

簡介〈歐盟提供合格信任服務者依循標準建議〉



簡介〈歐盟提供合格信任服務者依循標準建議〉

資訊工業策進會科技法律研究所
2021年6月25日

壹、事件摘要

歐盟於2014年通過「歐盟內部市場電子交易之電子身分認證及信賴服務規章」（簡稱eIDAS規章）[1]，並於2016年7月正式生效。eIDAS規章是在歐盟1999年電子簽章指令[2]的基礎上，進一步建構一個更安全、更具信賴、更易於使用電子簽章的法律框架，以促進整個歐盟跨境間的電子交易環境，進而達到歐盟數位單一市場的目標[3]。

eIDAS規章共有六章，其核心包含兩大部分[4]，在第二章中規範了電子識別機制（Electronic Identification），並於第三章中建構一系列電子交易中相關信任服務（Trust Services, TS）的法律架構，包含電子簽章（Electronic signatures）、電子封條（Electronic seals）、電子時戳（Electronic time stamps）、電子註冊傳輸服務（Electronic registered delivery services）、網站認證（Website authentication）。每種信任服務，又可以區分由一般的信任服務提供者（Trust Service Provider, TSP）或由合格信任服務提供者（Qualified Trust Service Provider, QTSP）提供，要成為QTSP必須經各成員國的監督機關授予合格地位後，才能提供該類合格信任服務（Qualified Trust Service, QTS），在eIDAS規章中合格信任服務具有更高的法律效力。譬如，根據eIDAS規章第25條第2項規定，合格電子簽章（qualified electronic signature）與手寫簽章具有同等的法律效力。

歐盟網路安全局（European Union Agency for Cybersecurity, ENISA[5]）於2021年3月發布一份報告，提供合格信任服務者依循標準的建議（Recommendations For QTSPs Based On Standards）[6]，給想要申請成為QTSP的業者參考。

貳、重點說明

承前所述，eIDAS規章的目的是要建構一個促進跨境、跨產業的電子交易的環境，為弭平各會員國對於電子識別服務的落差，報告中指出，必須透過法律框架（Legal framework）、信賴框架（Trust framework）、標準化框架（Standardisation framework）共同達成，以提升歐盟數位單一市場中企業和消費者的信任，並促進信任服務和產品的使用。

（一）法律框架

eIDAS規章中規定了9種QTS的安全要求及其提供者的義務，包括：

1. 電子簽章的合格憑證；
2. 電子封條的合格憑證；
3. 網站認證的合格憑證；
4. 合格電子時戳服務；
5. 合格電子簽章的合格驗證服務；
6. 合格電子封條的合格驗證服務；
7. 合格電子簽章的合格維護服務；
8. 合格電子封條的合格維護服務；
9. 合格電子註冊傳輸服務。

（二）信賴框架

其次，eIDAS規章透過事前（ex ante）和事後（ex post）監督的方式，來確保QTSP及其提供的QTS符合eIDAS規章中的法律要求。欲申請成為QTSP須先經過符合性評估機構（Conformity Assessment Body, CAB）的評估，由其出具評估報告後，再由各成員國的監督機關決定是否授予QTSP資格；取得QTSP資格後會受到不定期稽核，且至少每24個月須再次自費通過CAB評估審核[7]。

(三) 標準化框架

eIDAS規章中對各項TS的安全要求是採取技術中立 (technology-neutral) 的態度，並未限定要採用何種特定技術。換言之，TSP可以透過不同的技術達到eIDAS規章中要求的必要安全程度。事實上，歐盟希望在eIDAS規章所建構的法律框架和信賴框架中，透過產業自律，慢慢形成相關的標準共識。

歐盟從2009年開始，就由歐洲標準化委員會 (European Committee for Standardization, CEN)、歐洲電信標準協會 (European Telecommunications Standards Institute, ETSI) 等歐盟標準化組織協助擬定和更新電子簽章的相關標準，希望可以建立一個更完整的標準化框架，以解決歐盟跨境使用電子簽章遭遇的問題，至今已經建構出一系列電子簽章和相關信任服務的標準，以滿足國際及eIDAS規章的要求，ETSI/CEN與數位簽章有關的標準包含七個面向。

1.介紹性

此類標準主要是關於各類簽章的共通定義、研究、其他關於整體性架構的介紹。

2.簽章的建立與驗證

此類標準主要是關於簽章建立及驗證的政策與安全要求、所要遵循的規則和程序、格式、保護剖繪 (Protection Profiles, PP) [8]。

3.簽章建立和其他相關設備

此類標準主要是與電子簽章產生的設備，以及其他與數位簽章相關服務的設備有關。

4.加密

此類標準主要是與簽章的加密有關，譬如金鑰產生演算法 (key generation algorithms) 和雜湊函數 (hash functions) 等。

5.支持數位簽章及相關服務的TSP

此類標準主要是關於核發合格憑證的QTSP、網站認證憑證的TSP、時戳服務的TSP、提供簽章驗證服務的TSP等。

6.信任應用服務提供者

此類標準主要與應用電子簽章提供加值服務的TSP有關，如電子傳輸服務、資料檔案長期保存服務等。

7.信任服務資格提供者

此類標準主要與eIDAS規章中信任名單 (trusted lists) 相關的程序和格式有關[9]。

其中，在ETSI/CEN關於數位簽章的標準中，主要與QTSP有關的標準如下：

1.電子簽章的合格憑證 (eIDAS規章第28條)

ETSI EN 319 411-2 (且要符合EN 319 401、EN 319 411-1、EN 319 412-2、EN 319 412-5)。

2.電子封條的合格憑證 (eIDAS規章第38條)

ETSI EN 319 411-2 (且要符合EN 319 401、EN 319 411-1、EN 319 412-3、EN 319 412-5)。

3.網站認證的合格憑證 (eIDAS規章第45條)

ETSI EN 319 411-2 (且要符合EN 319 401、EN 319 411-1、EN 319 412-4、EN 319 412-5)。

4.合格電子時戳 (eIDAS規章第42條)

ETSI EN 319 421 (且要符合EN 319 401)、EN 319 422。

5.合格電子簽章的合格驗證服務 (eIDAS規章第33條)

ETSI TS 119 441 (且要符合EN 319 401)、TS 119 442、EN 319 102-1、TS 119 102-2、TS 119 172-4。

6.合格電子封條的合格驗證服務 (eIDAS規章第40條)

ETSI TS 119 441 (且要符合EN 319 401)、TS 119 442、EN 319 102-1、TS 119 102-2、TS 119 172-4。

7.合格電子簽章的合格維護服務 (eIDAS規章第34條)

ETSI EN 319 401、TS 119 511、TS 119 512。

8.合格電子封條的合格維護服務 (eIDAS規章第40條)

ETSI EN 319 401、TS 119 511、TS 119 512。

9.合格電子註冊傳輸服務 (eIDAS規章第44條)

ETSI EN 319 401、EN 319 521、EN 319 522、EN 319 531、EN 319 532。

參、事件評析

從歐盟ENISA的建議可以瞭解，歐盟希望透過介紹歐盟標準化組織所制定的相關電子簽章標準，來引導資通訊廠商申請成為QTSP，提供歐盟企業和使用者更安全、更值得信賴的電子簽章相關服務，以強化使用者的信心，進而促進整個歐盟電子交易的蓬勃發展。

近年來，我國企業也積極投入數位轉型，在邁向數位化的過程通常需要由外部的資通訊廠商協助。然而，由於企業對於資通訊技術不熟悉，因此在選擇資通訊廠商時，往往不知道如何判斷其專業能力，或許企業可以參考上述的介紹，以該廠商是否符合歐盟相關標準的要求，作為選擇資通訊廠商的參考依據，以確保資通訊廠商的能力具有一定水準，這樣對於企業數位轉型及進軍歐盟市場會相當有助益。

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, https://eur-lex.europa.eu/legal-content/ENTXT/?uri=uriserv%3AJOJL_2014.257.01.0073.01.ENG (last visited Jun. 24, 2021).

[2] Directive 1999/93/EC of the European Parliament and of the Council of 13 Dec. 1999 on the a Community Framework for Electronic Signatures, <https://eur-lex.europa.eu/legal-content/ENTXT/?uri=celex%3A31999L0093> (last visited Jun. 24, 2021).

[3] 參前註1，eIDAS前言(3)。

[4] 中文介紹可參考李姿瑩，〈歐盟eIDAS對國內電子簽章和身分認證規範之可能借鏡〉，《科技法律透析》，第31卷第11期，25-32頁，（2019年11月）。

[5] 「歐盟網路安全局」原名為「歐盟網路及資訊安全局」(European Union Agency for Network and Information Security)，2019年更改為現名，但該局的英文縮寫仍維持舊稱ENISA。The European Union Agency for Cybersecurity - A new chapter for ENISA, ENISA, <https://www.enisa.europa.eu/news/enisa-news/the-european-union-agency-for-cybersecurity-a-new-chapter-for-enisa> (last visited Jun. 24, 2021).

[6] European Union Agency for Cybersecurity [ENISA], *Recommendations for Qualified Trust Service Providers based on Standards* (2021), <https://www.enisa.europa.eu/publications/recommendations-for-qtsp-based-on-standards> (last visited Jun. 24, 2021).

[7] 參前註1，eIDAS規章第20條。

[8] 保護剖繪是指申請者依共同準則規章（common criteria, CC）製作之資通安全產品安全基本需求文件，可提供資通安全產品開發者開發產品之依據。〈常見問題/Q02.何謂保護剖繪？〉，國家通訊傳播委員會，<https://ise.ncc.gov.tw/faq>（最後瀏覽日：2021/06/24）。

[9] 參前註1，eIDAS規章第22條第2項、第4項。

相關連結

- [Regulation \(EU\) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC](#)
- [Directive 1999/93/EC of the European Parliament and of the Council of 13 Dec. 1999 on the a Community Framework for Electronic Signatures](#)
- [The European Union Agency for Cybersecurity - A new chapter for ENISA](#)
- [Recommendations for Qualified Trust Service Providers based on Standards](#)
- [常見問題/Q02.何謂保護剖繪？](#)

你可能會想參加

- 製造業及技術服務業個資保護及資安落實－經濟部工業局112年企業個人資料保護暨資訊安全宣導說明會
- 【已額滿】2023科技研發法制推廣活動—科專個資及反詐騙實務講座
- 供應鏈資安國際法制與政策趨勢分享會
- 112年度「領航臺灣數位轉型」國際研討會-實體場
- 112年度「領航臺灣數位轉型」國際研討會-直播場
- 「跨域數位協作與管理」講座活動
- 【實體】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
- 【線上】數位發展部數位經濟相關產業個資安維辦法說明會（南部場）
- 商業服務業個資保護宣導說明會
- 個人資料保護新思維企業法遵論壇
- 【實體】2024科技研發法制推廣活動—科專個資及反詐騙實務講座
- 【直播】2024科技研發法制推廣活動—科專個資及反詐騙實務講座
- 智慧港灣/休憩/育樂面面觀-跨界在地合作新商機
- 中部場-商業服務業個資保護工作坊
- 南部場-商業服務業個資保護工作坊
- 北部場-商業服務業個資保護工作坊
- 數位發展部數位產業署113年資訊服務業者個資安維辦法宣導說明會

謝明均

副法律研究員 編譯整理

上稿時間：2021年06月

文章標籤

推薦文章