定性使用 cookie 延伸保護以目標連線為導向之傳送，而狀態之卸載係由支援會期權證於會期恢復期間處理。會期權證係透過使用如 8.5 所述之交握後訊息 NewSessionTicket 提供至 TLS 客戶端。

8.8.4 所支援簽章演算法之標示

8.8.4.1 供交握訊息所支援簽章演算法之標示

RFG 8446 段落 4.2.3 規定〝signature_algorithm〞延伸。其適用於 CertificateVerify 訊息中之簽章。

宣稱符合本標準之實作，應如 RFG 8446 所定義，支援本項延伸。使用 TLSv1.3 之 TLS 客戶端，應包括 signature_algorithm 延伸，至少具備表 5 所表列的規定性演算法。

8.8.4.2 對憑證所支援簽章演算法之標示

RFC 8446 段落 4.2.3 規定〝signature_algorithm_cert〞延伸。其適用於憑證中之簽章。RFC 8446 指出，若客戶端未提供本項延伸，則使用〝signature_algorithm〞延伸中所表列之演算法。由於 signature_algorithm_cert 延伸亦支援 PKCS1 版本，本標準要求本項延伸之支援。

宣稱符合本標準之實作，應支援 RFC 8446 所定義之本項延伸。使用 TLSv1.3 之 TLS 客戶端，應包括 signature_algorithm_cert 延伸，至少具備表 6 所表列的規定性演算法。

8.8.5 所支援群組之標示

RFC 8446 於段落 4.2.7 規定〝supported_groups〞延伸。其係由 TLS 客戶端使用本項延伸，指

示客戶端對金鑰交換支援(對橢圓曲線組及對有限域組)之命名群組。其係按優先權排序。

宣稱符合本標準之實作，應支援 RFC 8446 所定義之本項延伸。使用 TLSv1.3 之 TLS 客戶端應包括 supported_groups 延伸，具備表 4 所表列之規定性及已選定的選項性支援群組。

8.8.6 金鑰共享之標示

RFC 8446 在段落 4.2.8 中規定〝key_share〞延伸。本項延伸傳送金鑰交換之密碼式參數(端點提出之 ECDHE 及 DHE)。此延伸容許支援不同參數集。若提出多個參數集，TLS 伺服器將判定擬使用之最終集合。

key_share 延伸係結構體，包含：

- 已命名群組，其至少應係表 4 中所表列規定性群組之一。
- 對應於所選群組之金鑰交換參數。RFC 8446 描述擬提供給有限域 Diffie-Hellman 群組(RFC 8446，段落 4.2.8.1)以及橢圓曲線 Diffie-Hellman 群組(RFC 8446，段落 4.2.8.)之參數集。

宣稱符合本標準之實作，應支援 RFC 8446 所定義之本項延伸。使用 TLSv1.3 之 TLS 客戶端，應包括 key_share 延伸，並且至少具備表 4 所表列之所選擇的規定性群組。其可表列出多個規定性或選項群組。

8.8.7 透過 Server Name Indication 對所擬定目標 TLS 伺服器之標示

RFC 8446 依賴 RFC 6066 規格上之〝server_name〞延伸。對於 TLSv1.2，本項延伸可由 TLS 客戶端在 ClientHello 訊息中使用。可能使用本項延伸簡化多個(虛擬)TLS 伺服器寄駐在單一網路位址上之情況。標示所擬定目標伺服器名稱，容許伺服器選擇適切之憑證以回傳給客戶端，或處置安全性政策所關切的其他層面。

於缺少應用程式剖繪時，RFC 8446 要求由實作支援本項延伸。

宣稱符合本標準之實作，宜根據 RFC 6066 支援本項延伸。

8.8.8 所支援憑證機構之標示

與 7.5.3 中所概述之 TLSv1.2 針對客戶端 trusted_CA 延伸的描述相比，TLSv1.3 在 RFC 8446 段落 4.2.4 中規定〝certificate_authorities〞延伸。

本項延伸可由任一端點使用來標示所支援之 CA，作為對接收端點的指引。

宣稱符合本標準之實作，宜支援本項延伸。

使用本項延伸之實作，可在 TLS 端點上規定所請求的 CA 所發行之憑證的選擇。

若未能選擇匹配之 CA 頒發之憑證，則應引發安全性事件(〝告警：未找到 TLSv1.3 對等方上所支援匹配之 CA 憑證〞/〝alarm: matching CA certificate supported on TLSv1.3 peer not found〞)。

8.8.9 支援依 PSK 金鑰之協議

RFC 8446 亦支援依 PSK 之金鑰協議，其係對恢復已終止會期或依既存會期建立第二個 TLS 會期有用處。RFC 8446 對 PSK 金鑰協商定義了不同模式。

根據 RFC 8446，若實作支援 PSK 金鑰協商，則必須支援以下 2 延伸事項：

- 〝pre_shared_key〞，用以協商與 PSK 金鑰建立相關聯之給定交握所要使用的預先共享金鑰之身份。
- 〝psk_key_exchange_modes〞，用於標示所要使用之 PSK 模式。此等模式係概述於 8.3.2。

根據 RFC 8446，於提出依 PSK 之金鑰協商時，所有實作必須支援此等延伸事項。宣稱符合本標準之實作，應由上述 2 延伸事項支援依 PSK 之金鑰協商。使用本項延伸之實作事項，應僅提出 RFC 8446 段落 4.2.9 所概述之 psk_dhe_ke 金鑰交換模式，以確保所要協商的會期金鑰之完美前向秘密性(forward secrecy)。

8.8.10 OCSP 回應訊息之裝訂

與 TLSv1.2 相比，RFC 8446 在段落 4.4.2.1 對端點憑證，以及對二端點(TLS 客戶端及 TLS 伺服器)之中間 CA 憑證，定義 OCSP 回應裝訂。此容許二端點皆在 TLS 交握過程中提供所採用之憑證(及其鏈結)的註銷資訊。若某端點不能夠檢索最新註銷訊息，則此機制可能係有用處。

於 TLSv1.3，處置如下：

- 關於 TLS 伺服器憑證之 OCSP 資訊，係在 CertificateEntry 之 status_request 延伸(如 RFC 6066 中所定義)中載送。此延伸必須包含 CertificateStatus 結構。
- 若 TLS 伺服器請求客戶端發送 OCSP 回應資訊，則在其 CertificateRequest 訊息中提供空 status_request 延伸。若客戶端願意(且能)提供本項資訊，則在其回應中包括含 CertificateStatus 結構之 status_request 延伸(如 RFC 6066 中所定義)。
- 宣稱符合本標準之實作應根據 RFC 8446(段落 4.4.2.1)之要求，並依據 RFC 6066 支援本項延伸。

要注意到此處不必要求 OCSP 與 OCSP 回應者互動之支援。

8.8.11 早期資料之標示

RFC 8446 段落 4.2.10 定義早期資料指示，其容許客戶端使用 PSK 在交握訊息中發送已加密資料。由於本標準不容許 0-RTT(亦參閱 8.3.2)，不應由符合本標準之實作使用本項延伸。

TLS 伺服器應忽略接收到之早期資料，直到交握完成。偵測到交握訊息中之早期資料時，應引發安全性事件(〝警告：偵測到交握訊息中遭忽略之早期資料〞/〝warning：Early data in handshake detected but ignored〞)。

9 可選用之安全措施支援

在某些部署中，額外支援係必要，用以進一步限制依其憑證序號及發行者之憑證的使用。本限制事項稱為憑證授權表列或憑證鎖定(certificate pinning)。憑證授權表列可選項性予以支援。若實作支援憑證授權表列，則此表列應採陳述已授權憑證之序號及發行者之方式建置。此作法不限於 TLS 中之憑證使用，係於 CNS 62351-9 在〝憑證授權及驗核(Certificate Authorization and Validation)〞表列(CertAVL，如 ISO/IEC 9594-8:2020 | Rec. ITU-T X.509 (2019)所定義)全景中進一步規定。

10 符合性

10.1 一般

對宣稱遵循本標準之實作，靜態符合性要求事項規定何者應實作、何者可實作以及何者不應實作。

要注意到本節係指節 6 及 7 中對 TLSv1.2，以及節 6 及 8 中對 TLSv1.3 所定義之設定。

10.2 符號

下列符號係用於規定符合性要求事項：

m 規定性支援。此項目應實作。

0 選項性支援。此項目可實作。

c 條件性支援。此項目應按條件規定實作。

x 排除。此項目不應支援。

F/S 功能性標準

10.3 符合所選定之 TLS 版本

表 7 陳述對 TLS 版本之符合性要求事項，其係定義於 6.2。

表 7 – 符合 TLS 版本

TLS 版本	客戶端		伺服器		值/備註
	F/S	已宣告	F/S	已宣告	
1.0 之前	x		x		
1.0	c		c		漏洞已知，僅供向後相容性
1.1	c		c		漏洞已知，僅供向後相容性
1.2	m		m		
1.3	o		o		
c -不同意使用 1.2 之前的 TLS 版本。					

10.4 符合憑證交握

表 8 陳述對憑證處置支援之符合性要求事項，其係定義於節 6。

表 8–符合憑證支援

	客戶端		伺服器		值/備註	參引
	F/S	已宣告	F/S	已宣告		
多重 CA 之支援 (根憑證)	m		m		支援至少 5 筆根 CA 憑證	6.4.1
憑證之支援處置最大長度 8192 位元組的憑證	m		m			6.4.2
遵循依據 RFC 5280(有效期間、CA 簽章、註銷狀態等)之憑證驗核規則	m		m			6.4.4
註銷狀態驗核使用 CRL	o1		o1		評估週期最少每 24 小時	6.4.4.4.2
憑證授權表列依據 CNS 62351-9	o		o		快取週期至多 24 小時	6.4.4.4.3
o1:實作應有能力驗核 OCSP 回應事項。						

10.5 符合 TLSv1.2 特定

10.5.1 符合所選定之密碼套組

表 9 陳述對密碼套組可與 TLSv1.2 一起使用之符合性要求事項，其係定義於 7.2 及 7.3。

表 9–符合 TLSv1.2 可用之密碼套組

密碼套組	客戶端		伺服器		值/備註
	F/S	已宣告	F/S	已宣告	
TLS_NULL_WITH_NULL_NULL	x		x		不容許
TLS_RSA_WITH_NULL_MD5	x		x		不容許
TLS_*_*_MD5	x		x		不容許
TLS_*_DES_*	x		x		
TLS_RSA_WITH_NULL_SHA256	c		c		
TLS_RSA_WITH_AES_128_CBC_SHA256	m		m		
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	m		m		
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	o		o		
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	m		m		
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	o		o		
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	m		m		
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	o		o		
c:若僅期待完整性，可予以支援。此等密碼套組應預設停用，並要求係由組織之安全性政策授權單獨啟用。 不同意使用含 SHA-1 作為雜湊功能之密碼套組，並要求由組織之安全性政策明確授權。					

10.5.2 符合密碼演算法支援

表 10 陳述供加密碼式演算法對憑證及交握支援之符合性要求事項，其係定義於 7.4.3。

表 10–符合密碼演算法支援

簽章及雜湊演算法	客戶端		伺服器		值/備註
	F/S	已宣告	F/S	已宣告	
RSA 2048 之支援	m		m		
RSA 1024 之支援	c		c		不同意
ECDSA 之支援	m		m		
曲線 secp256r1 之支援	m		m		
曲線 secp384r1 之支援	o		o		
曲線 secp521 r1 之支援	o		o		
曲線 brainpoolP256r1 之支援	o		o		
曲線 brainpoolP384r1 之支援	o		o		
曲線 brainpoolP512r1 之支援	o		o		
SHA-256 之支援	m		m		
SHA-1 之支援	c		c		不同意
MD5 之支援	x		x		不容許
c: 不同意。使用係旨在僅供向後相容性，且宜係組織安全策略之授權。					

10.5.3 符合 TLSv1.2 會期管理特徵

表 11 陳述對 TLSv1.2 之符合性要求事項，其係定義於 7.4.4 及 7.4.5。

表 11–符合 TLSv1.2 會期管理特徵

TLSv1.2 特徵	客戶端		伺服器		值/備註
	F/S	已宣告	F/S	已宣告	
TLS 會期恢復	m		m		
TLS 會期恢復發起，使用	m		x		僅指恢復之發起
TLS 會期恢復發起，使用會期權證	o		o		依據 RFC 5077
TLS 會期重新協商	m		m		
TLS 會期重新協商發起，使用	m		x		僅指重新協商之發起
TLSS 會期重新協商發起，使用	x		m		僅指重新協商之發起

10.5.4 符合所選之 TLSv1.2 延伸

表 12 陳述對 TLS 版本之符合性要求事項，其係定義於 7.5。

表 12–符合 TLSv1.2 交握延伸

TLSv1.2 延伸	客戶端		伺服器		值/備註	參引
	F/S	已宣告	F/S	已宣告		
TLS 會期恢復延伸	m		m		依據 RFC 5746	7.5.2
Trusted CA Indication	o		o		依據 RFC 6066	7.5.3
所支援之簽章演算法	m		m		依據 RFC 5246	7.5.4
OCSP 裝訂	m		m		依據 RFC 6066	7.5.5.2
OCSP 多重裝訂	o		o		依據 RFC 6961	7.5.5.3
Server Name Indication	o		o		依據 RFC 6066	7.5.6
encrypt_then_mac	m		m		依據 RFC 7366	7.5.7

10.6 符合 TLSv1.3 特定

10.6.1 符合所選之 TLSv1.3 密碼套組

表 13 陳述對 TLSv1.3 密碼套組之符合性要求，其係定義於 8.2。

表 13–符合 TLSv1.3 密碼套組

密碼套組	客戶端		伺服器		值/備註
	F/S	宣告	F/S	宣告	
TLS_AES_128_GCM_SHA256	m		m		
TLS_AES_256_GCM_SHA384	m		m		
TLS_CHACHA20_POLY1305_ SHA256	o		o		
TLS_AES_128_GCM_SHA256	m		m		
TLS_AES_128_GCM_8_SHA256	o		o		
TLS_SHA256_SHA256	c1		c1		
TLS_SHA384_SHA384	c1		c1		
c1: 若僅期待完整性，可能予以支援。此等密碼套組應預設停用，並要求係由組織之安全性政策授權單獨啟用。					

10.6.2 符合所選之 TLSv1.3 會期管理特徵

本子節陳述對 TLSv1.3 會期管理特徵之符合性要求，其係定義在 8.3、8.4 及 8.6，並在反映在表 14、表 15、表 16、表 17 及表 18。

交握模式係定義在 8.3.2。

表 14–符合 TLSv1.3 之交握模式

TLSv1.3 交握模式	客戶端		伺服器		值/備註
	F/S	已宣告	F/S	已宣告	
psk_ke	x		x		
psk_dheJe	m		m		

TLSv1.3 之早期資料選項的使用，係定義在 8.3.2。

表 15–符合 TLSv1.3 之早期資料特徵(O-RTT)

TLSv1.3 交握模式	客戶端	伺服器	值/備註

	F/S	已宣告	F/S	已宣告	
0-RTT (早期資料)	x		x		

Diffie-Hellman 群組支援係定義在 8.3.3。

表 16–符合在 TLSv1.3 內所支援之 Diffie Hellman 群組

TLSv1.3 所支援之 Diffie Hellman 群組	客戶端		伺服器		值/備註
	F/S	已宣告	F/S	已宣告	
secp256r1	m		m		
Secp384r1	o		o		
brainpoolP256r1	o		o		
brainpoolP384r1	o		o		
brainpoolP512r1	o		o		
ffdhe2048	m		m		
ffdhe3072	o		o		
ffdhe4096	o		o		

簽章演算法支援係定義在 8.3.4。

表 17–符合在 TLSv1.3 內對交握所支援之簽章演算法

TLSv1.3 所支援之簽章演算法	客戶端		伺服器		值/備註
	F/S	已宣告	F/S	已宣告	
rsa_pss_rsae_sha256	m		m		
rsa_pss_rsae_sha384	o		o		
rsa_pss_rsae_sha512	o		o		
rsa_pss_pss_sha256	m		m		
rsa_pss_pss_sha384	o		o		
rsa_pss_pss_sha512	o		o		
ecdsa_secp256r1_sha256	m		m		
ecdsa_secp384r1_sha384	o		o		
ecdsa_brai npoolP256r1_sha256	o		o		
ecdsa_brai npoolP384r1_sha384	o		o		
ecdsa_brai npoolP512r1_sha512	o		o		

對憑證之簽章演算法係定義在 8.3.4.2。

表 18–符合在 TLSv1.3 內對憑證所支援之簽章演算法

TLSv1.3 所支援之簽章演算法	客戶端		伺服器		值/備註
	F/S	已宣告	F/S	已宣告	
rsa_pkcs1_sha256	m		m		
rsa_pkcs1_sha384	o		o		
rsa_pkcs1_sha512	o		o		
rsa_pss_rsae_sha256	m		m		
rsa_pss_rsae_sha384	o		o		
rsa_pss_rsae_sha512	o		o		
rsa_pss_pss_sha256	m		m		
rsa_pss_pss_sha384	o		o		
rsa_pss_pss_sha512	o		o		
ecdsa_secp256r1_sha256	m		m		
ecdsa_secp384r1_sha384	o		o		
ecdsa_brai npoolP256r1_sha256	o		o		
ecdsa_brai npoolP384r1_sha384	o		o		
ecdsa_brai npoolP512r1_sha512	o		o		
註：德國 BSI 建議僅於 2025 年之前使用 RSA（lANA 值 0x0401、0x0501、0x0601），由於已知所使用的 PKCS#1 中的填充物問題。					

10.6.3 符合所選之 TLSv1.3 延伸

表 19 列出了 TLSv1.3 之一致性要求，此等要求在 8.8 中定義。

表 19–符合 TLSv1.3 延伸

TLSv1.3 延伸	客戶端		伺服器		客戶端	伺服器
	F/S	宣告	F/S	宣告		
所支援版本	m		m			8.8.2
訊錄	o		o			8.8.3

TLSv1.3 延伸	客戶端		伺服器		客戶端	伺服器
	F/S	宣告	F/S	宣告		
簽章演算法	m		m			8.8.4.1
簽章演算法憑證	m		m			8.8.4.2
所支援群組	m		m			8.8.5
金鑰共享	m		m			8.8.6
憑證機構	o		o			8.8.8
預先共享金鑰	m		m			8.8.9
psk_key_exchange_modes (PSK 模式)	m		m			8.8.9
Server Name Indication	o		o			8.8.7
status_request (OCSP 裝訂)	m		m			8.8.10
早期資料	x		x			8.8.11

10.6.4 符合所選之 TLSv1.3 交握後訊息

交握後訊息係定義在 8.4，如表 20 所示。

表 20–符合 TLSv1.3 之交握後訊息

TLSv1.3 交握後訊息	客戶端		伺服器		值/備註
	F/S	宣告	F/S	宣告	
KeyUpdate	m		m		
NewSessionTicket	o		o		

附錄 A
(資訊性)
安全性事件

A.1 安全性事件存錄

本附件包含本標準所定義之安全性事件與 IEC 62351-14 間的對照。

關於安全性事件之資訊以及可能包含在 Extranfo 中之細部資訊，僅能由相關實體依底層平台或所用組件之可用性提供。

所有安全性事件之 lEC 版本應為〝1〞。

對安全性事件，係使用以下分群：

- 值〝1〞與 TLS 交握特定安全性事件有關
- 值〝2〞與憑證處置特定安全性事件有關

A.2 TLS 事件與 TLS 交握有關之對照

表 A.1-與本標準所定義之 TLS 交握相關的安全性事件存錄，對應到 IEC 62351-14

安全性事件	本標準子節	助憶符	嚴重性	事件識別符	內文	額外資訊
TLS 交握成功執行\	6.1	TLS_HS_SUCCESS	通知	IEC 62351-3[14?]: 1.1	TLS 會期成功建立	
不安全通訊：所提之 TLS 版本不同意	6.2	TLS_DEPRECATED_VERSION	告警	IEC 62351-3: 1.2	所提之 TLS 版本不同意且停用 TLSv 1.2 以前 TLS 版本之支援	所提之 TLS 版本編號
不安全之 TLS 版本	6.2	TLS_WEAK_VERSION	警告	IEC 62351-3: 1.3	不同意所提之 TLS 版本且停用 TLSv 1.2 以前 TLS 版本之支援	所提之 TLS 版本編號
不安全通訊：所提之 TLS 版本不容許	6.2	TLS_DISALLOWED_VERSION	告警	IEC 62351-3: 1.4	所提之 TLS 版本(早於 TLSv1.0)不容許	所提之 TLS 版本編號
偵測到正進行之通訊所申請之 TLS 版本變更	6.2	TLS_VERSION_CHANGE	告警	IEC 62351-3: 1.5	TLS 版本變更(偵測到正進行之會期可能降級)	所提之 TLS 版本編號
對等方憑證不可用	6.4.3	TLS_NO_PEER_CERT	告警	IEC 62351-3: 1.6	於 TLS 交握期間對等方未提供端點憑證	
端點憑證不可用	6.4.3	TLS_NO_LOCAL_CERT	告警	IEC 62351-3: 1.7	本機端點憑證不可用	
已註銷之憑證造成會期終止	6.4.4.4	TLS_SESSION_CLOSED-REV	告警	IEC 62351-3: 1.8	接收到已註銷之端點憑證造成會期關閉	註銷理由
所提之 TLSv1.2 密碼法套件不容許	7.3	TLS_DISALLOWED_CIPHER	警告	IEC 62351-3: 1.9	所提出之密碼法套件不容許	所提出之密碼法套件
sessionID [session_ID?]逾期，會期不能恢復	7.4.4	TLS SESSIONID EXPIRED_FULL_HS	警告	IEC 62351-3: 1.10	sessionID [session_ID?]逾期，不可能恢復，整個 TLS 完畢	
會期重新協商間隔逾期	7.4.5	TLS_NO_RENEG	告警	IEC 62351-3: 1.11	重新協商間隔已過，TLSv1.2 對等方未重新協商	重新協商時間結束
不支援安全會期重新協商(初始交握)	7.5.2	TLS_NO_RENEG_SIG	警告	IEC 62351-3: 1.12	TLSv1.2：對等方未於重新協商交握標示安全重	

安全性事件	本標準子節	助憶符	嚴重性	事件識別符	內文	額外資訊
					新協商支援(會期權證)	
不支援安全會期重新協商(重新協商之交握)	7.5.2	TLS_NO_RENEG_TICKET	告警	IEC 62351-3: 1.13	TLSv1.2：對等方未於重新協商交握使用安全重新協商(會期權證)能力	
未找到供 TLSv1.2 客戶端所支援匹配之 CA 憑證	7.5.3	TLS_NO_TR_CA_MATCH_S	告警	IEC 62351-3: 1.14	TLSv1.2：未標示客戶端受信賴 CA 之伺服器端支援	受信賴 CA 憑證之 SKID
缺少簽章演算法延伸	7.5.4	TLS_NO-SIG_ALGO_EXT	警告	IEC 62351-3: 1.15	TLSv1.2：未包括簽章演算法延伸。落回至不同意之簽章演算法	
不同意之簽章演算法標示	7.5.4	TLS_DEP SIG_ALGO	警告	IEC 62351-3: 1.16	TLSv1.2：偵測到不同意之簽章演算法組合	所標示之密碼套組
於重新協商密碼套組時未包括加密後 MAC (encrypt-then-MAC [encrypt_then_mac?])延伸	7.5.7	TLS_NO_EPSK_MODE	警告	IEC 62351-3: 1.17	TLSv1.2：未支援加密後 MAC(encrypt-then-MAC[encrypt_then_mac?])延伸	
未提出短暫性 PSK 模式	8.3.2	TLS_NO_ENCRYPT-THEN-MAC	警告	IEC 62351-3: 1.18	TLSv1.3：無僅限短暫性 PSK 模式之支援	
會期金鑰更新間隔已逾期	8.4	TLS_NO_SK_UPDATE	告警	IEC 62351-3: 1.19	TLSv1.3：對應方未進行會期金鑰更新	
TLSv1.3 未找到供對應端匹配 CA 憑證之支援	8.8.8	TLS_NO_TR_CA_MATCH_SC	告警	IEC 62351-3: 1.20	TLSv1.3：未支援對應方所標示之受信賴 CA	受信賴 CA 憑證之 SKID
交握中遭忽略之早期資料	8.8.11	TLS_EARLY-DATA	警告	IEC 62351-3: 1.21	TLSv1.3：偵測到交握訊息中遭忽略之早期資料	

A.3 與憑證處置相關之 TLS 事件的對照

表 A.2 -與本標準所定義之憑證驗核相關的安全性事件存錄，對照至 IEC 62351-14

安全性事件	本標準子節	助憶符	嚴重性	事件識別符	內文	額外資訊
TLS 憑證長度超限	6.4.2	TLS_CERT_SIZE_MISMATCH	告警	IEC 62351-3[14?]: 2.1	端點憑證長度超限	接收到之憑證長度
憑證驗核：CA 憑證不可用	6.4.4.2	TLS_NO_CA_MATCH	告警	IEC 62351-3: 2.2	匹配根 CA 憑證供端點憑證驗核不可用	憑證路徑中所期望之根 CA 資訊
憑證驗核：來自獲獲授權 CA 之受信賴個別憑證不可用	6.4.4.3	TLS_NO_TRUSTED_CERT_MATCH	告警	IEC 62351-3: 2.3	端點憑證不在憑證信賴表列	端點憑證資訊
憑證驗核：已註銷之憑證	6.4.4.4[1?]	TLS_CERT_REVOKED	告警	IEC 62351-3: 2.4	端點憑證已註銷	註銷理由
本機 CRL 不可存取	6.4.4.4.2	TLS_NO_CRL	警告	IEC 62351-3: 2.5	本機 CRL 不可存取	
CRL 逾期	6.4.4.4.2	TLS_CRL_EXP	警告	IEC 62351-3:	CRL 已逾期	CRL 到期資訊

安全性事件	本標準子節	助憶符	嚴重性	事件識別符	內文	額外資訊
				2.6		
OCSP 回應已逾期	6.4.4.4.3	TLS_OCSP_RES_EXP	警告	IEC 62351-3: 2.7	OCSP 回應已逾期	OCSP 到期資訊
OCSP 回應者不可用	6.4.4.4.3	TLS_OCSP_RES_UNAVIL	警告	IEC 62351-3: 2.8	OCSP 回應者	
憑證驗核：已逾期之憑證	6.4.4.5	TLS_CERT_EXP	告警	IEC 62351-3: 2.8	端點憑證已逾期	端點憑證資訊 憑證到期資訊
憑證驗核：不支援之簽章演算法	6.4.4.6	TLS_SIG_ALG_MISMATCH	告警	IEC 62351-3: 2.9	簽章演算法在接收之端點不支援	所提出之簽章演算法
憑證驗核：查證失敗	6.4.4.6	TLS_SIG_V_FAILED	告警	IEC 62351-3: 2.10	憑證簽章不能查證	
RSA 金鑰長度不足	7.4.3	TLS_SHORT_RSA_KEY	告警	IEC 62351-3: 2.11	偵測到 RSA 金鑰長度低於 2048 位元	所提出之 RSA 金鑰長度
金鑰最低長度	7.4.3	TLS_MIN_KEY	警告	IEC 62351-3: 2.12	偵測到具 1024 位元最低金鑰長度且組態容許之 RSA 金鑰	所提出之 RSA 金鑰長度
金鑰長度不足	7.4.3	TLS_SHORT_KEY	告警	IEC 62351-3: 2.13	偵測到金鑰長度不足(低於 1024 位元)之 RSA 金鑰	所提出之 RSA 金鑰長度
使用不同意之雜湊演算法	7.4.3	TLS_DEP_HASH	警告	IEC 62351-3: 2.14	偵測到使用不同意之雜湊演算法	所提出之雜湊演算法

參考資料

[1] CNS???ISO/lEC 15946-2, Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures (withdrawn)

[2] 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

[3] CNS 62351-5，電力系統管理及關聯資訊交換－資料及通訊安全–第 4 部：IEC 60870-5 其衍生協定之安全

[4] CNS 62351-6，電力系統管理及關聯資訊交換－資料及通訊安全–第 6 部：CNS 61850 系列標準之安全

[5] CNS 62351-7，電力系統管理及關聯資訊交換－資料及通訊安全–第 7 部：網路及系統管理(NSM)資料物件模型

[6] CNS 62351-8，電力系統管理及關聯資訊交換－資料及通訊安全–第 8 部：Role-based access control 用於電力系統管理之角色存取控制

[7] lEC 62351 -14, Power systems management and associated information exchange - Data and communications security - Part 14: Cyber Security Events Logs[2]

[8] RFC 4492 :2006 , Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)

[9] RFC 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol- OCSP RFC 7027, Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS)

[10] RFC 8734, Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS) Version 1.3

[11] RFC 8744, Issues and Requirements for Server Name Identification (SNI) Encryption IETF Draft: TLS Encrypted Client Hello (https:lldatatracker.ietf.org/doc/draft-ietf-tls-esni/)

[12] NIST SP-800-57 Part 1 Rev. 5, Recommendations for Key Management, May 2020 (https:!/csrc.nist. gov/publications/detail/sp/800-57 -part-1 /rev-5/final)

[13] NSA Suite B, Suite B Cryptography 1 Cryptographic Interoperability

[14] BSI TR 02102-1 , Cryptographic Mechanisms, February 2022 (https :/lwww.bsi.bund.deIENIPublicationsITechnica/Guidelinesltr02102I tr02102_node.html)

[15] RFC 8996: Deprecating TLSv1.0 and TLSv1.1 (https:/ldatatracker.ietf.orgldoclhtmllrfc89961)

[16] IETF recommendations on TLS cipher suites (https://www. ia na. org/ ass ig n ments/tls-pa ra meters/tis-para meters.xhtm I#tls-para meters-4)

[17] IETF RFG 9155: Deprecating MD5 and SHA-1 signature hashes in TLS 1.2, December 2021 , (https :lldatatracker.ietf.org/doc/html/rfc9155)

名詞對照

- A -	
access control list, ACL	存取控制表列
active session	主動式會期
administrative domain	管理域
advanced encryption standard, AES	進階加密標準
application layer	應用層
assessment	評鑑
association control service element, ACSE	關聯控制服務元件
asymmetric	非對稱式
asymmetric handshake	非對稱式交握
asymmetric operation	非對稱式運作
attack	攻擊
attribute certificate	屬性憑證
audit	稽核
authenticated encryption, AE	鑑別加密
authenticated encryption with associated data, AEAD	以相關聯資料鑑別加密
authentication	鑑別
authorization	授權
automation	自動
availability	可用性；妥善率
- B -	
backward compatibility	向後相容性
best current practice, BCP	最佳現行實務
boundary condition	邊界條件
bump-in-the-wire	線間碰撞
- C -	
carry	載送
certificate	憑證
certificate chain	憑證鏈
certificate pinning	憑證鎖定
certificate revocation	憑證註銷
certificate revocation list, CRL	憑證註銷表列
certification	驗證
certification authority, CA	憑證機構
cipher-block chaining,CBC	加密區塊鏈
cipher suite	密碼套組 client authentication
client	客戶端
client authentication	客戶端鑑別
communication	通訊
communication network	通訊網路
confidentiality	機密性
configuration	組態
conformance	符合性

conformance testing	符合性測試
control protocol	控制協定
credential	信符
cryptographic algorithm	密碼演算法
cryptographic checksum, MAC	密碼式核對合
cryptographic key	密碼金鑰
cryptographic protection	密碼式保護
cryptographic VPN tunnel	密碼式 VPN 通道
cryptography	密碼學
cyber-attack	網宇攻擊
cyber security	網宇安全
- D -	
deployment	部署
Diffie Hellman(ephemeral) key agreement, DH(E)	Diffie-Hellman(暫時性)金鑰協議
digital signature	數位簽章
direct variant	直接變體
distinguished encoding rule, DER	區別編碼規則
- E -	
eavesdropping	竊聽
elliptic curve	橢圓曲線
elliptic curve based Diffie Hellman (ephemeral) key agreement, ECDH(E)	橢圓曲線 Diffie-Hellman(暫時性)金鑰協議
elliptic curve digital signature algorithm, ECDSA	橢圓曲線數位簽章演算法
encryption	加密
end-to-end	端對端
end-to-end authentication	端對端鑑別
error handling	錯誤處置
event log	事件存錄
extension	延伸
- F -	
finite prime field	有限質數體
forward secrecy	前向秘密性
- G -	
Galois/counter mode, GCM	伽羅瓦/計數器模式
group controller	群組控制者
- H -	
handshake	交握
hash	雜湊；雜湊值
hash algorithm	雜湊演算法
hash signature algorithm	雜湊簽章演算法
hash value	雜湊值
hashing	雜湊
hashing algorithm	雜湊演算法
host	寄駐
- I -	

identity	識別資訊;身分
impersonation	冒充
inaccessibility	不可存取性
individual certificate	個別憑證
Information and Communication Technology,ICT	資訊及通訊技術
information exchange	資訊交換
informative	資訊性
integrity	完整性
integrity protection	完整性保護
interoperability	互運性
initialization vector, IV	初始化向量
intrusion detection	入侵偵測
invoke	調用
- K -	
key	金鑰
key derivation function	金鑰衍生函數
key exchange	金鑰交換
- L -	
log	存錄
- M -	
MAC-then-encrypt	先 MAC 再加密
management protocol	管理協定
man-in-the-middle, MitM	中間人
measure	措施
message authentication code, MAC	訊息鑑別碼
mnemonic	助憶符
multiple trust anchor	多信任錨
- N -	
network address	網路位址
network and system management, NSM	網路及系統管理
normative	規定性
- O -	
object	物件；對象
OCSP stapling	OCSP 裝訂
online certificate status protocol, OCSP	線上憑證狀態協定
out-of-band	帶外
- P -	
parameter	參數
peer	對等方
peer support	對等方支援
post-handshake message	交握後訊息
protocol	協定

protocol implementation eXtra information for testing, PIXIT	測試用協定實作額外資訊
pre-master secret	預主秘密
pre-shared key, PSK	預先共享金鑰
private	隱私
private key	私密金鑰
profile	剖繪
public-key	公開金鑰
public-key certificate	公開金鑰憑證
power system	電力系統
power system domain	電力系統域
power system management	電力系統管理
protocol implementation conformance statement, PICS	協定實作符合性陳述

- R -

record layer	紀錄層
rekying	重設金鑰
reliability	可靠性
replay	重演
retrieve	檢索
revocation	註銷
risk assessment	風險評鑑
role-based access control, RBAC	基於角色之存取控制
root CA	根 CA

- S -

scenario	情節
secure sockets layer, SSL	安全資料傳送層
security audit trail	安全稽核存底
security breach	安全漏洞
security event	安全性事件
security measure	安全措施
security policy	安全政策
security threat	安全威脅
server certificate	伺服器憑證
session	會期
session cache	會期快取
session key	會期金鑰
session renegotiation	會期重新協商
session resumption	會期恢復
session ticket	會期權證
sequence number	序號
severity	嚴重性
signaling	標示
signature	簽署
stapling	裝訂
strength	強度

- T -	
tamper	篡改
telecontrol	遠端控制
ticket	權證
ticket-based TLS	權證式 TLS
TLS packet-level encryption	TLS 封包層加密
TLS record layer	TLS 紀錄層
traffic	訊務
transport layer	傳送層
transport layer security, TLS	傳送層安全
threat	威脅
trust anchor	信任錨
- U -	
use case	使用案例
- V -	
validation	驗核
virtual private network, VPN	虛擬私人網路
vulnerability	脆弱性
- W -	

相對應國際標準

IEC 62351-3:2023 Power systems management and associated information exchange - Data and communications security - Part 3: Communication network and system security - Profiles including TCPIIP