TCVN

TIÊU CHUẨN QUỐC GIA

TCVN XXX:2026

Xuất bản lần 1

GIAO DỊCH ĐIỆN TỬ - YÊU CẦU CHUNG VỀ VẬN HÀNH VÀ KIỂM SOÁT ĐỐI VỚI TỔ CHỨC CUNG CẤP DỊCH VỤ GỬI, NHẬN THÔNG ĐIỆP DỮ LIỆU BẢO ĐẢM

Electronic transactions– General Policy Requirements for Qualified Data Message Dispatch and Receipt Service Providers

HÀ NỘI – 2026

Nội dung

Lời giới thiệu

Các tổ chức cung cấp dịch vụ tin cậy đóng vai trò thiết yếu trong việc thiết lập lòng tin giữa các bên tham gia giao dịch điện tử, đặc biệt trên các mạng công cộng mở. Trong đó, dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm là một trong những dịch vụ quan trọng, giúp bảo đảm tính toàn vẹn, tính xác thực, tính không chối bỏ và khả năng cung cấp các bằng chứng về việc truyền tải thông điệp dữ liệu giữa các bên.

Để các bên tham gia thương mại điện tử tin tưởng vào mức độ an toàn và độ tin cậy của dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm, họ cần có niềm tin rằng các tổ chức cung cấp dịch vụ này đã thiết lập và duy trì một hệ thống các thủ tục, quy trình, biện pháp kỹ thuật và tổ chức quản lý chặt chẽ nhằm giảm thiểu các rủi ro về vận hành, an ninh mạng và tài chính liên quan.

Tài liệu này quy định các yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm. Các yêu cầu được xây dựng trên cơ sở các nguyên tắc quản trị, quản lý rủi ro, kiểm soát vận hành và giám sát liên tục, bảo đảm dịch vụ hoạt động đáng tin cậy, minh bạch và tuân thủ các quy định pháp lý liên quan.

Lời nói đầu

TCVN xxx:2026 được xây dựng trên cơ sở tham khảo Tiêu chuẩn quốc tế ETSI EN 319 521 và ETSI EN 319 531 của Viện Tiêu chuẩn Viễn thông Châu Âu (ETSI), có điều chỉnh, sửa đổi, bổ sung để phù hợp với điều kiện của Việt Nam.

TCVN xxx:2026 do Trung tâm Chứng thực điện tử quốc gia biên soạn, Ủy ban Tiêu chuẩn Đo lường Chất lượng Quốc gia thẩm định, Bộ Khoa học và Công nghệ công bố.

Giao dịch điện tử – Yêu cầu chung về vận hành và kiểm soát đối với Tổ chức cung cấp Dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm

Electronic transactions – General Policy Requirements for Qualified Data Message Dispatch and Receipt Service Providers

1 Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu liên quan đến quản lý và vận hành của Tổ chức cung cấp Dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm.

Tiêu chuẩn này không quy định cách thức một bên độc lập có thể đánh giá các yêu cầu đã xác định, bao gồm các yêu cầu về thông tin cần cung cấp cho các bên đánh giá độc lập đó, hoặc các yêu cầu đối với các bên đánh giá đó.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn dưới đây là cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

ETSI EN 319 401: Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers

ETSI EN 319 521: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers

ETSI EN 319 531: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers.

3 Thuật ngữ, định nghĩa và chữ viết tắt

3.1. Thuật ngữ và định nghĩa

3.1.1

Bằng chứng điện tử (electronic evidence)

Dữ liệu được tạo ra trong một quá trình điện tử và được sử dụng để chứng minh một sự kiện hoặc một hoạt động đã xảy ra tại một thời điểm xác định.

3.1.2

Bên gửi (sender)

Cá nhân hoặc tổ chức thực hiện gửi thông điệp dữ liệu thông qua dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm.

3.1.3

Bên nhận (recipient)

Cá nhân hoặc tổ chức được xác định là đối tượng nhận của thông điệp dữ liệu được gửi qua dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm.

3.1.4

Bên tin cậy (relying party)

Cá nhân hoặc tổ chức nhận và dựa vào kết quả của dịch vụ tin cậy (trong trường hợp này là bằng chứng từ dịch vụ gửi, nhận bảo đảm) để đưa ra quyết định.

3.1.5

Dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm (electronic registered delivery service - ERDS)

Dịch vụ cho phép truyền đưa thông điệp dữ liệu giữa các bên bằng phương tiện điện tử, cung cấp bằng chứng về việc xử lý thông điệp dữ liệu, bao gồm bằng chứng về việc gửi và nhận dữ liệu, và bảo vệ dữ liệu được truyền đưa chống lại các rủi ro mất mát, trộm cắp, hư hỏng hoặc thay đổi trái phép.

3.1.6

Dịch vụ thư điện tử bảo đảm (registered electronic mail service - REM)

Một loại hình dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm cụ thể, sử dụng giao thức thư điện tử để truyền đưa dữ liệu và bằng chứng.

3.1.7

Dịch vụ tin cậy (trust service - TS)

Dịch vụ do tổ chức cung cấp dịch vụ tin cậy thực hiện, bao gồm các dịch vụ: Dịch vụ cấp dấu thời gian, Dịch vụ chứng thực thông điệp dữ liệu và Dịch vụ chứng thực chữ ký số công cộng.

3.1.8

Quy chế chứng thực dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm (ERDS practice statement)

Văn bản mô tả cách thức tổ chức cung cấp dịch vụ vận hành dịch vụ của mình nhằm đáp ứng các yêu cầu về chính sách và kỹ thuật.

3.1.9

Thông điệp dữ liệu (data message/data object)

Thông tin được tạo ra, được gửi, được nhận và được lưu trữ bằng phương tiện điện tử.

3.1.10

Thuê bao (subscriber)

Cá nhân hoặc tổ chức ký kết thỏa thuận với tổ chức cung cấp dịch vụ tin cậy để sử dụng dịch vụ.

3.1.11

Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm (ERDS provider - ERDSP)

Tổ chức cung cấp dịch vụ tin cậy thực hiện vận hành dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm.

3.1.12

Phương thức giao tiếp bền vững

Phương tiện hoặc cách thức trao đổi, lưu trữ thông tin cho phép người nhận lưu giữ thông tin một cách lâu dài, truy cập được khi cần thiết và bảo đảm tính toàn vẹn của thông tin theo thời gian, bao gồm nhưng không giới hạn ở văn bản điện tử, thư điện tử, trang thông tin điện tử hoặc các phương tiện điện tử khác có khả năng lưu trữ và tái hiện thông tin mà không bị thay đổi.

3.1.13

Ngữ nghĩa bằng chứng

Cách thức tổ chức, cấu trúc và ý nghĩa của các thành phần thông tin trong bằng chứng điện tử do dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm tạo ra, nhằm bảo đảm rằng bằng chứng đó có thể được hiểu, xác minh và sử dụng một cách thống nhất giữa các bên liên quan.

3.2. Chữ viết tắt

ERDS	Electronic Registered Delivery Service	Dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm
ERDSP	Electronic Registered Delivery Service Provider	Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm
REM	Registered Electronic Mail	Thư điện tử bảo đảm
TS	Trust Service	Dịch vụ tin cậy
TSP	Trust Service Provider	Tổ chức cung cấp dịch vụ tin cậy
UTC	Coordinated Universal Time	Thời gian quốc tế
OID	Object Identifier	Định danh đối tượng

4 Quy định chung về chính sách và quy chế

4.1 Quy chế dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 6 khoản 6.2 Quy chế dịch vụ tin cậy TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải công bố bộ chính sách và quy chế của dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm trên trang thông tin điện tử hoặc phương tiện điện tử khác, trong đó nêu rõ các chính sách và quy chế cần được áp dụng để đáp ứng yêu cầu đối với dịch vụ và tổ chức cung cấp dịch vụ.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm không bắt buộc phải tiết lộ các khía cạnh chứa thông tin nhạy cảm.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải quy định rõ quy trình rà soát, đánh giá dựa theo bộ chính sách và quy chế, bao gồm phân công trách nhiệm duy trì quy chế, thực hiện việc thông báo các thay đổi dự kiến đối với bộ quy chế.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải nêu rõ trong quy chế nghĩa vụ của tất cả các bên tin cậy hỗ trợ cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm, bao gồm các chính sách và quy chế áp dụng đối với các bên tin cậy đó.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải chỉ định rõ phương tiện được sử dụng để báo cáo bất kỳ sửa đổi nào đối với nội dung người dùng trước khi giao hàng hoặc bàn giao.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải mô tả trong quy chế cách thức xác định và xác thực người gửi cũng như người nhận đang sử dụng dịch vụ.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải mô tả các biện pháp bảo đảm an ninh truyền tải, phòng chống các rủi ro như mất mát, trộm cắp, hư hỏng hoặc các thay đổi không được phép đối với dữ liệu.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải nêu rõ nghĩa vụ của người gửi, người nhận và các bên tin cậy tin cậy khác.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải nêu rõ các loại sự kiện liên quan đến quá trình gửi, nhận mà dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm có thể cung cấp bằng chứng.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải mô tả cách thức trích xuất bằng chứng liên quan đến việc xử lý dữ liệu được truyền tải.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải nêu rõ bất kỳ hạn chế nào về thời hạn hiệu lực của các bằng chứng.

4.2 Điều khoản và điều kiện

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 6 khoản 6.2 Điều khoản và điều kiện TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

- Các điều khoản và điều kiện phải xác định được những thành phần trong quá trình chuyển giao nội dung giữa người gửi và người nhận.

- Các điều khoản và điều kiện phải xác định được phương án xử lý khi dữ liệu hết hạn và thời gian dữ liệu được lưu trữ.

- Trước khi ký hợp đồng với khách hàng, tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải thông báo cho khách hàng về các điều khoản và điều kiện liên quan đến dịch vụ.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải thông báo các điều khoản và điều kiện qua phương thức giao tiếp bền vững (bảo đảm tính toàn vẹn theo thời gian).

- Các điều khoản và điều kiện có thể được thông báo qua phương thức điện tử.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải có bằng chứng chứng minh rằng các điều khoản và điều kiện đã được chấp nhận bởi khách hàng.

4.3 Chính sách bảo mật thông tin

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 6 khoản 6.3 Chính sách bảo mật thông tin TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

5 Quy định chung dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm

5.1 Tính toàn vẹn và bảo mật nội dung người dùng

5.1.1 Quy định chung

- Dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải bảo đảm tính sẵn sàng, tính toàn vẹn và tính bảo mật của dữ liệu người dùng trong quá trình cung cấp dịch vụ.

- Bảo mật danh tính người gửi/người nhận phải được bảo đảm, đặc biệt trong quá trình truyền tải dữ liệu giữa người gửi và người nhận.

- Tính toàn vẹn của dữ liệu người dùng và siêu dữ liệu liên quan phải được bảo vệ trong quá trình truyền tải, đặc biệt trong quá trình truyền tải dữ liệu giữa người gửi và người nhận.

- Nếu nội dung người dùng cần được sửa đổi trong quá trình cung cấp dịch vụ, các thay đổi phải được thông báo rõ ràng cho người gửi, người nhận và các bên tin cậy có liên quan.

5.2 Xác định và xác thực người dùng

5.2.1 Xác minh danh tính lần đầu của người dùng

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải trực tiếp xác minh danh tính của người gửi và người nhận hoặc xác minh thông qua bên tin cậy:

a) bằng sự hiện diện vật lý của cá nhân hoặc của đại diện được ủy quyền; hoặc

b) từ xa, sử dụng phương tiện xác thực điện tử; hoặc

c) bằng chứng thư được cấp cho cá nhân hoặc cho đại diện được ủy quyền; hoặc

d) bằng cách sử dụng các phương pháp xác minh khác được công nhận và bảo đảm tương đương về độ tin cậy với sự hiện diện vật lý. Sự tương đương của mức bảo đảm phải được xác nhận bởi tổ chức đánh giá sự phù hợp.

- Bên tin cậy xác minh danh tính của người gửi và người nhận có thể là một tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm khác, trong trường hợp người gửi hoặc người nhận đăng ký sử dụng hai tổ chức cung cấp dịch vụ khác nhau.

- Nếu sau xác minh danh tính ban đầu, tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm chưa liên kết phương tiện xác thực với người gửi hoặc người nhận, xác minh danh tính phải được thực hiện mỗi lần dữ liệu người dùng được gửi hoặc truyền tải.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải bàn giao dữ liệu từ người gửi tới người nhận chỉ sau khi xác minh thành công người nhận.

- Nếu xác minh người nhận dựa trên chữ ký số, xác thực chữ ký số phải thực hiện trước khi bàn giao dữ liệu.

- Nếu xác minh người nhận dựa trên quy trình nội bộ của dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm, tổ chức cung cấp dịch vụ cần thực hiện toàn bộ quy trình trong môi trường an toàn và kiểm soát.

- Nếu xác minh người nhận dựa trên quy trình nội bộ của dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm, tất cả bằng chứng về việc đã xác minh và quy trình truyền tải phải được thu thập và bảo vệ.

5.2.2 Xác thực trong dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải xác thực danh tính người gửi theo quy chế trước truyền tải dữ liệu.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải xác thực danh tính người nhận theo quy chế trước khi truyền tải dữ liệu từ người gửi đến người nhận. Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm có thể cung cấp phương thức xác minh cho người gửi, người nhận hoặc cả hai để sử dụng trong quy trình xác minh.

- Khi tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm liên kết phương thức xác minh danh tính người dùng đã được xác minh theo khoản 5.2.1, tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải sử dụng một trong các phương tiện sau:

a) Cơ chế xác thực đa yếu tố (tương đương mức Substantial IA theo IA 1502/2015, LoA3 theo ISO 29115, AAL2 theo NIST SP 800-63B hoặc mức tương đương); hoặc

b) Xác thực TLS lẫn nhau, bao gồm chứng thư cấp theo ETSI EN 319 411-1; hoặc

c) Chữ ký số được hỗ trợ bởi chứng thư cấp theo ETSI EN 319 411-1; hoặc

d) Phương tiện xác thực có mức an ninh tương đương với các phương tiện trên.

- Nếu người gửi hoặc người nhận kết nối với dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm theo một kết nối an toàn yêu cầu xác thực dựa trên chứng thư theo ETSI EN 319 411-1, thì sau khi thiết lập kết nối an toàn, tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm có thể áp dụng cơ chế xác thực một yếu tố cho giai đoạn thứ hai nếu quy trình tổ chức và biện pháp an ninh bảo đảm tin cậy vào quy trình xác thực người gửi hoặc người nhận.

- Nếu tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm không cung cấp phương tiện xác thực cho người dùng, tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm hợp chuẩn phải xác minh danh tính người gửi mỗi lần nộp nội dung người dùng và xác minh danh tính người nhận trước khi bàn giao nội dung người dùng.

5.3 Tham chiếu thời gian

5.3.1 Quy định chung

- Tham chiếu thời gian phải phù hợp với các quy định tại khoản 4.2 Điều khoản và Điều kiện.

5.3.2 Quy định đối với tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm

- Ngày và giờ gửi, nhận và bất kỳ thay đổi nào của dữ liệu người dùng phải được xác nhận bởi dấu thời gian.

- Bằng chứng gửi và nhận phải được liên kết với dữ liệu người dùng và đóng dấu thời gian.

- Trong trường hợp tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm thuê tổ chức cung cấp dịch vụ dấu thời gian như một bên tin cậy, tổ chức cung cấp dịch vụ chứng thực thông điệp dữ phải kiểm tra định kỳ rằng nhà cung cấp dịch vụ dấu thời gian vẫn hợp chuẩn.

- Tình trạng hợp chuẩn của dịch vụ dấu thời gian có thể được kiểm tra bằng cách kiểm tra danh sách tin cậy nơi dịch vụ đã đề cập nên được liệt kê là dịch vụ hợp chuẩn. Tổ chức cung cấp dịch vụ cấp dấu thời gian có nghĩa vụ thông báo cho khách hàng (ở đây là tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm) về bất kỳ thay đổi nào trong tình trạng hợp chuẩn.

5.4 Sự kiện và bằng chứng

5.4.1 Quy định chung

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải cung cấp bằng chứng về việc gửi và nhận dữ liệu (hoặc cả hai) cho người gửi.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải tạo bằng chứng về việc gửi dữ liệu bởi người gửi.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải lưu trữ tối thiểu các thông tin sau:

a) Dữ liệu xác minh người dùng;

b) Dữ liệu xác thực người dùng;

c) Bằng chứng về việc danh tính người gửi đã được xác minh;

d) Nhật ký vận hành dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm, xác minh danh tính của người gửi và người nhận, và truyền tải dữ liệu;

e) Bằng chứng về việc xác minh danh tính của người nhận trước khi truyền tải dữ liệu;

f) Phương thức để chứng minh rằng nội dung dữ liệu chưa bị sửa đổi trong quá trình truyền tải;

g) một bản tham chiếu hoặc tóm tắt nội dung đầy đủ do người dùng gửi;

h) Dấu thời gian tương ứng với ngày và giờ gửi, nhận, truyền tải và sửa đổi nội dung dữ liệu bởi người dùng (nếu phù hợp).

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải bảo đảm bảo mật, tính toàn vẹn và tính sẵn có của các nhật ký được quy định tại khoản này.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải lưu trữ tất cả bằng chứng liên quan trong thời gian phù hợp với quy định của pháp luật tính từ ngày gửi.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm có thể tạo và cung cấp cho các bên liên quan có thẩm quyền bằng chứng về các sự kiện trong quá trình cung cấp dịch vụ.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải lưu trữ bằng chứng và/hoặc bản tóm tắt bằng chứng cho mỗi bằng chứng mà tổ chức đã ban hành.

- Bằng chứng của dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm được tạo bởi tổ chức cung cấp dịch vụ cần tuân thủ ngữ nghĩa bằng chứng.

5.4.2 Quy định đối với tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm

- Tất cả sự kiện liên quan đến việc xác và xác thực minh danh tính người gửi phải được ghi nhật ký.

- Tất cả sự kiện liên quan đến việc xác minh danh tính người nhận và/hoặc xác thực thêm phải được ghi nhật ký.

- Nếu thông tin xác minh danh tính được cung cấp, các thông tin xác minh danh tính phải được lưu lại. Các thông tin xác minh danh tính có thể bao gồm loại tài liệu được trình bày bởi người nộp đơn để hỗ trợ xác định; bất kỳ hồ sơ nào tham chiếu đến dữ liệu xác định duy nhất; hoặc bản sao của đơn và tài liệu xác định, bao gồm hợp đồng người gửi đã ký.

5.5 Tương tác

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải xác minh rằng dịch vụ mà tổ chức tương tác cũng phải là một tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải xác thực bất kỳ tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm khác trước khi truyền tải hoặc chấp nhận dữ liệu.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải xác minh rằng các giao tiếp truyền tải được bảo vệ để bảo đảm tính toàn vẹn và bảo mật của nội dung dữ liệu truyền tải.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm không được chuyển tiếp dữ liệu cho một tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm khác, trừ khi có thể xác nhận rằng tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm kia tuân thủ các ràng buộc và tùy chọn được xác định trong chính sách hiện hành.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải cung cấp bằng chứng về các sự kiện về việc gửi, nhận và chuyển giao nội dung giữa người gửi và người nhận thành công hoặc không thành công.

- Nếu tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm hỗ trợ việc nhận dữ liệu được chuyển tiếp từ một tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm khác, tổ chức đó phải cung cấp bằng chứng về các sự kiện chấp nhận hoặc từ chối chuyển tiếp.

- Nếu tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm hỗ trợ việc nhận dữ liệu được chuyển tiếp từ một tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm khác, tổ chức đó phải cung cấp bằng chứng tương ứng về việc người nhận đã nhận được dữ liệu chuyển tiếp.

6 Đánh giá Rủi ro

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 5 Đánh giá rủi ro TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

7 Quản lý và vận hành tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm

7.1 Tổ chức nội bộ

7.1.1 Độ tin cậy tổ chức

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 7 khoản 7.1.1 Độ tin cậy tổ chức TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

7.1.2 Phân tách nhiệm vụ

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 7 khoản 7.1.2 Phân tách nhiệm vụ TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

7.2 Nguồn nhân lực

7.2.1 Quy định chung

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 7 khoản 7.2 Nguồn nhân lực TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

7.2.2 Quy định đối với tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải bổ nhiệm một cá nhân thực hiện việc xác minh danh tính.

- Cá nhân thực hiện việc xác minh danh tính phải chịu trách nhiệm bảo đảm rằng các quy trình thực tế được thực hiện để xác minh danh tính của người gửi và người nhận tuân thủ quy trình xác minh danh tính ban đầu được chỉ định.

7.3 Quản lý tài sản

7.3.1 Yêu cầu chung

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 7 khoản 7.3.1 Yêu cầu chung (Quản lý tài sản) TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

7.3.2 Xử lý phương tiện

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 7 khoản 7.3.3 Xử lý phương tiện lưu trữ (Quản lý tài sản) TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

7.4 Kiểm soát truy cập

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 7 khoản 7.4 Biện pháp kiểm soát truy cập TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

7.5 Kiểm soát mật mã

Các yêu cầu sau chỉ áp dụng khi tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm tạo chứng thư và/hoặc tạo khóa bí mật và/hoặc tạo chữ ký số:

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 7 khoản 7.5 Biện pháp kiểm soát mật mã TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

- Khóa ký của tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải được giữ cách ly vật lý khỏi hoạt động bình thường theo cách mà chỉ cá nhân đáng tin cậy được chỉ định mới có quyền truy cập vào khóa để sử dụng trong việc ký nội dung dữ liệu và/hoặc bằng chứng.

- Khóa bí mật của tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải được lưu trữ và sử dụng trong thiết bị mật mã an toàn.

- Khóa bí mật của tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải được bảo đảm mức độ bảo vệ tương đương như được cung cấp bởi thiết bị mật mã an toàn.

- Khóa bí mật của tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải được sao lưu, lưu trữ và phục hồi chỉ bởi cá nhân đáng tin cậy được chỉ định có thể sử dụng, tối thiểu kiểm soát kép trong môi trường an toàn vật lý. Số lượng cá nhân đáng tin cậy được chỉ định có thể thực hiện chức năng này phải được giữ ở mức tối thiểu và phù hợp với các thực hành tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm.

- Bản sao của khóa bí mật của tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải được bảo đảm kiểm soát an ninh ở cùng mức độ hoặc cao hơn so với khóa bí mật đang sử dụng.

- Khóa bí mật của tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm và bất kỳ bản sao nào được lưu trữ trong thiết bị mật mã an toàn chuyên dụng phải được kiểm soát truy cập để bảo đảm rằng khóa không thể bị truy cập từ bên ngoài thiết bị này.

- Thiết bị mật mã an toàn không được can thiệp trong quá trình vận chuyển và lưu trữ.

- Khóa bí mật của tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm được lưu trữ trên thiết bị mật mã an toàn của tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải bị hủy khi thiết bị dừng hoạt động.

7.6 An ninh vật lý và môi trường

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 7 khoản 7.6 An ninh vật lý và môi trường TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

- Chính sách an ninh vật lý và môi trường của tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm cho các hệ thống liên quan đến việc cung cấp dịch vụ phải bảo đảm kiểm soát truy cập vật lý, bảo vệ thiên tai, yếu tố an toàn phòng chống cháy nổ, tình huống mất kết nối tiện ích hỗ trợ (ví dụ: điện, viễn thông), sụp đổ cấu trúc, rò rỉ ống nước, bảo vệ chống trộm cắp, đột nhập và phục hồi thảm họa.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải thực hiện biện pháp kiểm soát bảo đảm thiết bị, thông tin, phương tiện và phần mềm liên quan đến việc cung cấp dịch vụ không thể bị mang ra khỏi địa điểm mà không được ủy quyền.

- Kiểm soát an ninh vật lý và môi trường phải được thực hiện để bảo vệ cơ sở hệ thống tài nguyên và các cơ sở được sử dụng để hỗ trợ hoạt động cung cấp dịch vụ.

- Bất kỳ thành phần nào của cơ sở được chia sẻ với các tổ chức cung cấp dịch vụ khác phải nằm ngoài hệ thống.

- Mọi truy cập logic phải được ghi nhật ký.

- Mọi truy cập vào khu vực an toàn vật lý phải chịu sự giám sát và được ghi nhật ký an toàn.

- Người không được ủy quyền phải được giám sát bởi người được ủy quyền trong truy cập khu vực an toàn.

7.7 An toàn vận hành

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 7 khoản 7.7 An toàn vận hành TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

7.8 An toàn thông tin

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 7 khoản 7.8 An toàn thông tin TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải giám sát nhu cầu công suất.

- Dự báo nhu cầu công suất tương lai phải bảo đảm rằng khả năng xử lý và lưu trữ đầy đủ có thể được bảo đảm.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải sử dụng các giao thức và thuật toán hiện đại cho mã hóa ở tầng vận chuyển.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải sử dụng chứng thư xác thực trang web cho tầng vận chuyển nếu dữ liệu được gửi bên ngoài mạng nội bộ.

7.9 Quản lý sự cố

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 7 khoản 7.9 Quản lý sự cố TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

7.10 Thu thập bằng chứng

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 7 khoản 7.10 Thu thập bằng chứng TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải ghi nhật ký các sự kiện liên quan đến việc gửi, nhận và truyền tải dữ liệu.

- Tất cả sự kiện an ninh phải được ghi nhật ký, bao gồm các thay đổi liên quan đến chính sách an ninh, khởi động và tắt hệ thống, sụp đổ hệ thống và lỗi phần cứng, hoạt động tường lửa và bộ định tuyến và các nỗ lực truy cập hệ thống PKI.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải xác định thời gian lưu giữ cho các nhật ký được chỉ định trong điều khoản này theo pháp luật hiện hành; thời gian lưu giữ phải bảo đảm không ít hơn 02 năm.

7.11 Kế hoạch duy trì hoạt động

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 7 khoản 7.11 Kế hoạch duy trì hoạt động TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

- Hệ thống dữ liệu của tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm cần thiết để liên tục hoạt động cung cấp dịch vụ phải được sao lưu và lưu trữ ở nơi an toàn phù hợp để cho phép tổ chức cung cấp dịch vụ quay lại hoạt động kịp thời trong trường hợp sự cố/thảm họa.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải sao lưu định kỳ các bản sao của thông tin thiết yếu và các phần mềm.

- Các cơ sở phục hồi dữ liệu phải được cung cấp để bảo đảm rằng tất cả thông tin thiết yếu và phần mềm có thể được phục hồi sau thảm họa hoặc lỗi phương tiện.

- Các thiết kế để phục hồi sau thảm họa phải được kiểm tra định kỳ để bảo đảm đáp ứng yêu cầu của kế hoạch duy trì hoạt động.

- Nếu phân tích rủi ro xác định rằng thông tin yêu cầu kiểm soát kép phục vụ quản lý thì kiểm soát kép phải được áp dụng để phục hồi.

- Kế hoạch duy trì hoạt động của tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải giải quyết sự ảnh hưởng, mất mát hoặc nghi ngờ của khóa bí mật của tổ chức cung cấp dịch vụ như một thảm họa và các quy trình được lập kế hoạch phải được đặt ra.

- Sau thảm họa, tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải thực hiện các bước để tránh lặp lại thảm họa.

- Trong trường hợp có sự ảnh hưởng tới tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm, tổ chức cung cấp dịch vụ phải thông báo cho tất cả khách hàng, các bên liên quan mà tổ chức cung cấp dịch vụ có hợp đồng hoặc hình thức quan hệ khác trong quá trình cung cấp dịch vụ. Thông tin được cung cấp phải chỉ ra rằng thông tin bằng chứng được cung cấp sử dụng khóa bị ảnh hưởng sẽ không còn hợp lệ từ thời điểm sự ảnh hưởng được xác định.

- Nếu bất kỳ thuật toán nào, hoặc tham số liên quan, được sử dụng bởi tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm trở nên không còn đủ hoặc phù hợp cho mục đích sử dụng thì tổ chức cung cấp dịch vụ phải:

a) thông báo cho tất cả khách hàng và bên liên quan mà tổ chức cung cấp dịch vụ có hợp đồng hoặc hình thức quan hệ khác; và

b) bảo mật tài liệu bằng chứng hiện có bằng dấu thời gian mới.

7.12 Chấm dứt dịch vụ

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 7 khoản 7.12 Chấm dứt dịch vụ TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải giữ bằng chứng đã thu thập trong thời gian phù hợp theo pháp luật hiện hành.

7.13 Tuân thủ pháp luật

- Tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm phải đáp ứng các yêu cầu tại Mục 7 khoản 7.13 Tuân thủ pháp luật TCVN 14618:2026: Công nghệ thông tin – Dịch vụ tin cậy – Yêu cầu chung về vận hành và kiểm soát đối với tổ chức cung cấp dịch vụ tin cậy.

- Trong trường hợp khả thi, tổ chức cung cấp dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm và sản phẩm phải được làm cho phù hợp đối với người khuyết tật.