

QUY CHẾ CHỨNG THỰC
DỊCH VỤ CHỨNG THỰC THÔNG ĐIỆN DỮ LIỆU

MỤC LỤC

BẢNG GHI NHẬN THAY ĐỔI.....	Error! Bookmark not defined.
MỤC LỤC	1
THÔNG TIN CHUNG	4
1. PHẠM VI ÁP DỤNG.....	5
2. TÀI LIỆU THAM CHIẾU	5
2.1. Tài liệu tham chiếu mang tính tiêu chuẩn.....	5
2.2. Tài liệu tham chiếu mang tính tham khảo.....	5
3. THUẬT NGỮ, CHỮ VIẾT TẮT VÀ KÝ HIỆU	7
3.1. Thuật ngữ.....	7
3.2. Chữ viết tắt	9
3.3. Ký hiệu	10
4. CÁC KHÁI NIỆM CHUNG	10
4.1. Các khái niệm về yêu cầu chính sách chung	10
4.2. Dịch vụ chứng thực thông điệp dữ liệu	11
4.3. Tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu	11
4.4. Thuê bao	12
4.5. Chính sách chứng thực thông điệp dữ liệu và quy chế chứng thực của tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu	12
5. QUY ĐỊNH VÀ CÁC YÊU CẦU CHUNG VỀ DỊCH VỤ CHỨNG THỰC THÔNG ĐIỆP DỮ LIỆU	13
5.1. Tính toàn vẹn và bảo mật nội dung của thuê bao	13
5.1.1. Các quy định chung	13
5.1.2. Quy định đối với tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu	13
5.2. Định danh và xác thực thuê bao.....	14
5.2.1. Quy định về xác minh danh tính ban đầu đối với tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu	14
5.2.2. Quy định về xác thực đối với tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu.....	16
5.3. Tham chiếu thời gian	17
5.3.1. Các quy định chung	17

Quy chế chứng thực thông điệp dữ liệu

5.3.2. Quy định đối với tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu.....	17
5.4. Sự kiện và bằng chứng.....	17
5.4.1. Các quy định chung	17
5.4.2. Quy định đối với tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu.....	19
5.5. Khả năng liên thông.....	20
6. CHÍNH SÁCH VÀ THỰC THI.....	20
6.1. Đánh giá rủi ro	20
6.2. Quy chế chứng thực của tổ chức cung cấp dịch vụ tin cậy.....	20
6.3. Điều khoản và điều kiện áp dụng	20
6.4. Chính sách an toàn thông tin	21
6.5. Nghĩa vụ của tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu	21
6.5.1. Tổng quan	21
6.5.2. Nghĩa vụ của tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu đối với thuê bao.....	21
6.6. Thông tin dành cho bên tin tưởng.....	21
7. QUẢN LÝ VÀ VẬN HÀNH TỔ CHỨC CUNG CẤP DỊCH VỤ CHỨNG THỰC THÔNG ĐIỆP DỮ LIỆU	22
7.1. Tổ chức nội bộ	22
7.1.1. Độ tin cậy của tổ chức	22
7.1.2. Phân tách công việc.....	23
7.2. Quản lý nhân sự	23
7.2.1. Các quy định chung	23
7.2.2. Quy định đối với tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu.....	23
7.3. Quản lý tài sản	24
7.3.1. Yêu cầu chung.....	24
7.3.2. Xử lý phương tiện lưu trữ	24
7.4. Kiểm soát truy cập	25
7.5. Kiểm soát mật mã	25
7.6. An ninh vật lý và môi trường.....	25
7.7. An ninh vận hành.....	26
7.8. An ninh mạng	26
7.9. Quản lý sự cố.....	26

Quy chế chứng thực thông điệp dữ liệu

7.10. Thu thập bằng chứng cho các dịch vụ nội bộ của tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu	27
7.11. Quản lý tính liên tục trong hoạt động kinh doanh	28
7.11.1. Quy trình duy trì và phục hồi hoạt động dịch vụ.....	28
7.11.2. Quy trình sao lưu và kiểm tra khả năng phục hồi	29
7.11.3. Quy trình xử lý trường hợp khóa mật mã của hệ thống bị mất, lộ hoặc nghi ngờ lộ	30
7.11.4. Quy trình duy trì giá trị kiểm chứng lâu dài của bằng chứng điện tử.....	31
7.11.4.1. Quy trình giám sát nhu cầu gia hạn	31
7.11.4.2. Quy trình gia hạn dấu thời gian.....	32
7.11.4.3. Quy trình gia hạn thuật toán	33
7.11.5. Nguồn nhân lực và phân công trách nhiệm.....	34
7.12. Chấm dứt hoạt động của tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu và kế hoạch chấm dứt.....	35
7.13. Tuân thủ quy định.....	35

THÔNG TIN CHUNG

Viettel-CA là tên gọi dịch vụ Chứng thực thông điệp dữ liệu do Tập đoàn Công nghiệp – Viễn thông Quân đội cung cấp.

Quy chế chứng thực của Viettel-CA được xây dựng tuân thủ quy định của - Luật Giao dịch điện tử số 20/2023/QH15 ngày 22 tháng 6 năm 2023, Nghị định số 23/2025/NĐ-CP ngày 21 tháng 02 năm 2025 của Chính phủ quy định về chữ ký điện tử và dịch vụ tin cậy và các quy định pháp luật liên quan.

Tài liệu này mô tả các chính sách, quy trình và thông lệ được áp dụng trong việc triển khai, vận hành và quản lý dịch vụ chứng thực thông điệp dữ liệu. Nội dung tài liệu bao gồm các quy định liên quan đến việc cung cấp các nhóm dịch vụ chính sau:

- Dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm (Electronic Registered Delivery Service – ERDS);
- Dịch vụ gửi, nhận thư điện tử (Registered Electronic Mail Service – REMS);
- Dịch vụ lưu trữ và xác nhận tính toàn vẹn của thông điệp dữ liệu (Long-Term Archiving Service – LTAS).

Để bảo đảm giá trị chứng minh của thông điệp dữ liệu trong môi trường điện tử, Viettel triển khai hạ tầng kỹ thuật và các cơ chế bảo mật nhằm tạo lập và quản lý bằng chứng điện tử trong suốt vòng đời giao dịch. Các cơ chế kỹ thuật được áp dụng bao gồm việc sử dụng hàm băm mật mã, dấu thời gian điện tử và các kỹ thuật bảo đảm tính toàn vẹn dữ liệu nhằm:

- Ghi nhận chính xác thời điểm xảy ra các sự kiện liên quan đến thông điệp dữ liệu (gửi, nhận, truy cập hoặc lưu trữ);
- Tạo lập và quản lý các bằng chứng điện tử chứng minh việc gửi và nhận thông điệp dữ liệu;
- Hình thành và duy trì hồ sơ bằng chứng điện tử liên quan đến giao dịch;
- Lưu trữ và gia hạn giá trị kiểm chứng của dữ liệu trong suốt thời gian lưu trữ đối với dịch vụ bảo quản dữ liệu dài hạn.

Viettel công bố bản quy chế chứng thực nhằm tuân thủ theo các yêu cầu về pháp lý và tiêu chuẩn/yêu cầu của Bộ Khoa học và Công nghệ.

1. PHẠM VI ÁP DỤNG

Văn bản này là một bộ quy chế chứng thực (Certificate Practices Statement – CPS) tuyên bố về mặt nguyên tắc các chính sách quản trị của Viettel trong quá trình cung cấp dịch vụ chứng thực thông điệp dữ liệu. Bản CPS này quy định các yêu cầu pháp lý, yêu cầu kỹ thuật và yêu cầu nghiệp vụ liên quan đến việc gửi nhận thông điệp, tạo lập và lưu trữ bằng chứng lâu dài.

Các yêu cầu trong CPS có nhiệm vụ bảo đảm tính bảo mật và toàn vẹn cho dịch vụ Viettel, và được áp dụng bắt buộc đối với tất cả các thành phần tham gia sử dụng dịch vụ chứng thực thông điệp Viettel.

Bản CPS này không phải là thỏa thuận về mặt pháp lý giữa Viettel với thuê bao cũng như các thành phần khác tham gia dịch vụ Viettel.

Mục tiêu của văn bản này là:

- Viettel với tư cách là nhà cung cấp dịch vụ chứng thực thông điệp dữ liệu hoạt động trên cơ sở Quy chế chứng thực và tuân thủ theo các yêu cầu trong CPS này;
- Cung cấp thông tin cho bên tin tưởng về mức độ bảo đảm của bằng chứng chứng thực được Viettel tạo lập và duy trì.

CPS này tuân theo luật pháp Việt Nam cũng như các chính sách, quy chế liên quan đến dịch vụ chứng thực thông điệp dữ liệu được ban hành Bộ Khoa học và Công nghệ cũng như các cơ quan nhà nước có thẩm quyền liên quan.

Tài liệu được xây dựng theo cấu trúc tham chiếu RFC 3647, đồng thời điều chỉnh thuật ngữ và nội dung phù hợp với mô hình Viettel Qualified Electronic Registered e-Delivery.

2. TÀI LIỆU THAM CHIẾU

2.1. Tài liệu tham chiếu mang tính tiêu chuẩn

- Luật Giao dịch điện tử số 20/2023/QH15 ngày 22 tháng 6 năm 2023;
- Nghị định 23/2025/NĐ-CP ngày 21/02/2025 của Chính phủ về việc Quy định về chữ ký điện tử và Dịch vụ tin cậy;
- Thông tư 53/2025/TT-BKHCN ngày 31/12/2025 của Bộ Khoa học và Công nghệ về việc Ban hành “Quy chuẩn kỹ thuật quốc gia về yêu cầu đối với dịch vụ chứng thực thông điệp dữ liệu”;
- Thông tư số 16/2025/TT-BKHCN ngày 20/8/2025 của Bộ Khoa học và Công nghệ quy định về Quy chế chứng thực mẫu của tổ chức cung cấp dịch vụ tin cậy đối với dịch vụ chứng thực thông điệp dữ liệu.

2.2. Tài liệu tham chiếu mang tính tham khảo

- [1] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
- [2] ETSI EN 319 102-1: "Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation"
- [3] ISO 29115: "Information technology -- Security techniques - Entity authentication assurance framework"
- [4] NIST SP 800-63B: "Digital Identity Guidelines Authentication and Lifecycle Management"
- [5] ETSI EN 319 521: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers"
- [6] ETSI EN 319 532-3: "Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REMS) Services; Part 3: Formats"
- [7] IETF RFC 2045: "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies"
- [8] IETF RFC 5322: "Internet Message Format"
- [9] ETSI EN 319 531: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers"
- [10] ETSI TS 119 511: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques"
- [11] ISO/IEC 15408 (parts 1 to 3): "Information technology -- Security techniques -- Evaluation criteria for IT security"
- [12] ISO/IEC 19790: "Information technology -- Security techniques -- Security requirements for cryptographic modules"
- [13] FIPS PUB 140-2: "Security Requirements for Cryptographic Modules"
- [14] FIPS PUB 140-3: "Security Requirements for Cryptographic Modules"
- [15] ETSI TR 119 001: "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations"
- [16] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites"
- [17] ETSI TS 119 122-3: "Electronic Signatures and Infrastructures (ESI); CAdES"

digital signatures; Part 3: Incorporation of Evidence Record Syntax (ERS) mechanisms in CAdES"

- [18] ETSI EN 319 162-1: "Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); Part 1: Building blocks and ASiC Baseline containers"
- [19] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements"
- [20] ETSI TS 119 512: "Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services"
- [21] ISO/IEC 21320-1 (2015): "Information technology - Document Container File -- Part 1: Core"
- [22] ISO 14641-1:2018: "Electronic archiving -- Part 1: Specifications concerning the design and the operation of an information system for electronic information preservation"
- [23] ISO 14721:2012: "Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model"
- [24] ISO 16363:2011: "Space data and information transfer systems -- Audit and certification of trustworthy digital repositories"
- [25] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)"
- [26] IETF RFC 3986: "Uniform Resource Identifier (URI): Generic Syntax"
- [27] IETF RFC 4998: "Evidence Record Syntax (ERS)"
- [28] IETF RFC 5280 (2008): "Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
- [29] IETF RFC 5816 (2010): "ESSCertIDv2 Update for RFC 3161"
- [30] IETF RFC 6283 (2011): "Extensible Markup Language Evidence Record Syntax (XMLERS)"
- [31] IETF RFC 6960 (2013): "Online Certificate Status Protocol - OCSP"

3. THUẬT NGỮ, CHỮ VIẾT TẮT VÀ KÝ HIỆU

3.1. Thuật ngữ

TT	Thuật ngữ	Giải thích
----	-----------	------------

Quy chế chứng thực thông điệp dữ liệu

1.	Dịch vụ chứng thực thông điệp dữ liệu	Dịch vụ do tổ chức cung cấp dịch vụ tin cậy thực hiện nhằm chứng minh việc gửi, nhận, thời điểm gửi, nhận, tính toàn vẹn và nguồn gốc của thông điệp dữ liệu giữa người gửi và người nhận.
2.	Thông điệp dữ liệu	Thông tin được tạo ra, gửi đi, nhận hoặc lưu trữ bằng phương tiện điện tử.
3.	Dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm	Dịch vụ chứng thực thông điệp dữ liệu cung cấp bằng chứng về việc gửi, việc nhận, thời điểm gửi, thời điểm nhận và danh tính của người gửi, người nhận.
4.	Dịch vụ gửi, nhận thư điện tử	Dịch vụ chứng thực thông điệp dữ liệu chuyên biệt dành cho thư điện tử, cung cấp bằng chứng về việc gửi, việc nhận và tính toàn vẹn của thư điện tử cùng các phần đính kèm.
5.	Dịch vụ lưu trữ và xác nhận tính toàn vẹn của thông điệp dữ liệu	Dịch vụ lưu trữ và bảo quản dữ liệu điện tử trong thời gian dài nhằm duy trì khả năng kiểm chứng tính toàn vẹn và giá trị pháp lý của dữ liệu theo thời gian.
6.	Dấu thời gian	<i>Dấu thời gian</i> là dữ liệu điện tử gắn với thông điệp dữ liệu cho phép xác định thời gian của thông điệp dữ liệu đó tồn tại ở một thời điểm cụ thể.
7.	Bằng chứng điện tử	Tập hợp dữ liệu điện tử do hệ thống dịch vụ tạo lập nhằm chứng minh sự kiện xảy ra trong quá trình giao dịch như gửi, nhận hoặc truy cập thông điệp dữ liệu.
8	Gói bằng chứng	Tập hợp có cấu trúc của các dữ liệu và bằng chứng điện tử được hệ thống dịch vụ chứng thực thông điệp dữ liệu tạo lập hoặc thu thập trong quá trình xử lý một giao dịch liên quan đến thông điệp dữ liệu.
9.	Bên gửi	Cá nhân hoặc tổ chức thực hiện việc gửi thông điệp dữ liệu thông qua dịch vụ.
10.	Bên nhận	Cá nhân hoặc tổ chức nhận thông điệp dữ liệu được gửi thông qua dịch vụ.
11	Mã bảo đảm toàn vẹn thông điệp dữ liệu	Hay còn gọi là giá trị băm (hash), Một dãy ký tự được sử dụng để kiểm tra được tính toàn vẹn của thông điệp dữ liệu.
12	Bản ghi bằng chứng (evidence record)	Đơn vị dữ liệu có thể được sử dụng để chứng minh sự tồn tại của một đối tượng dữ liệu được bảo quản hoặc một nhóm đối tượng dữ liệu được bảo quản tại một thời điểm xác định.
13	Dấu thời gian lưu trữ	Dấu thời gian được tạo để bảo vệ tính toàn vẹn và chứng minh sự tồn tại của dữ liệu hoặc bằng chứng điện tử tại một thời điểm xác định trong quá trình lưu trữ lâu dài.
14	Chuỗi dấu thời gian lưu trữ	Tập hợp các dấu thời gian lưu trữ được tạo nối tiếp nhau, trong đó dấu thời gian mới bảo vệ dấu thời gian trước đó nhằm duy trì khả năng kiểm chứng của bằng chứng theo thời gian.

Quy chế chứng thực thông điệp dữ liệu

15	Dãy dấu thời gian lưu trữ	Tập hợp một hoặc nhiều chuỗi dấu thời gian lưu trữ; chuỗi mới được bổ sung khi cần chuyển sang thuật toán băm mới để tiếp tục duy trì khả năng kiểm chứng lâu dài của bằng chứng.
----	---------------------------	---

3.2. Chữ viết tắt

TT	Thuật ngữ	Diễn giải	Giải thích
1.	CA	Certification Authority	Tổ chức chứng thực
2.	ERDS	Electronic Registered Delivery Service	Dịch vụ gửi nhận thông điệp dữ liệu bảo đảm
3.	REMS	Registered Electronic Mail Service	Dịch vụ gửi nhận thư điện tử
4.	LTAS	Long Term Archiving Service	Dịch vụ lưu trữ và xác nhận tính toàn vẹn của thông điệp dữ liệu
5.	CP	Certificate Policy	Chính sách chứng thư
6.	CPS	Certification Practice statement	Quy chế chứng thực
7.	CRL	Certificate Revocation List	Danh sách chứng thư bị thu hồi
8.	DN	Distinguished Name	Tên phân biệt (trong định danh X.509)
9.	ETSI	European Telecommunications Standards Institute	Viện Tiêu chuẩn Viễn thông Châu Âu
10.	FIPS	Federal Information Processing Standards	Bộ tiêu chuẩn xử lý thông tin liên bang Hoa Kỳ
11.	HSM	Hardware Security Module	Thiết bị bảo mật phần cứng (thiết bị lưu và xử lý khóa bí mật)
12.	ISO/IEC	International Organization for Standardization / International Electrotechnical Commission	Tổ chức Tiêu chuẩn hóa Quốc tế / Ủy ban Kỹ thuật điện quốc tế
13.	OCSP	Online Certificate Status Protocol	Giao thức kiểm tra trạng thái chứng thư trực tuyến
14.	PKCS	Public-Key Cryptography Standards	Bộ tiêu chuẩn mật mã khóa công khai
15.	PKI	Public Key Infrastructure	Hạ tầng khóa công khai
16.	RA	Registration Authority	Tổ chức đăng ký
17.	RFC	Request for Comments	Tài liệu tiêu chuẩn kỹ thuật do IETF ban hành
18.	RSA	Rivest-Shamir-Adleman	Thuật toán mật mã khóa công khai
19.	SHA	Secure Hash Algorithm	Thuật toán băm an toàn

Quy chế chứng thực thông điệp dữ liệu

TT	Thuật ngữ	Diễn giải	Giải thích
20.	TSP	Trust Service Provider	Tổ chức cung cấp dịch vụ tin cậy
21.	UTC	Coordinated Universal Time	Giờ Phối hợp Quốc tế
22.	DC	Digital Certificate	Chứng thư số
23.	RootCA	RootCA - Trung tâm chứng thực điện tử quốc gia - Bộ Khoa học và Công nghệ.	RootCA - Trung tâm chứng thực điện tử quốc gia - Bộ Khoa học và Công nghệ.
24.	PKI	Public Key Infrastructure	Hạ tầng khoá công khai
25.	CMND	Số chứng minh của khách hàng cá nhân	Số chứng minh của khách hàng cá nhân
26.	MST	Mã số thuế của khách hàng doanh nghiệp	Mã số thuế của khách hàng doanh nghiệp
27.	CSDL	Cơ sở dữ liệu	Cơ sở dữ liệu
28.	IP	Internet Protocol	Internet Protocol
29.	IPS	Intrusion Prevention System	Hệ thống ngăn chặn xâm nhập bất hợp pháp.
30.	ATS	Archive Time-Stamp	Dấu thời gian lưu trữ
31.	ATSC	Archive Time-Stamp Chain	Chuỗi dấu thời gian lưu trữ
32.	ATSS	Archive Time-Stamp Sequence	Dãy dấu thời gian lưu trữ

3.3. Ký hiệu

Không sử dụng.

4. CÁC KHÁI NIỆM CHUNG

4.1. Các khái niệm về yêu cầu chính sách chung

Tài liệu này được xây dựng trên cơ sở tham chiếu các yêu cầu chính sách chung quy định trong tiêu chuẩn ETSI EN 319 401 – Electronic Signatures and Infrastructures (ESI): General Policy Requirements for Trust Service Providers. Tiêu chuẩn này quy định các yêu cầu chung áp dụng cho các nhà cung cấp dịch vụ tin cậy (Trust Service Provider – TSP), bao gồm nhưng không giới hạn ở dịch vụ cấp dấu thời gian, dịch vụ lưu trữ điện tử lâu dài, dịch vụ chứng thực thông điệp dữ liệu và dịch vụ chứng thực chữ ký điện tử.

Trong phạm vi tài liệu này, các yêu cầu chính sách được áp dụng để mô tả cách thức Viettel triển khai các biện pháp quản lý, vận hành và kỹ thuật nhằm cung cấp dịch vụ chứng thực thông điệp dữ liệu, bao gồm việc tiếp nhận, xử lý, xác thực và lưu trữ các bằng chứng điện tử liên quan đến thông điệp dữ liệu được chứng thực.

Khách hàng, thuê bao sử dụng dịch vụ và các bên phụ thuộc cần tham khảo tài liệu Quy chế thực hành dịch vụ chứng thực thông điệp dữ liệu này để biết thêm các thông tin chi tiết về cách thức Viettel triển khai các chính sách, quy trình và cơ chế kỹ thuật liên

quan đến việc cung cấp dịch vụ chứng thực thông điệp dữ liệu, bao gồm các giao thức, phương thức vận hành và các kiểm soát an toàn được áp dụng trong hệ thống.

4.2. Dịch vụ chứng thực thông điệp dữ liệu

Dịch vụ chứng thực thông điệp dữ liệu là dịch vụ tin cậy nhằm tạo lập, xác nhận và lưu giữ các bằng chứng điện tử liên quan đến việc gửi, nhận và lưu trữ thông điệp dữ liệu trong môi trường điện tử.

Thông qua việc áp dụng các cơ chế kỹ thuật, bao gồm các phương pháp mật mã và hệ thống quản lý bằng chứng điện tử, dịch vụ chứng thực thông điệp dữ liệu cho phép xác minh các thông tin liên quan đến thông điệp dữ liệu như: nguồn gốc, danh tính các bên tham gia, thời điểm phát sinh, quá trình truyền nhận và tính toàn vẹn của nội dung thông điệp dữ liệu. Các bằng chứng được tạo lập từ dịch vụ chứng thực thông điệp dữ liệu có thể được sử dụng để đối chiếu, kiểm tra và làm căn cứ chứng minh trong các giao dịch điện tử hoặc khi phát sinh tranh chấp.

Theo Thông tư 53/2025/TT-BKHCN, dịch vụ chứng thực thông điệp dữ liệu bao gồm các loại dịch vụ sau:

- **Dịch vụ gửi, nhận thông điệp dữ liệu bảo đảm:** Là dịch vụ cung cấp cơ chế trung gian tin cậy trong quá trình gửi và nhận thông điệp dữ liệu giữa các bên tham gia giao dịch điện tử. Dịch vụ thực hiện xác thực các bên tham gia, bảo đảm tính toàn vẹn của thông điệp dữ liệu trong quá trình truyền nhận, ghi nhận chính xác thời điểm xảy ra các sự kiện (gửi, nhận, truy cập) và tạo lập, lưu trữ các bằng chứng điện tử tương ứng. Các bằng chứng này cho phép chứng minh việc gửi và nhận thông điệp dữ liệu, đồng thời bảo đảm tính chống chối bỏ của các bên liên quan.
- **Dịch vụ gửi, nhận thư điện tử:** Là dịch vụ cung cấp cơ chế bảo đảm cho việc gửi và nhận thư điện tử thông qua việc ghi nhận và chứng thực các sự kiện phát sinh trong quá trình trao đổi thư điện tử, bao gồm thời điểm gửi, thời điểm nhận và tính toàn vẹn của thông điệp dữ liệu. Dịch vụ tạo lập và lưu trữ các bằng chứng điện tử về quá trình gửi – nhận thư điện tử nhằm phục vụ việc chứng minh sự kiện giao dịch điện tử. Dịch vụ này không bao gồm việc chứng thực danh tính pháp lý của người gửi hoặc người nhận thư điện tử.
- **Dịch vụ lưu trữ và xác nhận tính toàn vẹn của thông điệp dữ liệu:** Là dịch vụ cung cấp cơ chế lưu trữ và bảo quản dữ liệu điện tử trong thời gian dài, bảo đảm duy trì khả năng chứng minh tính toàn vẹn, tính xác thực, thời điểm và giá trị pháp lý của dữ liệu theo thời gian. Dịch vụ thực hiện gia hạn và củng cố các bằng chứng mật mã như dấu thời gian, chữ ký điện tử hoặc các bằng chứng chứng thực khác nhằm bảo đảm dữ liệu vẫn có giá trị pháp lý ngay cả khi các thuật toán mật mã, chứng thư số hoặc hạ tầng kỹ thuật ban đầu bị suy yếu hoặc không còn tin cậy.

4.3. Tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu

Tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu là thành phần quan trọng nhất trong hệ thống dịch vụ chứng thực thông điệp dữ liệu, chịu trách nhiệm vận hành toàn bộ hạ tầng kỹ thuật và quy trình nghiệp vụ nhằm đảm bảo:

- Tiếp nhận và xử lý yêu cầu sử dụng các dịch vụ ERDS, REMS và LTAS;
- Vận hành hệ thống dịch vụ nhằm bảo đảm tính toàn vẹn, tính bảo mật và tính sẵn sàng của thông điệp dữ liệu và các bằng chứng điện tử;
- Tạo lập và quản lý các bằng chứng điện tử liên quan đến việc gửi, nhận hoặc lưu trữ thông điệp dữ liệu;
- Lưu trữ và duy trì khả năng kiểm chứng của các bằng chứng điện tử trong suốt thời gian cung cấp dịch vụ;
- Duy trì cơ sở dữ liệu bằng chứng điện tử và cung cấp các chức năng tra cứu, xác minh khi cần thiết.
- Tạm ngừng, thay đổi hoặc chấm dứt việc cung cấp dịch vụ theo quy định của pháp luật và theo thỏa thuận với khách hàng.

Viettel-CA là tổ chức cung cấp dịch vụ chứng thực thông điệp do Tập đoàn Công nghiệp-Viễn thông Quân đội xây dựng. Đồng thời đây là đơn vị được tổ chức theo quy định của pháp luật Việt Nam, trực thuộc RootCA (Trung tâm Chứng thực điện tử Quốc gia) do Bộ Khoa học và Công nghệ quản lý, được phép cung cấp trực tiếp cho người dùng cuối trong mạng tin cậy này.

4.4. Thuê bao

Thuê bao là tổ chức, cá nhân (đủ điều kiện theo quy định của pháp luật và Quy chế chứng thực này) đăng ký sử dụng dịch vụ chứng thực thông điệp dữ liệu do Viettel cung cấp, tham gia với vai trò người gửi, người nhận hoặc các bên liên quan trong giao dịch điện tử và được hệ thống ghi nhận, xác thực thông tin phục vụ việc tạo lập và quản lý bằng chứng điện tử.

4.5. Chính sách chứng thực thông điệp dữ liệu và quy chế chứng thực của tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu

Viettel xây dựng và ban hành Chính sách chứng thực thông điệp dữ liệu và Quy chế chứng thực làm cơ sở quy định các nguyên tắc, yêu cầu và thông lệ áp dụng trong việc cung cấp, vận hành và quản lý dịch vụ chứng thực thông điệp dữ liệu. Chính sách và Quy chế chứng thực được xây dựng phù hợp với các quy định pháp luật hiện hành, các tiêu chuẩn kỹ thuật áp dụng đối với dịch vụ tin cậy và các yêu cầu liên quan đến hoạt động của tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu.

Viettel công bố công khai Chính sách chứng thực thông điệp dữ liệu, Quy chế chứng thực và các điều khoản, điều kiện sử dụng dịch vụ trên trang thông tin điện tử của Viettel-

CA tại địa chỉ: <http://Viettel-CA.vn/download>, để các bên liên quan có thể tiếp cận, tra cứu miễn phí và thuận tiện. Các phiên bản đã sửa đổi, cập nhật được công bố kèm theo số hiệu phiên bản, ngày hiệu lực và tóm tắt nội dung thay đổi; các phiên bản trước đó được lưu trữ để phục vụ tra cứu, đối chiếu khi cần thiết.

5. QUY ĐỊNH VÀ CÁC YÊU CẦU CHUNG VỀ DỊCH VỤ CHỨNG THỰC THÔNG ĐIỆP DỮ LIỆU

5.1. Tính toàn vẹn và bảo mật nội dung của thuê bao

5.1.1. Các quy định chung

Viettel bảo đảm rằng tính sẵn sàng, tính toàn vẹn và tính bảo mật của nội dung thông điệp dữ liệu được duy trì trong suốt thời gian hệ thống xử lý và quản lý thông điệp dữ liệu, từ thời điểm tiếp nhận yêu cầu gửi thông điệp dữ liệu cho đến khi thông điệp được chuyển giao cho bên nhận hoặc được lưu trữ theo chính sách của dịch vụ.

Trong quá trình cung cấp dịch vụ và truyền thông, danh tính của bên gửi/nhận thông điệp dữ liệu được bảo vệ nghiêm ngặt bằng các cơ chế kiểm soát truy cập và bảo mật, đảm bảo chỉ sử dụng cho mục đích cung cấp dịch vụ. Tổ chức chứng thực và các bên tham gia phải tuân thủ nghiêm ngặt các quy định pháp luật liên quan đến bảo vệ dữ liệu cá nhân và quyền riêng tư của người dùng không giới hạn ở Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân và các văn bản pháp luật có liên quan.

Viettel áp dụng các cơ chế kỹ thuật nhằm bảo đảm tính toàn vẹn của nội dung thông điệp dữ liệu và các siêu dữ liệu liên quan trong suốt quá trình truyền nhận và lưu trữ. Các biện pháp này bao gồm việc sử dụng các thuật toán băm mật mã, cơ chế ký số, dấu thời gian điện tử hoặc các cơ chế bảo vệ dữ liệu tương đương nhằm ngăn ngừa việc thay đổi, thất thoát nội dung dữ liệu mà không thể phát hiện.

Trong trường hợp phát hiện sự cố hoặc dấu hiệu vi phạm liên quan đến tính toàn vẹn hoặc bảo mật của thông điệp dữ liệu, Viettel phải thông báo cho các bên liên quan trong thời gian sớm nhất. Sự cố phải được ghi nhận đầy đủ trong hệ thống nhật ký kiểm toán (audit log), đồng thời tiến hành điều tra nguyên nhân, thực hiện các biện pháp khắc phục và ngăn ngừa tái diễn.

5.1.2. Quy định đối với tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu

Viettel với tư cách là tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu có trách nhiệm triển khai và vận hành các biện pháp kỹ thuật và tổ chức nhằm đảm bảo tính toàn vẹn, bảo mật.

Đối với việc đảm bảo tính toàn vẹn, hệ thống Viettel hoạt động theo nguyên tắc chuyển tiếp thông điệp nguyên vẹn. Viettel không thực hiện bất kỳ thao tác biến đổi nào đối với nội dung thông điệp dữ liệu của người dùng trong suốt quá trình xử lý. Ngay tại thời điểm tiếp nhận, hệ thống tính toán giá trị băm (hash) của thông điệp và ghi nhận vào

bằng chứng điện tử kèm dấu thời gian. Toàn bộ bằng chứng điện tử sau khi tạo lập được ký số bởi khóa bí mật của hệ thống ERDS lưu giữ trong thiết bị HSM, bảo đảm phát hiện ngay bất kỳ sự thay đổi nào đối với dữ liệu bằng chứng kể từ thời điểm ký.

Về tính bảo mật, toàn bộ kênh truyền tải giữa hệ thống và người dùng bên ngoài được mã hóa bằng TLS phiên bản 1.2 trở lên. Kênh truyền nội bộ giữa các thành phần của hệ thống cũng được mã hóa và kiểm soát chặt chẽ thông qua hệ thống tường lửa nhiều lớp, bảo đảm các thành phần ở vùng bảo mật thấp hơn không thể truy cập trực tiếp vào dữ liệu ở vùng bảo mật cao hơn. Nhân viên vận hành của Viettel không có quyền truy cập nội dung thông điệp dữ liệu của người dùng. Mọi thao tác truy cập vào hệ thống đều được kiểm soát theo nguyên tắc phân quyền tối thiểu và ghi nhận đầy đủ vào hệ thống log tập trung.

Ngoài ra, Viettel xây dựng và thực hiện chính sách quản lý vòng đời dữ liệu rõ ràng đối với các thông điệp dữ liệu.

Các thông điệp tạm thời chưa hoàn tất quá trình xử lý được lưu trữ trong một khoảng thời gian nhất định, cụ thể là 7 ngày, sau đó sẽ được xóa nếu không có hoạt động tiếp theo.

Đối với các thông điệp đã hoàn tất giao dịch, dữ liệu được lưu trữ trong thời hạn phù hợp với đặc thù của từng ngành, lĩnh vực theo quy định của pháp luật hiện hành hoặc theo thỏa thuận giữa Viettel và khách hàng.

Sau khi hết thời hạn lưu trữ, dữ liệu có thể được xóa theo yêu cầu của người dùng hoặc theo chính sách quản lý dữ liệu của Viettel. Việc xóa dữ liệu phải được thực hiện bằng các phương pháp xóa an toàn nhằm đảm bảo dữ liệu không thể được phục hồi bằng các phương pháp kỹ thuật thông thường.

5.2. Định danh và xác thực thuê bao

5.2.1. Quy định về xác minh danh tính ban đầu đối với tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu

5.2.1.1. Các quy định chung

Viettel thực hiện xác minh danh tính của thuê bao trước khi cấp phát tài khoản sử dụng dịch vụ chứng thực thông điệp dữ liệu thông qua quy trình đăng ký trực tiếp tại các điểm giao dịch. Việc xác minh danh tính được thực hiện theo phương thức hiện diện vật lý, bảo đảm độ tin cậy cao và tuân thủ quy định pháp luật hiện hành. Cụ thể, khách hàng thực hiện đăng ký dịch vụ trực tiếp tại các chi nhánh Viettel hoặc đơn vị được ủy quyền. Nhân viên giao dịch tiếp nhận hồ sơ, kiểm tra, đối chiếu thông tin định danh của khách hàng với giấy tờ gốc hợp lệ. Kết quả xác minh và các tài liệu liên quan được lưu trữ phục vụ công tác kiểm tra, đối soát và chứng minh khi cần thiết.

Hiện tại, Viettel áp dụng phương thức xác minh danh tính trực tiếp đối với hai nhóm đối tượng:

a) Tổ chức

Thông tin xác minh tối thiểu bao gồm tên tổ chức, địa chỉ trụ sở, quốc gia, tỉnh/thành phố và các thông tin pháp lý liên quan đến tổ chức. Việc xác minh phải đảm bảo rằng tổ chức có hiện diện hợp pháp tại địa điểm được khai báo và thông tin đăng ký là chính xác.

Để thực hiện việc xác minh, Viettel cần yêu cầu các tài liệu và văn bản chứng minh gồm có:

- Quyết định thành lập tổ chức (đối với các tổ chức được thành lập theo quyết định của cơ quan có thẩm quyền);
- Điều lệ tổ chức và hoạt động;
- Giấy chứng nhận đăng ký doanh nghiệp hoặc giấy tờ pháp lý tương đương;
- Thông tin về người đại diện theo pháp luật hoặc người đại diện hợp pháp của tổ chức;
- Thông tin về người được ủy quyền sử dụng dịch vụ;
- Các thông tin liên quan đến hệ thống hoặc dịch vụ điện tử của tổ chức (nếu cần thiết cho mục đích cung cấp dịch vụ).

Trong quá trình đăng ký dịch vụ, cơ chế ủy quyền giữa người đại diện pháp luật của tổ chức và cá nhân khác chỉ được chấp nhận khi có đầy đủ hồ sơ chứng minh hợp lệ và được tổ chức cung cấp dịch vụ kiểm tra, xác minh theo quy trình nội bộ.

Toàn bộ quá trình xác minh danh tính của tổ chức phải được ghi nhận và lưu trữ dưới dạng hồ sơ điện tử theo quy trình cung cấp dịch vụ của hệ thống Viettel.

b) Cá nhân

Đối với cá nhân đăng ký sử dụng dịch vụ chứng thực thông điệp dữ liệu, danh tính của cá nhân phải được xác minh bởi tổ chức cung cấp dịch vụ. Thông tin định danh của cá nhân có thể bao gồm:

- Họ và tên;
- Địa chỉ;
- Số giấy tờ tùy thân hợp lệ (Căn cước công dân, hộ chiếu hoặc giấy tờ tương đương);
- Thông tin liên hệ như địa chỉ thư điện tử hoặc số điện thoại;
- Các thông tin bổ sung cần thiết cho việc cung cấp dịch vụ.

Trong giai đoạn hiện tại, Viettel áp dụng phương thức xác minh danh tính trực tiếp đối với thuê bao đăng ký sử dụng dịch vụ chứng thực thông điệp dữ liệu. Tuy nhiên, trong quá trình mở rộng phương thức cung cấp dịch vụ, Viettel sẽ nghiên cứu và triển khai bổ sung các hình thức đăng ký, xác minh danh tính trên môi trường điện tử, phù hợp với quy định pháp luật và điều kiện kỹ thuật của hệ thống. Các phương thức này có thể bao gồm

việc khách hàng tự thực hiện đăng ký dịch vụ trên hệ thống Viettel và xác minh danh tính thông qua các nền tảng định danh điện tử được pháp luật Việt Nam công nhận, như VNeID. Việc áp dụng các phương thức xác minh mới sẽ được Viettel đánh giá về mức độ đảm bảo, yêu cầu an toàn thông tin và cập nhật vào quy trình cung cấp dịch vụ trước khi chính thức triển khai.

5.2.1.2. Định danh người nhận và bàn giao nội dung người dùng

Cơ chế xác định danh tính người nhận và điều kiện bàn giao thông điệp được áp dụng khác nhau giữa dịch vụ ERDS và dịch vụ REMS.

a) Đối với dịch vụ ERDS

Hệ thống chỉ bàn giao thông điệp dữ liệu đến người nhận sau khi xác định thành công danh tính người nhận. Người nhận trong hệ thống ERDS là thuê bao đã hoàn thành quy trình đăng ký và được cấp tài khoản dịch vụ với thông tin xác thực ràng buộc danh tính. Hệ thống ERDS Core thực hiện xác thực người nhận bằng chữ ký số khi thực hiện bàn giao.

Toàn bộ bằng chứng về quá trình xác định danh tính và bàn giao được thu thập và bảo vệ trong gói bằng chứng của giao dịch, bao gồm kết quả xác thực danh tính các bên, phương thức xác thực đã áp dụng, dấu thời gian tại từng sự kiện và mã định danh phiên xác thực. Bằng chứng điện tử sau khi tạo lập được ký số bởi hệ thống ERDS và lưu trữ trong môi trường kiểm soát chặt chẽ.

b) Đối với dịch vụ REMS

Dịch vụ REMS vận hành theo giao thức SMTP theo mô hình chuyển tiếp thư điện tử và đối tượng được xác minh là mail server đích của người nhận.

Cụ thể, hệ thống REMS ghi nhận và chứng minh rằng thông điệp đã được chuyển tiếp thành công đến mail server của người nhận và mail server đó đã xác nhận tiếp nhận. Sự kiện này được ghi nhận dưới dạng Proof of Relay kèm dấu thời gian chính xác. Đây là mức độ bằng chứng tối đa mà giao thức SMTP cho phép thu thập, bởi sau thời điểm mail server đích tiếp nhận, hành trình của thông điệp trong hệ thống nội bộ của người nhận nằm ngoài phạm vi kiểm soát của hệ thống REMS.

Do đó, bằng chứng điện tử trong dịch vụ REMS chứng minh được hai sự kiện: thông điệp đã được gửi bởi người gửi tại thời điểm xác định, và mail server của người nhận đã tiếp nhận thông điệp tại thời điểm xác định. Dịch vụ REMS không cam kết và không tạo lập bằng chứng về việc cá nhân người nhận đã đọc hoặc truy cập thông điệp.

5.2.2. Quy định về xác thực đối với tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu

Viettel triển khai các cơ chế xác thực nhằm đảm bảo rằng người gửi và người nhận thông điệp dữ liệu được xác thực trước khi thực hiện các hành động liên quan đến dịch vụ

chứng thực thông điệp dữ liệu.

Cơ chế xác thực được ràng buộc với tài khoản thuê bao đã được xác minh danh tính ban đầu theo Mục 5.2.1. Các phương tiện xác thực này có thể bao gồm:

- Cơ chế xác thực đa yếu tố (Multi-Factor Authentication);
- Cơ chế xác thực TLS hai chiều sử dụng chứng thư số được cấp theo chính sách chứng thư phù hợp;
- Cơ chế xác thực dựa trên chữ ký số với chứng thư số hợp lệ;
- Các phương thức xác thực khác có mức độ an toàn tương đương.

5.3. Tham chiếu thời gian

5.3.1. Các quy định chung

Toàn bộ dấu thời gian được sử dụng trong hệ thống Viettel tuân theo định nghĩa thời gian quy định trong Điều khoản và Điều kiện dịch vụ. Hệ thống sử dụng nguồn thời gian đồng bộ với Viện Đo lường Quốc gia Việt Nam làm chuẩn tham chiếu.

5.3.2. Quy định đối với tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu

Viettel phải đảm bảo rằng các sự kiện quan trọng trong quá trình cung cấp dịch vụ, bao gồm thời điểm gửi thông điệp, thời điểm nhận thông điệp và các thay đổi liên quan đến nội dung thông điệp, đều được ghi nhận kèm theo thông tin thời gian chính xác. Thông tin thời gian này có thể được gắn với thông điệp dữ liệu hoặc các bằng chứng giao dịch thông qua các cơ chế dấu thời gian điện tử đáng tin cậy nhằm đảm bảo khả năng xác minh về mặt pháp lý của các sự kiện phát sinh.

Bằng chứng về việc gửi thông điệp và bằng chứng về việc nhận thông điệp phải được liên kết với nội dung thông điệp dữ liệu và được gắn thông tin thời gian nhằm đảm bảo khả năng xác định chính xác thời điểm phát sinh các sự kiện này.

Trong trường hợp Viettel sử dụng dịch vụ dấu thời gian do bên thứ ba cung cấp, Viettel phải định kỳ kiểm tra và đảm bảo rằng dịch vụ dấu thời gian đó vẫn đáp ứng các yêu cầu về độ tin cậy và tuân thủ các quy định pháp luật hiện hành. Việc kiểm tra này có thể được thực hiện thông qua việc đánh giá tình trạng cung cấp dịch vụ của nhà cung cấp dấu thời gian, kiểm tra các chứng nhận liên quan hoặc thông qua các danh sách dịch vụ tin cậy được cơ quan có thẩm quyền công bố.

5.4. Sự kiện và bằng chứng

5.4.1. Các quy định chung

Viettel tạo lập, lưu trữ và cung cấp bằng chứng điện tử cho các bên tham gia giao dịch trong suốt thời gian lưu trữ theo quy định. Bằng chứng điện tử có thể được truy xuất thông qua giao diện dịch vụ hoặc API tích hợp. Tùy theo loại dịch vụ đăng ký, nội dung và phạm

vi bằng chứng điện tử được quy định cụ thể như sau.

a) Đối với dịch vụ ERDS

Hệ thống ERDS tạo lập bằng chứng điện tử tại từng sự kiện trong vòng đời giao dịch, bao gồm:

- Bằng chứng nộp thông điệp: Được tạo lập tự động ngay tại thời điểm hệ thống tiếp nhận thành công thông điệp từ người gửi. Bằng chứng này ghi nhận việc người gửi đã nộp thông điệp vào hệ thống, là cơ sở pháp lý xác nhận thời điểm bắt đầu nghĩa vụ xử lý của Viettel.
- Bằng chứng gửi thông điệp: Ghi nhận hệ thống đã thực hiện chuyển tiếp thông điệp đến phía người nhận, kèm dấu thời gian tương ứng.
- Bằng chứng tiếp nhận thông điệp: Được tạo lập khi người nhận xác nhận tiếp nhận thông điệp thông qua cơ chế xác thực tài khoản. Bằng chứng này ràng buộc danh tính người nhận với sự kiện tiếp nhận và thời điểm nhận.
- Dữ liệu lưu trữ bắt buộc cho mỗi giao dịch ERDS bao gồm:
- Dữ liệu định danh và xác thực của người gửi và người nhận
- Bằng chứng xác minh danh tính ban đầu của người gửi
- Bằng chứng xác minh danh tính người nhận trước khi bàn giao thông điệp
- Nhật ký vận hành hệ thống, nhật ký xác minh danh tính và nhật ký truyền thông
- Giá trị hash của thông điệp dữ liệu, làm căn cứ chứng minh thông điệp không bị sửa đổi trong quá trình truyền tải
- Tham chiếu hoặc giá trị digest của toàn bộ nội dung thông điệp đã nộp
- Dấu thời gian tương ứng với thời điểm nộp, chuyển tiếp, bàn giao và các sự kiện xử lý liên quan

b) Đối với dịch vụ REMS

Hệ thống REMS vận hành theo giao thức SMTP theo mô hình chuyển tiếp thư điện tử. Do đặc thù kỹ thuật của giao thức này, phạm vi bằng chứng điện tử của dịch vụ REMS được xác định như sau:

- Bằng chứng nộp thư: Được tạo lập tại thời điểm hệ thống REMS tiếp nhận thành công thư điện tử từ người gửi, ghi nhận nội dung, thời điểm gửi và thông tin định danh người gửi.
- Bằng chứng chuyển tiếp hệ thống non-ERDS: Ghi nhận hệ thống REMS đã chuyển tiếp thành công thư điện tử đến mail server của người nhận và mail server đó đã xác nhận tiếp nhận.

Lưu ý: Dịch vụ REMS chỉ bảo đảm và tạo lập bằng chứng đến phạm vi mail server của người nhận đã tiếp nhận thư. Dịch vụ REMS không tạo lập bằng chứng và không cam kết về việc cá nhân người nhận đã đọc, truy cập hoặc xử lý thư điện tử, do hành trình của thư sau khi vào hệ thống nội bộ của người nhận nằm ngoài phạm vi kiểm soát của hệ thống REMS.

Dữ liệu lưu trữ bắt buộc cho mỗi giao dịch REMS bao gồm:

- Dữ liệu định danh và xác thực của người gửi
- Thông tin địa chỉ thư điện tử của người nhận và tên miền mail server đích
- Nhật ký vận hành hệ thống REMS và nhật ký kết nối SMTP
- Giá trị hash của nội dung thư điện tử
- Dấu thời gian tại thời điểm tiếp nhận từ người gửi và thời điểm mail server đích xác nhận tiếp nhận

c) Đối với dịch vụ LTAS

Dịch vụ LTAS không tạo lập bằng chứng điện tử mới mà thực hiện bảo quản và gia hạn giá trị pháp lý của các bằng chứng điện tử đã được tạo lập bởi ERDS hoặc REMS trong suốt thời gian lưu trữ dài hạn.

Cơ chế bảo quản bao gồm:

- Lưu trữ bằng chứng gốc: Toàn bộ bằng chứng điện tử phát sinh từ ERDS và REMS được chuyển sang hệ thống LTAS kèm đầy đủ metadata và dấu thời gian gốc.
- Gia hạn bằng chứng định kỳ: Hệ thống LTAS định kỳ thực hiện gắn dấu thời gian mới và củng cố chữ ký số theo tiêu chuẩn ETSI TS 119 512 và RFC 4998, bảo đảm bằng chứng điện tử duy trì khả năng kiểm chứng và giá trị pháp lý ngay cả khi thuật toán mật mã hoặc chứng thư số ban đầu bị suy yếu hoặc hết hạn theo thời gian.
- Khả năng truy xuất: Bằng chứng điện tử được lưu trữ trong LTAS có thể được truy xuất và cung cấp cho các bên liên quan hoặc cơ quan có thẩm quyền trong suốt thời hạn lưu trữ theo quy định pháp luật.

5.4.2. Quy định đối với tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu

Toàn bộ sự kiện liên quan đến xác minh danh tính ban đầu và xác thực tiếp theo của người gửi đều được ghi nhật ký đầy đủ. Tương tự, toàn bộ sự kiện liên quan đến xác minh danh tính ban đầu và xác thực tiếp theo của người nhận đều được ghi nhật ký đầy đủ.

Thông tin xác minh danh tính ban đầu và các lần xác minh tiếp theo được ghi nhận vào hồ sơ thuê bao, bao gồm loại giấy tờ do khách hàng xuất trình để hỗ trợ xác định danh tính, số định danh duy nhất hoặc tổ hợp thông tin định danh, bản sao hồ sơ đăng ký và giấy

tờ định danh kèm thỏa thuận ký kết với người gửi. Các thông tin này được lưu trữ trên hệ thống RA tập trung với cơ chế mã hóa và kiểm soát truy cập.

5.5. Khả năng liên thông

Trong trường hợp hệ thống Viettel kết nối và trao đổi thông điệp với hệ thống ERDS của tổ chức khác, các yêu cầu sau đây được áp dụng bắt buộc.

Về xác minh tư cách của hệ thống đối tác, trước khi chuyển tiếp thông điệp đến hoặc chấp nhận thông điệp chuyển tiếp từ một hệ thống khác, Viettel xác minh rằng hệ thống đó ít nhất đáp ứng tiêu chuẩn của một ERDS. Việc xác minh dựa trên thông tin trong Danh sách dịch vụ tin cậy được công nhận hoặc các tài liệu pháp lý tương đương.

Về xác thực hệ thống đối tác, Viettel xác thực bất kỳ hệ thống ERDS đối tác nào trước khi chuyển tiếp thông điệp đến họ hoặc chấp nhận thông điệp từ họ. Xác thực được thực hiện thông qua cơ chế mutual TLS với chứng thư được cấp theo chính sách NCP hoặc tương đương, bảo đảm không có hệ thống trung gian không xác định có thể chen vào luồng thông điệp.

Về bảo vệ kênh truyền liên hệ thống, Viettel bảo đảm toàn bộ kênh truyền tải thông điệp giữa hệ thống Viettel và các hệ thống ERDS đối tác được bảo vệ để đảm bảo tính toàn vẹn và bảo mật của nội dung thông điệp người dùng trong suốt quá trình truyền tải liên hệ thống. Mọi kết nối liên hệ thống bắt buộc sử dụng kênh mã hóa và chỉ được thiết lập sau khi xác thực lẫn nhau thành công.

6. CHÍNH SÁCH VÀ THỰC THI

6.1. Đánh giá rủi ro

Viettel thực hiện dò quét lỗ hổng bảo mật định kỳ hàng quý đối với các ứng dụng phần mềm và hệ thống hạ tầng. Ngoài ra, Viettel tiến hành kiểm thử xâm nhập hằng năm đối với các thành phần dịch vụ trọng yếu. Các phát hiện từ hoạt động quét và kiểm thử được xác định, rà soát, ưu tiên và khắc phục nhằm duy trì tính toàn vẹn và an toàn của các ứng dụng cũng như hạ tầng vận hành dịch vụ.

6.2. Quy chế chứng thực của tổ chức cung cấp dịch vụ tin cậy

Viettel đảm bảo chất lượng, hiệu năng hoạt động của dịch vụ chứng thực thông điệp dữ liệu thông qua việc triển khai các chính sách và biện pháp kiểm soát bảo mật khác nhau.

Các chính sách và biện pháp kiểm soát bảo mật được một đơn vị độc lập đánh giá thường xuyên, cùng đó đội ngũ nhân sự vận hành sẽ được đào tạo và kiểm tra việc tuân thủ các biện pháp kiểm soát bảo mật theo chính sách.

6.3. Điều khoản và điều kiện áp dụng

Viettel là đơn vị có thẩm quyền phê duyệt và ban hành các điều khoản, điều kiện sử dụng dịch vụ của dịch vụ chứng thực thông điệp dữ liệu Viettel. Các điều khoản, điều kiện

sử dụng dịch vụ được công bố công khai trên trang thông tin điện tử của Viettel-CA.

Tất cả các phiên bản điều khoản và điều kiện sử dụng dịch vụ đã được sửa đổi hoặc cập nhật được công bố và lưu trữ trên trang thông tin điện tử của Viettel-CA tại: <http://Viettel-CA.vn/download>.

6.4. Chính sách an toàn thông tin

Viettel đã thực hiện chính sách an toàn thông tin mà mọi nhân viên phải tuân thủ.

Chính sách an toàn thông tin được xem xét thường xuyên và khi cần có những thay đổi để đáp ứng.

6.5. Nghĩa vụ của tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu

6.5.1. Tổng quan

Viettel cam kết:

- Tuân thủ các nội dung tại CPS này và các chính sách và quy trình nội bộ đã công bố.
- Tuân thủ các quy định của pháp luật.

6.5.2. Nghĩa vụ của tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu đối với thuê bao

Viettel đảm bảo rằng:

- Thực hiện các quy định trong Quy chế chứng thực một cách nghiêm túc, chính xác và đúng thời hạn
- Dịch vụ được cung cấp tuân thủ theo các tiêu chuẩn đã cam kết
- Thực hiện đầy đủ nghĩa vụ cam kết với thuê bao
- Chịu trách nhiệm về việc quản lý và xác minh các điều kiện hoạt động của thuê bao theo quy định của pháp luật

6.6. Thông tin dành cho bên tin tưởng

Nghĩa vụ của Bên tin tưởng được quy định trong Thỏa thuận giữa Tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu và Bên tin tưởng. Ngoài ra, Bên tin tưởng phải có các nghĩa vụ:

- Xác nhận dấu thời gian đã được ký chính xác và khóa được sử dụng để ký không bị lộ lọt cho đến thời điểm xác minh.
- Chấp nhận các điều kiện về việc sử dụng dấu thời gian được nêu trong chính sách cung cấp dịch vụ cấp dấu thời gian.
- Áp dụng các biện pháp phòng ngừa rủi ro trong quy định hoặc giữa thỏa thuận 2

bên.

7. QUẢN LÝ VÀ VẬN HÀNH TỔ CHỨC CUNG CẤP DỊCH VỤ CHỨNG THỰC THÔNG ĐIỆP DỮ LIỆU

7.1. Tổ chức nội bộ

7.1.1. Độ tin cậy của tổ chức

Nhân sự tham gia vận hành hệ thống dịch vụ chứng thực thông điệp dữ liệu Viettel phải được xem xét và xác nhận trước khi được giao các vị trí tin cậy.

Người tin cậy là các cá nhân có quyền truy cập hoặc kiểm soát các quá trình có thể ảnh hưởng đáng kể đến hoạt động của dịch vụ chứng thực thông điệp dữ liệu, bao gồm nhưng không giới hạn:

- Quá trình kiểm tra và xác minh thông tin đăng ký dịch vụ của thuê bao;
- Quá trình cung cấp dịch vụ chứng thực thông điệp dữ liệu;
- Việc ban hành hoặc thu hồi quyền truy cập đối với các khu vực hạn chế của hệ thống;
- Việc chuyển giao thông tin hoặc yêu cầu của thuê bao.
- Người tin cậy có thể bao gồm:
 - Nhân viên giao dịch và nhân viên chăm sóc khách hàng;
 - Nhân viên vận hành hệ thống;
 - Nhân viên an ninh hệ thống;
 - Nhân viên quản trị hệ thống;
- Các kỹ sư thiết kế và phát triển hệ thống.

Tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu thiết lập các quy trình kiểm soát nhằm đảm bảo việc phân công nhiệm vụ dựa trên năng lực và đảm bảo rằng nhiều người tin cậy cùng tham gia thực hiện các công việc có mức độ bảo mật cao.

Tất cả mọi đối tượng muốn trở thành người tin cậy, quy trình xác thực định danh được thực hiện với sự hiện diện về mặt con người (vật lý) của đối tượng này trước khi quy trình kiểm tra thông thường bắt đầu (như kiểm tra chứng minh thư nhân dân, hộ chiếu,...). Quá trình xác thực định danh được thực hiện thêm một lần nữa thông qua thủ tục kiểm tra lý lịch.

Viettel đảm bảo những nhân viên đạt được vị trí được tin cậy và trao quyền cho các nhân viên này:

- Được cấp phép truy cập tới các phạm vi cần thiết;

- Được cấp tài liệu điện tử để có thể truy cập đến và thực hiện một số chức năng trên hệ thống của Viettel hay các hệ thống IT khác.

7.1.2. Phân tách công việc

Viettel thực hiện phân tách trách nhiệm giữa các vị trí công việc nhằm giảm thiểu nguy cơ lạm dụng quyền hạn.

Các nhiệm vụ cần phân tách trách nhiệm bao gồm:

- Xác nhận thông tin trong đơn đăng ký dịch vụ của thuê bao;
- Quá trình chấp nhận hoặc từ chối đăng ký dịch vụ; hoặc các quá trình khác của ứng dụng chứng thực, yêu cầu gia hạn hoặc hủy gia hạn;
- Quá trình tạo, lưu trữ hoặc tiêu hủy dữ liệu chứng thực;
- Quá trình tạo và quản lý bằng chứng chứng thực.

7.2. Quản lý nhân sự

7.2.1. Các quy định chung

Tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu xây dựng chính sách quản lý nhân sự và chính sách bảo mật nhằm đảm bảo nhân sự vận hành hệ thống có năng lực chuyên môn và độ tin cậy phù hợp.

Việc tuân thủ các chính sách này được kiểm tra định kỳ thông qua các hoạt động kiểm toán nội bộ và đánh giá độc lập.

7.2.2. Quy định đối với tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu

a) Yêu cầu về phẩm chất, kinh nghiệm và độ tin cậy

Các cá nhân làm việc tại vị trí tin cậy phải chứng minh có:

- Lý lịch rõ ràng;
- Phẩm chất đạo đức tốt;
- Kinh nghiệm và trình độ chuyên môn phù hợp.

Quá trình kiểm tra lý lịch được thực hiện định kỳ ít nhất một lần mỗi năm đối với các nhân sự giữ vị trí tin cậy.

b) Thủ tục kiểm tra lý lịch

Trước khi được giao vị trí tin cậy, tổ chức cung cấp dịch vụ thực hiện kiểm tra lý lịch bao gồm:

- Xác nhận thông tin cá nhân và gia đình;
- Xác nhận từ đơn vị công tác trước đây;

- Tham khảo ý kiến từ đồng nghiệp;
- Xác nhận trình độ đào tạo;
- Kiểm tra tiền án tiền sự;
- Kiểm tra thông tin tài chính.

Những trường hợp phát hiện thông tin không trung thực, có tiền án tiền sự hoặc không đáp ứng yêu cầu về độ tin cậy có thể bị loại khỏi vị trí tin cậy.

c) Đào tạo

Nhân sự của tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu được đào tạo trước khi tham gia vận hành hệ thống.

Chương trình đào tạo bao gồm:

- Kiến thức về hạ tầng khóa công khai và dịch vụ tin cậy;
- Quy trình vận hành hệ thống;
- Chính sách và quy định an toàn thông tin;
- Sử dụng và vận hành các thiết bị phần cứng và phần mềm;
- Quy trình khôi phục sau sự cố.

d) Đào tạo lại

Trong quá trình làm việc, nhân sự được đào tạo nâng cao định kỳ để duy trì năng lực chuyên môn và khả năng thực hiện công việc.

e) Kỷ luật

Các hành vi vi phạm quy định an toàn thông tin hoặc quy chế vận hành sẽ bị xử lý kỷ luật tùy theo mức độ vi phạm.

7.3. Quản lý tài sản

7.3.1. Yêu cầu chung

Viettel duy trì hệ thống lưu trữ và quản lý đầy đủ các bản ghi liên quan đến hoạt động của dịch vụ, bao gồm dữ liệu kiểm tra hệ thống, thông tin đăng ký dịch vụ của thuê bao, thông tin về vòng đời của dữ liệu chứng thực và các tài liệu hồ sơ liên quan. Tài sản thông tin được phân loại theo mức độ nhạy cảm và áp dụng biện pháp bảo vệ tương ứng.

7.3.2. Xử lý phương tiện lưu trữ

Các phương tiện lưu trữ chứa dữ liệu nhạy cảm được bảo vệ bằng kiểm soát truy cập vật lý và logic trong suốt vòng đời sử dụng. Khi không còn nhu cầu sử dụng, phương tiện lưu trữ chứa thông tin nhạy cảm phải được tiêu hủy theo quy trình bảo đảm không thể phục

hồi dữ liệu, có ghi nhận và chứng từ tiêu hủy.

7.4. Kiểm soát truy cập

Viettel áp dụng nguyên tắc phân quyền tối thiểu đối với toàn bộ tài khoản và quyền truy cập vào hệ thống dịch vụ. Mỗi cá nhân chỉ được cấp quyền truy cập đúng với phạm vi công việc được giao, không hơn.

Truy cập vật lý vào khu vực đặt thiết bị được kiểm soát theo mô hình nhiều lớp: lớp ngoài cùng là kiểm soát bảo vệ tòa nhà, tiếp theo là xác thực sinh trắc học để vào trung tâm dữ liệu, sau đó là xác thực thẻ từ để vào vùng máy chủ dịch vụ, và lớp trong cùng là xác thực thẻ từ cấp cao hơn để vào vùng đặt máy chủ ERDS Core và thiết bị HSM. Mọi sự kiện ra vào đều được ghi nhận log và lưu trữ.

Truy cập logic vào hệ thống yêu cầu xác thực tài khoản cá nhân. Không sử dụng tài khoản dùng chung. Quyền truy cập được rà soát và cập nhật định kỳ, đặc biệt khi nhân sự thay đổi vị trí công tác hoặc rời tổ chức. Toàn bộ thao tác quản trị trên hệ thống được ghi nhận vào log tập trung phục vụ kiểm toán.

7.5. Kiểm soát mật mã

Viettel áp dụng các thuật toán mật mã đáp ứng tiêu chuẩn quốc tế hiện hành cho toàn bộ hoạt động mật mã trong hệ thống dịch vụ. Cụ thể, thuật toán ký số sử dụng RSA với độ dài khóa tối thiểu 2048 bit hoặc ECDSA P-256 trở lên; thuật toán băm sử dụng SHA-256 trở lên; thuật toán mã hóa đối xứng sử dụng AES-256 để bảo vệ khóa bí mật và dữ liệu lưu trữ.

Toàn bộ khóa mật mã của hệ thống được sinh ra, lưu giữ và thực hiện các phép toán mật mã hoàn toàn bên trong thiết bị HSM Utimaco CryptoServer đạt chuẩn FIPS 140-2 Level 3. Khóa bí mật không bao giờ rời thiết bị HSM dưới dạng có thể đọc được. Việc kích hoạt và sử dụng HSM được kiểm soát theo cơ chế đa thành phần, yêu cầu sự tham gia đồng thời của nhiều cán bộ quản lý được ủy quyền.

Vòng đời của khóa mật mã, bao gồm sinh khóa, kích hoạt, sử dụng, gia hạn và tiêu hủy, được quản lý theo quy trình có tài liệu hóa. Mọi sự kiện liên quan đến vòng đời khóa đều được ghi nhận vào log hệ thống.

7.6. An ninh vật lý và môi trường

Hệ thống dịch vụ chứng thực thông điệp dữ liệu được triển khai trong môi trường vật lý được bảo vệ nhằm ngăn chặn truy cập trái phép.

Các biện pháp an ninh vật lý bao gồm:

- Kiểm soát ra vào bằng thẻ nhân viên và hệ thống sinh trắc học;
- Giám sát bằng camera 24/7;

- Hệ thống phòng cháy chữa cháy;
- Hệ thống chống nước;
- Hệ thống nguồn điện dự phòng UPS và máy phát điện.

Hệ thống dự phòng được triển khai tại địa điểm tách biệt với hệ thống chính tối thiểu 10 km.

7.7. An ninh vận hành

Viettel ghi nhận toàn bộ sự kiện vận hành hệ thống phục vụ kiểm toán và truy vết. Các sự kiện được ghi nhận bao gồm khởi động và tắt hệ thống, thay đổi cấu hình, truy cập của người dùng và quản trị viên, lỗi hệ thống, và các sự kiện liên quan đến xử lý dữ liệu chứng thực và bằng chứng điện tử.

Log được phân chia theo ngày, lưu phân tán tại từng thành phần ứng dụng và đồng thời lưu tập trung trên hệ thống quản lý log tập trung của hạ tầng Viettel. Log được sao lưu sang trung tâm dự phòng và lưu trữ tối thiểu năm năm. Tính bảo mật, toàn vẹn và sẵn sàng của log được bảo đảm thông qua kiểm soát truy cập nghiêm ngặt và cơ chế phát hiện thay đổi.

7.8. An ninh mạng

Hệ thống mạng của Viettel được thiết kế theo mô hình phân vùng bảo mật nhiều lớp, kiểm soát chặt chẽ luồng dữ liệu giữa các vùng. Vùng Trust Service Zone (nơi đặt ERDS Core và HSM) có mức bảo mật cao nhất và không có kết nối trực tiếp từ Internet. Vùng Security Zone chứa hệ thống lưu trữ và giám sát. Vùng DMZ là vùng duy nhất tiếp xúc với bên ngoài, chứa Service Gateway và các dịch vụ cung cấp cho khách hàng.

Hệ thống tường lửa Fortinet được triển khai tại ranh giới giữa các vùng, kiểm soát truy cập theo giao thức, cổng dịch vụ và địa chỉ IP. Hệ thống IPS của Cisco được triển khai tại gateway của vùng DMZ, thực hiện phát hiện và ngăn chặn tấn công theo thời gian thực 24/7. Cảnh báo an ninh được gửi tự động đến quản trị viên qua email và SMS. Mọi kết nối từ bên ngoài vào hệ thống đều phải sử dụng TLS phiên bản 1.2 trở lên.

7.9. Quản lý sự cố

Khi xảy ra sự cố đối với hệ thống hoặc nghi ngờ có sự cố an ninh, Viettel kích hoạt ngay quy trình xử lý sự cố.

Đơn vị xử lý sự cố có trách nhiệm:

- Đánh giá mức độ ảnh hưởng của sự cố;
- Triển khai biện pháp khắc phục;
- Thông báo cho các bên liên quan;

- Lưu trữ bằng chứng phục vụ điều tra.

7.10. Thu thập bằng chứng cho các dịch vụ nội bộ của tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu

Viettel thực hiện thu thập, bảo vệ, lưu trữ và cung cấp bằng chứng điện tử phát sinh trong quá trình cung cấp và vận hành dịch vụ nhằm phục vụ kiểm toán, truy vết, xử lý sự cố, chứng minh hoạt động của dịch vụ và đáp ứng yêu cầu của cơ quan có thẩm quyền khi cần thiết.

Bước 1 – Ghi nhận sự kiện

Các thành phần hệ thống ghi nhận vào nhật ký (log) các sự kiện phát sinh trong quá trình cung cấp dịch vụ, bao gồm: sự kiện liên quan đến vòng đời bằng chứng điện tử (tạo lập, ký số, gia hạn); sự kiện truy cập và quản trị hệ thống; sự kiện liên quan đến khóa mật mã và thiết bị HSM; thay đổi cấu hình; khởi động, dừng hoặc lỗi hệ thống; sự kiện an toàn thông tin; và sự kiện truy cập vật lý khu vực đặt hệ thống.

Thời điểm phát sinh sự kiện được ghi nhận theo nguồn thời gian đã được đồng bộ của hệ thống, theo quy định tại Mục 5.3.

Bước 2 – Thu thập và tập trung bằng chứng

Nhật ký và bằng chứng phát sinh tại các thành phần hệ thống được thu thập và chuyển về hệ thống quản lý nhật ký/kho bằng chứng tập trung. Các bản ghi thuộc cùng một giao dịch được liên kết thông qua mã định danh giao dịch, mã thông điệp hoặc mã bằng chứng tương ứng.

Bước 3 – Kiểm tra việc thu thập

Đơn vị vận hành kiểm tra định kỳ trạng thái thu thập nhằm phát hiện thiếu bản ghi, lỗi thu thập hoặc dấu hiệu dữ liệu không nhất quán. Việc kiểm tra không làm thay đổi nội dung bản ghi gốc.

Bước 4 – Bảo vệ và lưu trữ bằng chứng

Bằng chứng và nhật ký sau khi thu thập được lưu trữ trên hệ thống có kiểm soát truy cập, áp dụng cơ chế phát hiện thay đổi hoặc xóa trái phép, và được sao lưu sang hệ thống dự phòng theo quy trình sao lưu tại Mục 7.11.2.

Thời hạn lưu trữ áp dụng nguyên tắc tối thiểu hai (02) năm đối với nhật ký và bằng chứng nội bộ nói chung. Đối với từng loại bằng chứng, dữ liệu hoặc lĩnh vực dịch vụ cụ thể, thời hạn lưu trữ thực tế có thể dài hơn mức tối thiểu nêu trên, tùy theo quy định pháp luật chuyên ngành áp dụng tại từng thời điểm (ví dụ: bằng chứng của dịch vụ ERDS phục vụ tố tụng có thể yêu cầu thời hạn lưu trữ dài hơn theo quy định của cơ quan tố tụng có thẩm quyền) hoặc theo thỏa thuận với khách hàng. Đối với các loại dữ liệu đã có cam kết thời hạn lưu trữ cụ thể tại các mục khác của CPS này, thời hạn đó được ưu tiên áp dụng.

Bước 5 – Giám sát trong thời gian lưu trữ

Trong thời gian lưu trữ, Viettel giám sát khả năng truy cập và tính toàn vẹn của bằng chứng. Khi phát hiện sự cố ảnh hưởng đến tính toàn vẹn hoặc khả năng truy cập, quy trình xử lý sự cố tại Mục 7.9 được kích hoạt.

Bước 6 – Tra cứu và xuất trình bằng chứng

Việc tra cứu, trích xuất và xuất trình bằng chứng ra ngoài hệ thống chỉ được thực hiện bởi nhân sự được phân quyền, khi có một trong các căn cứ sau: yêu cầu của cơ quan nhà nước có thẩm quyền (thanh tra, điều tra, tố tụng), yêu cầu phục vụ giải quyết tranh chấp theo thỏa thuận với khách hàng, hoặc yêu cầu kiểm toán/đánh giá tuân thủ nội bộ.

Trước khi cung cấp, Viettel xác minh thẩm quyền của bên yêu cầu và kiểm tra tính toàn vẹn của bằng chứng được trích xuất. Bằng chứng được cung cấp dưới hình thức bảo đảm khả năng xác minh nguồn gốc và tính toàn vẹn (kèm giá trị băm và/hoặc dấu thời gian xác nhận). Toàn bộ quá trình truy cập, trích xuất và cung cấp được ghi nhật ký phục vụ truy vết.

7.11. Quản lý tính liên tục trong hoạt động kinh doanh

Viettel duy trì các quy trình nhằm bảo đảm khả năng tiếp tục cung cấp dịch vụ và khả năng tiếp tục kiểm chứng bằng chứng điện tử trong suốt thời gian cung cấp và lưu trữ dịch vụ, bao gồm: quy trình phục hồi hoạt động khi có sự cố (7.11.1), quy trình sao lưu và phục hồi dữ liệu (7.11.2), quy trình xử lý khi khóa mật mã của hệ thống bị mất/lộ (7.11.3), quy trình duy trì giá trị kiểm chứng lâu dài của bằng chứng điện tử (7.11.4), và nguồn nhân lực phục vụ công tác duy trì tính liên tục (7.11.5).

7.11.1. Quy trình duy trì và phục hồi hoạt động dịch vụ

Bước 1 – Phát hiện và ghi nhận sự cố

Sự cố có khả năng gây gián đoạn dịch vụ được phát hiện, ghi nhận và xử lý ban đầu theo quy trình quản lý sự cố tại Mục 7.9.

Bước 2 – Đánh giá mức độ ảnh hưởng

Đơn vị vận hành đánh giá phạm vi ảnh hưởng đối với hệ thống ứng dụng, cơ sở dữ liệu, hệ thống lưu trữ, hệ thống mạng, thiết bị mật mã và các dịch vụ phụ thuộc, làm căn cứ quyết định tiếp tục xử lý trên hệ thống chính hoặc kích hoạt hệ thống dự phòng.

Bước 3 – Kích hoạt hệ thống dự phòng

Trường hợp hệ thống chính không thể tiếp tục cung cấp dịch vụ, Viettel kích hoạt hệ thống dự phòng đặt tại địa điểm tách biệt với hệ thống chính (khoảng cách tối thiểu theo Mục 7.6 của CPS này).

Bước 4 – Phục hồi dữ liệu

Dữ liệu được đồng bộ hoặc phục hồi từ bản sao lưu gần nhất theo quy trình tại Mục 7.11.2. Sau phục hồi, hệ thống kiểm tra tính đầy đủ, toàn vẹn và khả năng truy cập của dữ liệu trước khi tiếp tục cung cấp dịch vụ.

Bước 5 – Kiểm tra dịch vụ sau phục hồi

Đơn vị vận hành xác nhận các thành phần trọng yếu hoạt động bình thường trước khi đưa dịch vụ trở lại trạng thái cung cấp cho người sử dụng.

Bước 6 – Thông báo cho khách hàng, các bên liên quan và cơ quan nhà nước có thẩm quyền

Trường hợp sự cố làm gián đoạn hoặc ảnh hưởng đến khả năng cung cấp dịch vụ, Viettel thông báo kịp thời cho khách hàng và các bên liên quan theo phạm vi ảnh hưởng và các điều khoản đã thỏa thuận, bao gồm tình trạng dịch vụ, phạm vi ảnh hưởng, trạng thái xử lý và cập nhật khi có thay đổi đáng kể.

Thông tin về sự cố được tổng hợp và báo cáo cơ quan nhà nước có thẩm quyền theo hình thức báo cáo định kỳ hoặc báo cáo đột xuất (bất thường) theo quy định pháp luật hiện hành áp dụng đối với tổ chức cung cấp dịch vụ tin cậy.

Bước 7 – Khôi phục hệ thống chính

Sau khi khắc phục nguyên nhân sự cố, Viettel phục hồi hệ thống chính và đồng bộ dữ liệu phát sinh trong thời gian vận hành trên hệ thống dự phòng. Dịch vụ chỉ chuyển trở lại hệ thống chính sau khi xác nhận đủ điều kiện vận hành.

Bước 8 – Tổng kết và cập nhật phương án

Nguyên nhân, thời gian gián đoạn, thao tác phục hồi và kết quả được ghi nhận, sử dụng làm cơ sở cập nhật phương án phục hồi khi cần thiết.

Trường hợp xảy ra sự cố nghiêm trọng, Viettel thực hiện các biện pháp cần thiết để khôi phục các chức năng cơ bản của dịch vụ trong thời gian không quá 8 giờ kể từ thời điểm xác định sự cố.

7.11.2. Quy trình sao lưu và kiểm tra khả năng phục hồi

Bước 1 – Thực hiện sao lưu

Dữ liệu, cấu hình hệ thống, bằng chứng điện tử và thông tin cần thiết để phục hồi dịch vụ được sao lưu theo lịch sao lưu nội bộ đã được phê duyệt.

Bước 2 – Lưu bản sao tại môi trường dự phòng

Bản sao lưu được chuyển tới môi trường lưu trữ dự phòng tách biệt với hệ thống nguồn.

Bước 3 – Kiểm tra bản sao lưu

Đơn vị vận hành định kỳ kiểm tra tính toàn vẹn và khả năng sử dụng của dữ liệu sao lưu; trường hợp phát hiện bất thường, thực hiện lại việc sao lưu hoặc biện pháp khắc phục.

Bước 4 – Thử nghiệm phục hồi

Viettel định kỳ tối thiểu một (01) lần mỗi năm thực hiện thử nghiệm phục hồi từ bản sao lưu nhằm kiểm tra khả năng sử dụng thực tế của dữ liệu dự phòng. Kết quả thử nghiệm được lập thành văn bản, lưu trữ và sử dụng làm cơ sở cải thiện phương án phục hồi.

Bước 5 – Áp dụng kiểm soát kép đối với quản lý khóa mật mã trên thiết bị HSM

Đối với việc sao lưu, phục hồi, kích hoạt hoặc sử dụng lại khóa mật mã trên thiết bị HSM, Viettel áp dụng cơ chế xác thực đa thành phần M-of-N, bảo đảm mức tối thiểu là hai (02) cá nhân được ủy quyền độc lập (M) phải tham gia xác thực đồng thời trong tổng số tối thiểu ba (03) cá nhân nắm giữ thông tin xác thực (N), phù hợp với mức tối thiểu theo thông lệ và quy chuẩn kỹ thuật hiện hành về quản lý khóa mật mã. Không một cá nhân nào được tự thực hiện toàn bộ thao tác quản lý khóa mật mã một mình.

Giá trị M, N thực tế áp dụng (có thể cao hơn mức tối thiểu nêu trên), danh sách nhân sự tương ứng và quy trình thực hiện chi tiết được quy định tại quy trình quản lý khóa và tài liệu vận hành nội bộ về HSM của Viettel (không công bố công khai trong CPS này nhằm bảo đảm an toàn thông tin), phù hợp với Mục 7.5 (Kiểm soát mật mã) của CPS này.

Đối với việc phục hồi, kích hoạt hoặc sử dụng lại khóa bí mật và thiết bị mật mã sau sự cố, việc thực hiện phải tuân thủ cơ chế kiểm soát kép nêu trên.

7.11.3. Quy trình xử lý trường hợp khóa mật mã của hệ thống bị mất, lộ hoặc nghi ngờ lộ

Trường hợp phát hiện hoặc nghi ngờ khóa bí mật của hệ thống bị lộ, mất hoặc sử dụng trái phép, Viettel thực hiện:

Bước 1 – Ngừng sử dụng khóa bị ảnh hưởng

Hệ thống ngừng ngay việc sử dụng khóa bị ảnh hưởng để tạo mới chữ ký hoặc bằng chứng.

Bước 2 – Xác định phạm vi ảnh hưởng

Viettel xác định thời điểm xảy ra hoặc thời điểm sớm nhất có khả năng xảy ra sự cố, và xác định các bằng chứng đã được tạo bằng khóa bị ảnh hưởng.

Bước 3 – Báo cáo Root CA và cơ quan nhà nước có thẩm quyền

Viettel báo cáo Trung tâm Chứng thực điện tử quốc gia (Root CA) trong vòng 24 giờ kể từ khi phát hiện dấu hiệu khóa bí mật bị lộ, bị đánh cắp hoặc bị sử dụng sai mục đích, theo nghĩa vụ của tổ chức cung cấp dịch vụ tin cậy quy định tại Nghị định số 23/2025/NĐ-CP và CP/CPS của Root CA.

Bước 4 – Thông báo cho khách hàng và các bên liên quan

Viettel thông báo kịp thời cho khách hàng và các bên liên quan bị ảnh hưởng theo các điều khoản đã thỏa thuận, cung cấp thông tin về phạm vi ảnh hưởng đã xác định, trạng thái xử lý và hướng dẫn cần thiết. Thông tin được cập nhật khi phạm vi/mức độ ảnh hưởng được xác định rõ hơn.

Bước 5 – Kích hoạt khóa hoặc phương tiện mật mã thay thế

Khóa và phương tiện mật mã dự phòng được kích hoạt theo quy trình quản lý khóa nội bộ và cơ chế kiểm soát kép tại Mục 7.11.2.

Bước 6 – Xử lý các bằng chứng liên quan

Các bằng chứng đã tạo trước thời điểm xảy ra sự cố được đánh giá khả năng tiếp tục kiểm chứng. Trường hợp cần thiết, bằng chứng còn hợp lệ được bảo vệ bổ sung bằng dấu thời gian hoặc cơ chế bảo quản dài hạn trước khi giá trị chứng minh bị ảnh hưởng, không xóa bỏ bằng chứng gốc đã tạo lập trước đó.

Bước 7 – Khôi phục và ghi nhận

Hoạt động tạo lập bằng chứng được chuyển sang khóa mới. Toàn bộ quá trình xử lý được ghi nhận phục vụ truy vết và kiểm toán.

7.11.4. Quy trình duy trì giá trị kiểm chứng lâu dài của bằng chứng điện tử

Đối với dịch vụ lưu trữ và xác nhận tính toàn vẹn của thông điệp dữ liệu (LTAS), Viettel thực hiện giám sát và gia hạn Bản ghi bằng chứng ("Evidence Record") theo tiêu chuẩn IETF RFC 4998 và RFC 6283 nhằm duy trì khả năng kiểm chứng trong toàn bộ thời gian lưu trữ.

Việc gia hạn được thực hiện trước khi Dấu thời gian lưu trữ ("Archive Time-Stamp") hiện tại không còn đủ khả năng phục vụ kiểm chứng, hoặc thuật toán mật mã hiện tại không còn đáp ứng yêu cầu an toàn theo quy chuẩn kỹ thuật hiện hành. Dấu thời gian lưu trữ mới được cấp phải bảo đảm hợp lệ, an toàn, sử dụng thuật toán được đánh giá còn an toàn trong thời gian dài, phù hợp với thời hạn lưu trữ còn lại của Bản ghi bằng chứng. Sau mỗi lần gia hạn, Dấu thời gian lưu trữ mới trở thành đối tượng tiếp tục được giám sát cho lần gia hạn tiếp theo.

7.11.4.1. Quy trình giám sát nhu cầu gia hạn

Bước 1 – Xác định Dấu thời gian lưu trữ hiện tại

Hệ thống xác định Dấu thời gian lưu trữ mới nhất (Dấu thời gian lưu trữ hiện tại) trong Bản ghi bằng chứng đang được lưu trữ.

Bước 2 – Theo dõi các thành phần mật mã

Hệ thống định kỳ theo dõi: thời hạn hiệu lực và trạng thái chứng thư số của Dịch vụ

cấp dấu thời gian đang sử dụng; trạng thái tin cậy của Dịch vụ cấp dấu thời gian; thuật toán ký/tham số mật mã sử dụng trong Dấu thời gian hiện tại; thuật toán băm được sử dụng trong Chuỗi dấu thời gian lưu trữ (Archive Time-Stamp Chain) hiện tại; và các thay đổi trong danh mục thuật toán mật mã được phép sử dụng theo quy chuẩn kỹ thuật hiện hành.

Bước 3 – Xác định phương thức gia hạn

Nếu thuật toán băm hiện tại vẫn đáp ứng yêu cầu an toàn nhưng Dấu thời gian lưu trữ hiện tại có nguy cơ không còn bảo đảm khả năng kiểm chứng lâu dài, hệ thống thực hiện gia hạn dấu thời gian theo Mục 7.11.4.2.

Nếu thuật toán băm hiện tại không còn đáp ứng yêu cầu an toàn cho thời gian lưu trữ còn lại, hệ thống thực hiện gia hạn thuật toán theo Mục 7.11.4.3.

7.11.4.2. Quy trình gia hạn dấu thời gian

Gia hạn Dấu thời gian lưu trữ được thực hiện khi thuật toán băm hiện tại vẫn đáp ứng yêu cầu an toàn nhưng Dấu thời gian lưu trữ hiện tại cần được bảo vệ tiếp, bao gồm nhưng không giới hạn ở các trường hợp sau: chứng thư số của Dịch vụ cấp dấu thời gian sắp hết hiệu lực; thuật toán ký hoặc độ dài khóa của Dịch vụ cấp dấu thời gian có nguy cơ không còn đủ an toàn; chứng thư số của Dịch vụ cấp dấu thời gian bị tạm dừng, thu hồi hoặc mất trạng thái tin cậy; hoặc Dấu thời gian lưu trữ hiện tại có nguy cơ không còn đủ dữ liệu kiểm chứng (chứng thư, thông tin trạng thái chứng thư) để xác minh trong tương lai.

Bước 1 – Kiểm tra Dấu thời gian lưu trữ hiện tại

Hệ thống xác minh Dấu thời gian lưu trữ hiện tại còn khả năng kiểm chứng tại thời điểm gia hạn.

Bước 2 – Thu thập dữ liệu kiểm chứng

Hệ thống thu thập chứng thư số, chuỗi chứng thư và thông tin trạng thái chứng thư (OCSP, CRL hoặc thông tin tương đương) cần thiết để kiểm chứng Dấu thời gian lưu trữ hiện tại, gắn với Dấu thời gian lưu trữ hiện tại để được bảo vệ bởi lần gia hạn tiếp theo.

Bước 3 – Tính giá trị băm phục vụ gia hạn

Hệ thống sử dụng cùng thuật toán băm của Chuỗi dấu thời gian lưu trữ hiện tại để tính giá trị băm trên nội dung Dấu thời gian lưu trữ hiện tại, bao gồm các thông tin kiểm chứng đã bổ sung.

Bước 4 – Yêu cầu Mã thông báo dấu thời gian mới

Giá trị băm được gửi tới Dịch vụ cấp dấu thời gian để yêu cầu cấp Mã thông báo dấu thời gian mới. Mã thông báo dấu thời gian mới phải do tổ chức cung cấp dịch vụ cấp dấu thời gian được cấp phép theo quy định của cơ quan nhà nước có thẩm quyền phát hành, sử dụng chứng thư số và thuật toán còn hiệu lực, an toàn và có thời hạn sử dụng dài hơn tại thời điểm cấp.

Bước 5 – Kiểm tra Mã thông báo dấu thời gian mới

Hệ thống kiểm tra tối thiểu giá trị mã băm, chữ ký của Mã thông báo dấu thời gian mới, chứng thư của Dịch vụ cấp dấu thời gian và thời gian tạo dấu thời gian trước khi sử dụng. Chỉ Mã thông báo dấu thời gian đáp ứng yêu cầu kiểm tra mới được sử dụng để gia hạn Bản ghi bằng chứng.

Bước 6 – Bổ sung Dấu thời gian lưu trữ mới

Dấu thời gian lưu trữ mới được bổ sung vào cuối Chuỗi dấu thời gian lưu trữ hiện tại. Các Dấu thời gian lưu trữ đã tồn tại trước đó (bao gồm Dấu thời gian lưu trữ cũ vừa được gia hạn) không bị thay đổi hoặc loại bỏ.

Bước 7 – Kiểm tra Bản ghi bằng chứng sau gia hạn

Hệ thống xác minh lại Bản ghi bằng chứng sau cập nhật, ghi nhận kết quả gia hạn và tiếp tục lưu trữ. Dấu thời gian lưu trữ mới trở thành Dấu thời gian lưu trữ hiện tại, được sử dụng làm đối tượng giám sát cho lần gia hạn tiếp theo.

7.11.4.3. Quy trình gia hạn thuật toán

Gia hạn thuật toán được thực hiện khi thuật toán băm hiện tại đang bảo vệ Bản ghi bằng chứng không còn đáp ứng mức an toàn theo quy chuẩn kỹ thuật hiện hành hoặc được dự báo không còn đủ an toàn trong thời gian lưu trữ còn lại.

Bước 1 – Xác định thuật toán thay thế

Viettel xác định thuật toán băm mới đáp ứng yêu cầu an toàn tại thời điểm gia hạn, phù hợp quy chuẩn kỹ thuật quốc gia hiện hành do Bộ Khoa học và Công nghệ ban hành và bảo đảm thời gian sử dụng an toàn phù hợp với thời hạn lưu trữ còn lại theo quy định pháp luật. Thuật toán mới phải khác và có mức an toàn cao hơn hoặc tương đương thuật toán cũ đang sử dụng.

Bước 2 – Kiểm tra Bản ghi bằng chứng hiện tại

Trước khi gia hạn, hệ thống xác minh toàn bộ Bản ghi bằng chứng hiện tại (bao gồm Dãy dấu thời gian lưu trữ – "Archive Time-Stamp Sequence" – hiện có và các dữ liệu được bảo vệ) bằng thuật toán cũ. Việc gia hạn chỉ tiếp tục khi bằng chứng hiện tại được xác minh thành công.

Bước 3 – Thu thập dữ liệu kiểm chứng cần thiết

Hệ thống thu thập và lưu kèm chứng thư, OCSP, CRL hoặc dữ liệu kiểm chứng tương ứng cần thiết để kiểm chứng các Dấu thời gian lưu trữ hiện có.

Bước 4 – Tính lại giá trị băm bằng thuật toán mới

Hệ thống sử dụng thuật toán băm mới để tính lại giá trị băm đối với các đối tượng dữ liệu đang được bảo quản và Dãy dấu thời gian lưu trữ đã hình thành bằng thuật toán cũ

trước thời điểm gia hạn.

Bước 5 – Xây dựng cây băm mới

Các giá trị băm mới được sử dụng để xây dựng cây băm (hash tree) mới, bảo vệ đồng thời dữ liệu gốc và lịch sử bằng chứng đã tồn tại bằng thuật toán cũ. Giá trị băm tại nút gốc của cây băm mới (giá trị băm gốc của cây băm) trở thành giá trị được sử dụng để yêu cầu cấp Dấu thời gian mới.

Bước 6 – Yêu cầu và kiểm tra Mã thông báo dấu thời gian mới

Hệ thống gửi giá trị băm gốc của cây băm tới Dịch vụ cấp dấu thời gian (do tổ chức cung cấp dịch vụ cấp dấu thời gian được cấp phép theo quy định của cơ quan nhà nước có thẩm quyền cung cấp) để nhận Mã thông báo dấu thời gian mới, sử dụng thuật toán mới đã xác định tại Bước 1, và thực hiện kiểm tra theo Bước 5 của Mục 7.11.4.2 trước khi sử dụng.

Bước 7 – Tạo Chuỗi dấu thời gian lưu trữ mới

Dấu thời gian lưu trữ mới được đặt làm Dấu thời gian lưu trữ đầu tiên của Chuỗi dấu thời gian lưu trữ mới (sử dụng thuật toán mới); Chuỗi dấu thời gian lưu trữ mới được bổ sung vào cuối Dãy dấu thời gian lưu trữ hiện tại. Các Chuỗi dấu thời gian lưu trữ cũ được giữ nguyên nhằm duy trì toàn bộ lịch sử kiểm chứng của Bản ghi bằng chứng.

Bước 8 – Kiểm tra và hoàn tất gia hạn

Hệ thống xác minh lại Bản ghi bằng chứng sau gia hạn bằng thuật toán mới. Kết quả gia hạn, thuật toán cũ, thuật toán mới, thời điểm thực hiện, Dấu thời gian mới và trạng thái kiểm tra được ghi nhận phục vụ kiểm toán và truy vết. Sau khi gia hạn thành công, Dấu thời gian lưu trữ mới trở thành Dấu thời gian lưu trữ hiện tại, tiếp tục được giám sát theo Mục 7.11.4.1.

7.11.5. Nguồn nhân lực và phân công trách nhiệm

Nhân sự tham gia thực hiện các quy trình tại Mục 7.11 thuộc nhóm người tin cậy được xác định tại Mục 7.1 và Mục 7.2 của CPS này, bao gồm tối thiểu: nhân viên vận hành hệ thống (thực hiện đánh giá sự cố, kích hoạt hệ thống dự phòng, sao lưu và phục hồi dữ liệu), nhân viên an ninh hệ thống (giám sát an toàn thông tin trong quá trình xử lý sự cố) và nhân viên quản trị hệ thống/mật mã (thực hiện các thao tác liên quan đến khóa mật mã và thiết bị HSM theo cơ chế kiểm soát kép tại Mục 7.11.2).

Việc phân công nhiệm vụ cụ thể cho từng vị trí trong quy trình xử lý sự cố và khôi phục hoạt động được thực hiện theo quyết định phân công nội bộ của Viettel, tuân thủ nguyên tắc phân tách công việc tại Mục 7.1.2.

Nhân sự đảm nhận các vị trí liên quan đến quản lý tính liên tục được đào tạo trước khi phân công nhiệm vụ và đào tạo lại định kỳ theo quy định tại Mục 7.2. Viettel tổ chức rà soát, kiểm thử phương án phục hồi hoạt động (bao gồm thử nghiệm phục hồi dữ liệu tại

Mục 7.11.2) định kỳ tối thiểu một (01) lần mỗi năm nhằm bảo đảm nhân sự nắm rõ vai trò, trách nhiệm và trình tự xử lý khi có sự cố thực tế.

7.12. Chấm dứt hoạt động của tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu và kế hoạch chấm dứt

Trong trường hợp chấm dứt cung cấp dịch vụ, tổ chức cung cấp dịch vụ chứng thực thông điệp dữ liệu sẽ:

- Thông báo cho thuê bao và các bên liên quan;
- Duy trì hệ thống lưu trữ dữ liệu theo quy định;
- Đảm bảo khả năng truy xuất và xác minh dữ liệu đã phát hành;
- Thực hiện các nghĩa vụ pháp lý theo quy định của pháp luật.

7.13. Tuân thủ quy định

a) Hệ thống căn cứ pháp lý

Tài liệu quy chế chứng thực được điều chỉnh bởi các văn bản quy phạm pháp luật, bao gồm:

- Luật Giao dịch điện tử số 20/2023/QH15 ngày 22 tháng 6 năm 2023;
- Nghị định số 23/2025/NĐ-CP ngày 21 tháng 02 năm 2025 của Chính phủ quy định về chữ ký điện tử và dịch vụ tin cậy.

b) Tuân thủ quy định pháp luật hiện hành

- Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19 tháng 11 năm 2015;
- Luật An ninh mạng số 24/2018/QH14 ngày 12 tháng 6 năm 2018;
- Luật Dữ liệu số 60/2024/QH15 ngày 30 tháng 11 năm 2024;
- Nghị định số 13/2023/NĐ-CP ngày 17 tháng 4 năm 2023 của Chính phủ về bảo vệ dữ liệu cá nhân;
- Nghị định số 69/2024/NĐ-CP ngày 25 tháng 6 năm 2024 của Chính phủ quy định về định danh và xác thực điện tử;
- Thông tư số 13/2025/TT-BTC ngày 19 tháng 3 năm 2025 của Bộ trưởng Bộ Tài chính quy định mức thu, chế độ thu, nộp, quản lý và sử dụng phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư chữ ký số.
- ...

Tổ chức, cá nhân có trách nhiệm cung cấp thông tin phục vụ công tác đấu tranh, phòng, chống tội phạm lợi dụng dịch vụ để thực hiện các hành vi vi phạm pháp luật.