CÔNG TY CỔ PHẦN CÔNG NGHỆ SAVIS

PHỤ LỤC 03

QUY CHẾ - CHÍNH SÁCH CHỨNG THỰC

DỊCH VỤ ĐÓNG DẤU THỜI GIAN TRUSTCA - QUALIFIED TIMESTAMPING CA

Phiên bản: v1.0

Hà Nội, năm 2021

MỤC LỤC

1 Giới thiệu

Công ty Cổ phần Công nghệ SAVIS (SAVIS) là một trong những công ty công nghệ hàng đầu trong khu vực với đội ngũ chuyên môn có kinh nghiệm, tâm huyết, sáng tạo và tài năng; chuyên cung cấp các sản phẩm, giải pháp và dịch vụ công nghệ thông tin cho các khách hàng thuộc khối Chính phủ, Tài chính - Ngân hàng, Truyền hình - Viễn thông, Y tế, Giáo dục...

Công ty SAVIS là một trong số những doanh nghiệp được Bộ Thông tin và Truyền thông lựa chọn cấp phép trở thành đơn vị cung cấp dịch vụ chứng thực chữ ký số. TrustCA là tên gọi của dịch vụ chứng thực chữ ký số công cộng do Công ty Cổ phần Công nghệ SAVIS (SAVIS) cung cấp. SAVIS có đầy đủ thẩm quyền cấp chứng thư số cho các tổ chức, doanh nghiệp, cá nhân có yêu cầu xin cấp và sử dụng chứng thư số.

Văn bản này là một bộ quy chế chứng thực (CPS) tuyên bố về mặt nguyên tắc các chính sách (CP) quản trị của TrustCA Time Stamping Authority (TrustCA TSA) trong quá trình cung cấp dịch vụ cung cấp dấu thời gian điện tử đủ tiêu chuẩn.

Bản CP/CPS đưa ra các yêu cầu pháp lý, các yêu cầu về kỹ thuật, cũng như yêu cầu kinh doanh cho hỗ trợ các xác nhận bằng chứng chứng minh rằng một bản ghi điện tử đã tồn tại trước một thời điểm cụ thể. Các dịch vụ này có thể được sử dụng để hỗ trợ cho các dịch vụ chống chối bỏ, để chứng minh rằng chữ ký điện tử đã được tạo trong thời gian hiệu lực của chứng chỉ khóa công khai, để hỗ trợ lưu trữ điện tử dài hạn... Các yêu cầu của CP/CPS đảm bảo tính bảo mật và toàn vẹn cho dịch vụ TrustCA Time Stamping Authority, được áp dụng cho tất cả các thành phần tham gia dịch vụ chứng thực chữ ký số TrustCA.

Bản CP/CPS này không phải thỏa thuận về mặt luật pháp giữa SAVIS và các thực thể sử dụng dịch vụ chứng thực chữ ký số công cộng.

Dịch vụ cung cấp dấu thời gian của TrustCA TSA có thể được truy cập qua đường link: https://tsa.trustca.vn/

Dấu thời gian điện tử đủ điều kiện tuân thủ các yêu cầu sau:

- Gắn kết ngày giờ với thông điệp điện tử, thông qua phương pháp có khả năng xác định bất cứ thay đổi nào đối với thông điệp điện tử
- Dựa trên nguồn thời gian chính xác liên kết với Giờ Quốc tế Phối hợp Coordinated Universal Time (UTC); Tuân thủ theo quy định quốc gia về nguồn thời gian chuẩn quốc gia, đồng bộ theo múi giờ Việt Nam theo ISO 8601.
- Được ký với một chữ ký số đảm bảo hoặc đủ điều kiện; hoặc được đóng dấu với một dấu thời gian đảm bảo hoặc đủ điều kiện của TrustCA Time Stamping Authority với tư cách là một nhà cung cấp dịch vụ chứng nhận dấu thời gian đủ điều kiện.

2 Phạm vi

Dịch vụ TrustCA Time Stamping Authority được áp dụng cho tất cả các thành phần tham gia dịch vụ chứng thực chữ ký số TrustCA.

Việc cung cấp dấu thời gian điện tử đủ điều kiện dựa trên cơ sở hạ tầng với khóa công khai, nguồn thời gian an toàn và chứng chỉ định dạng X.509.

3 Sự tuân thủ và tài liệu tham khảo

Tài liệu này tuân thủ theo các tiêu chuẩn và tài liệu tiêu chuẩn hóa, thủ tục, chỉ thị,

luật pháp quốc gia và Quy định về dịch vụ nhận dạng và chứng nhận điện tử trong các giao dịch điện tử bao gồm:

- Tiêu chuẩn Dịch vụ dấu thời gian đã được tổ chức Tiêu chuẩn hóa quốc tế ISO/IEC ban hành năm 2002 theo bộ tiêu chuẩn ISO/IEC 18014: Công nghệ thông tin - Kỹ thuật an toàn - Dịch vụ dấu thời gian, bao gồm: Phần 1: Khung tổng quát; phần 2: Cơ chế tạo thẻ độc lập; phần 3: Cơ chế tạo thẻ có liên kết.
- Bên cạnh đó một số tổ chức khác cũng đã ban hành các tiêu chuẩn liên quan tới dịch vụ dấu thời gian, chẳng hạn như RFC 3161: Giao thức dấu thời gian (2001) và RFC 3628: Các yêu cầu về chính sách đối với Tổ chức cấp dấu thời gian (2003) của IETF (Internet Engineering Tast Force). Trong hệ thống các tiêu chuẩn của Mỹ, dịch vụ dấu thời gian cũng chỉ được đề cập tới trong một phần của Tiêu chuẩn FIPS PUB 186-3: Chữ ký số của NIST.
- Tại Việt Nam, cùng với Tiêu chuẩn về Chữ ký số, Mã hóa dữ liệu, Quản lý khóa, Tiêu chuẩn Dịch vụ dấu thời gian sẽ góp phần thống nhất việc thực hiện, đánh giá tính an toàn trong các giao dịch điện tử và là những công cụ thuận lợi để nâng cao tính pháp lý của các giao dịch trong môi trường điện tử. Dịch vụ dấu thời gian đã bước đầu được ứng dụng trong một số hoạt động giao dịch điện tử của nhiều tổ chức trong nước. Bởi vậy, theo đề xuất của Ban Cơ yếu Chính phủ, ngày 31/12/2007 Bộ trưởng Bộ Khoa học - Công nghệ đã có quyết định số 3223/QĐ-BKHCN về việc công bố các Tiêu chuẩn Quốc gia về Mật mã, trong đó có các Tiêu chuẩn về dịch vụ dấu thời gian là TCVN 7818-1: 2007 – Công nghệ thông tin - Kỹ thuật mật mã - Dịch vụ dấu thời gian, Phần 1: Khung tổng quát (dựa hoàn toàn theo tiêu chuẩn ISO/IEC 18014 –1) và TCVN 7818-2:2007, Công nghệ thông tin - Kỹ thuật mật mã – Dịch vụ dấu thời gian; Phần 2: Các cơ chế tạo thẻ độc lập (dựa hoàn toàn theo tiêu chuẩn ISO/IEC 18014 – 2). Phần dưới đây của bài báo giới thiệu nội dung cơ bản của 2 Tiêu chuẩn này.
- Nghị định 165/2018/NĐ-CP về giao dịch điện tử trong hoạt động tài chính
- Thông tư 41/2017/TT-BTTTT của Bộ Thông tin và Truyền thông: Quy định sử dụng chữ ký số cho văn bản điện tử trong cơ quan nhà nước
- Nghị định số 130/2018/NĐ-CP quy định chi tiết thi hành luật Giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số

Ngoài ra hệ thống Time Stamping Authority của chúng tôi cũng tuân thủ theo các tiêu chuẩn quốc tế như:

- eIDAS: Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
- ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
- ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".
- ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping

protocol and timestamp token profiles".

- IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".
- ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".
- ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service provider issuing EU qualified certificates".

4 Định nghĩa và từ viết tắt

4.1. Định nghĩa

Thuật ngữ	Giải thích
Coordinated Universal Time (UTC)	Giờ Phối hợp Quốc tế được hiểu là một tiêu chuẩn quốc tế về thời gian toàn cầu được báo cáo theo Khuyến nghị ITU-R TF.460-6 [1];
Network Time Protocol (NTP)	Một giao thức mạng được sử dụng bởi các chương trình đồng bộ hóa thời gian trên một hệ thống hoặc một mạng lưới các hệ thống thông tin;
Electronic time stamp (Time-Stamp)	Dữ liệu ở dạng điện tử liên kết các dữ liệu khác ở dạng điện tử tại một thời điểm cụ thể và thể hiện bằng chứng cho thấy dữ liệu mới nhất tồn tại vào thời điểm đó;
Qualified Electronic Time-stamp	Dấu thời gian điện tử đáp ứng các yêu cầu của Quy định (EU) số 910/2014;
TrustCA (Trust Certification Authority)	Hệ thống cung cấp dịch vụ chứng thực chữ ký số TrustCA
TrustCA Time Stamping Authority (TrustCA TSA)	Một đơn vị cơ sở hạ tầng nội bộ của TrustCA phát hành dấu thời gian điện tử đủ điều kiện;
Qualified Time-Stamping Service (TSS)	Dịch vụ xác minh ngày và giờ nộp tài liệu điện tử;
Time-Stamp token profiles (TST)	Đối tượng thông tin được xác định trong đề xuất IETF RFC 3161 (Profile của chứng thư "TrustCA TSA" được ký số nhằm chứng minh cho sự tồn tại của thông điệp dữ liệu thuộc tài liệu điện tử trước một thời điểm xác định (thời điểm được đề cập trên chứng thư); và đảm bảo tính toàn vẹn của nội dung sau thời điểm ấy. TST được đính kèm với chữ ký điện tử/chữ ký số, và chứng thư đảm bảo tính chống chối bỏ của chữ ký tại mốc thời gian ký);
Time-Stamping Unit (TSU)	Phần cứng và phần mềm được định cấu hình được quản lý như một hệ thống hợp nhất và có khóa bí

	mật / khóa riêng để ký trong quá trình cung cấp Dịch vụ chứng nhận dấu thời gian đủ điều kiện.
Long term	Thời gian lưu trữ đủ dài, liên quan đến thời gian có thể thay đổi công nghệ (trong thuật toán mật mã, kích thước khóa, hàm băm) hoặc của công nghệ lưu trữ
E-document	Một tài liệu điện tử có chứa ít nhất một chữ ký hoặc con dấu điện tử phù hợp với Quy định của eIDAS. Tùy thuộc vào loại tài liệu điện tử, nó có thể chứa các tài liệu điện tử bổ sung và hồ sơ tương ứng (siêu dữ liệu), chữ ký, chữ ký và dấu thời gian
Archive	Cơ sở dữ liệu để lưu trữ các đối tượng dữ liệu trong các container lưu trữ với (các) mục đích cụ thể và các thành phần liên quan (hệ thống máy tính, liên kết truyền thông, cung cấp điện, hệ thống an ninh và phòng cháy chữa cháy và vật lý và dự phòng của chúng)
Subscribers	Một người hoặc tổ chức ký thỏa thuận dịch vụ với Nhà cung cấp để sử dụng DỊCH VỤ
Submitter	Người gửi tài liệu điện tử đến DỊCH VỤ, người có thể khác với Người đăng ký, nhưng có quyền (quyền truy cập) để sử dụng DỊCH VỤ
Preservation mechanism	một cơ chế được sử dụng để lưu trữ tài liệu điện tử

4.2. Từ viết tắt

1. TSA - Time-Stamping Authority;
2. TSS - Time-Stamping Service;
3. TSU - Time-Stamping Unit;
4. TST - Time-stamp Token;
5. UTC - Coordinated Universal Time;
6. PKI - Public Key Infrastructure;
7. LTANS - Long-Term Archive and Notary Services;
8. LTV - Long Term Validation.

5 Khái niệm chung

5.1. Time Stamping Services

Việc trao đổi dữ liệu trong cơ sở hạ tầng của TrustCA TSA, được sử dụng để phát hành và quản lý dấu thời gian điện tử đủ điều kiện, bao gồm hai thành phần chính:

1. Hệ thống công nghệ phát hành dấu thời gian điện tử đủ điều kiện, duy trì hồ sơ và lưu trữ mã thông báo thời gian được tạo cho dấu thời gian điện tử;

2. Hệ thống quản lý, theo dõi và kiểm soát các hoạt động nhận yêu cầu trực tuyến, phát hành, kiểm tra và phê duyệt mã thông báo đã phát hành cho dấu thời gian điện tử bao gồm cả đồng bộ hóa với nguồn thời gian tham chiếu UTC

5.2. Mục tiêu lưu trữ dài hạn (Long-term preservation goals)

Các kế hoạch lưu trữ dài hạn được trình bày trong tài liệu này đề cập đến các mục tiêu sau:

- Bằng chứng về tính toàn vẹn của một tài liệu điện tử;
- Bằng chứng về sự tồn tại của một tài liệu điện tử (tại một thời điểm / trong quá khứ);
- Duy trì trạng thái hiệu lực của chữ ký điện tử / con dấu trong thời gian dài. Tính toàn vẹn dữ liệu được xác minh trong thời gian lưu trữ bằng bằng chứng về tính toàn vẹn (hàm băm, chữ ký / dấu).

Sự tồn tại của một đối tượng kỹ thuật số tại một thời điểm cụ thể được duy trì bằng sự kết hợp của bằng chứng về tính toàn vẹn (tính đầy đủ) và dấu thời gian đủ điều kiện. Theo tài liệu này, hai loại đối tượng kỹ thuật số cơ bản mà DỊCH VỤ được sử dụng là:

- Tài liệu điện tử đã ký / đóng dấu (chữ ký bao bọc và chữ ký / con dấu), trong đó trạng thái hiệu lực phải được lưu giữ trong một thời gian dài;
- Chữ ký / con dấu tách rời và đối tượng kỹ thuật số liên quan (tài liệu / tệp).

Để duy trì trạng thái hiệu lực của chữ ký điện tử / con dấu, mỗi dữ liệu xác thực của chúng phải được lưu giữ, tính hợp lệ của tài khoản này sẽ hết hạn (không thể được đảm bảo) trong tương lai (chứng chỉ, thông tin đình chỉ / hủy bỏ - CRL, OCSP phản hồi, danh sách đáng tin cậy, vv).

Các mục tiêu bổ sung để lưu trữ có thể là nhận dạng của Nhà cung cấp dịch vụ, không thoái thác việc gửi các đối tượng kỹ thuật số cho DỊCH VỤ và bảo mật dữ liệu trong trao đổi. Các mục tiêu bảo tồn này (hiện tại) nằm ngoài phạm vi của Chính sách hiện tại.

DỊCH VỤ tạo bằng chứng lưu trữ được sử dụng để xác minh hiệu suất của các mục tiêu lưu trữ tương ứng cho các đối tượng kỹ thuật số được chỉ định.

5.3. Tài liệu điện tử (E-document) và container

Tài liệu điện tử là dữ liệu được xử lý bởi DỊCH VỤ cho mục đích lưu trữ dài hạn chữ ký / con dấu. Nó có thể là (các) đối tượng dữ liệu cơ bản (chữ ký bao bọc / chữ ký / con dấu), phải được lưu giữ hoặc siêu dữ liệu được nộp bởi Người gửi hoặc được chính dịch vụ thu thập và thêm vào. Nhiều tài liệu điện tử có thể được kết hợp vào một container.

Các container lưu trữ có thể bao gồm:

- nhiều hơn một tài liệu điện tử;
- nhiều tài liệu điện tử được liên kết cục bộ - ví dụ, trong một lần gửi / gửi hoặc được lưu trong một thư mục của Người gửi.

Các đối tượng kỹ thuật số được thêm vào bởi DỊCH VỤ có thể là các chứng chỉ về CA, phản hồi CRL / OCSP-, chữ ký / con dấu, tem thời gian, bằng chứng, báo cáo xác nhận.

Không phải tất cả các tài liệu điện tử nên được gửi cùng nhau để lưu trữ.

Một container lưu trữ cơ bản chỉ chứa một tài liệu điện tử (nghĩa là nó giải quyết ít nhất một mục tiêu lưu trữ).

Người gửi là chủ thể gửi tài liệu điện tử đến DỊCH VỤ. DỊCH VỤ tạo POCID (mã định danh vùng chứa), được trả lại cho Người gửi (nếu DỊCH VỤ bao gồm lưu trữ). POCID là một định danh duy nhất của bộ lưu trữ. Nó được tạo trên cơ sở hàm băm, tức là nó là mã băm với một định danh cụ thể của thuật toán băm.

5.4. Time Stamping Authority

Cơ quan đóng dấu thời gian TrustCA TSA chịu trách nhiệm cung cấp Dịch vụ đóng dấu thời gian đủ điều kiện như được mô tả trong tài liệu này. TrustCA TSA phát hành Dấu thời gian đủ điều kiện theo phân cấp sau:

- **Hệ thống cung cấp dịch vụ ký số đóng đấu thời gian**

Cấp 1: Root CA

CN = Vietnam National Root CA
OU = National Centre of Digital Signature Authentication
O = Ministry of Information and Communications
C = VN

Cấp 2:TrustCA Qualified Timestamping CA(TSA01)

CN = TrustCA Qualified Timestamping CA
OU = TrustCA Time Stamping Authority
O = SAVIS TECHNOLOGY GROUP
S = Hà Nội
C = VN

6 Chính sách của Time Stamp

6.1. Yêu cầu chung

Chính sách này quy định bộ quy tắc mà TrustCA TSA tuân thủ khi phát hành dấu thời gian tiêu chuẩn, đảm bảo cung cấp thời gian chính xác so với Giờ quốc tế phối hợp (UTC) chính xác đến 0,5 giây. TrustCA TSA đảm bảo:

1. Công bố cổng truy cập để tiếp nhận và xác minh chứng thư cho dấu thời gian đã cấp;
2. Các biện pháp an ninh thích hợp được áp dụng, phù hợp với thông lệ quốc tế;
3. Hồ sơ mã thông báo đóng dấu thời gian (Time-stamp token - TST) tuân thủ tiêu chuẩn ETSI EN 319 422;
4. Các dấu thời gian được phát hành phải tuân thủ khuyến nghị RFC 3161. Dịch vụ xác minh thời gian tiêu chuẩn sẽ phát hành dấu thời gian điện tử đủ điều kiện được mã hóa RSA 2048-bit sử dụng thuật toán SHA256
5. Thời hạn chứng thư số TrustCA Timestamping CA (TSA01) có hiệu lực theo chu kỳ là 05 năm.

Chứng thư số của TrustCA TSA sử dụng để xác minh dấu thời gian điện tử trong TST đã ban hành là:

TSA01

Base Certificate		
Version	3	
Serial number	Defined by the CA software.	
Issuer	CN = Vietnam National Root CA OU = National Centre of Digital Signature Authentication O = Ministry of Information and Communications C = VN	
Validity Period	5 years	
Subject	CN = TrustCA Qualified Timestamping CA OU = TrustCA Time Stamping Authority O = SAVIS TECHNOLOGY GROUP S = Hà Nội C = VN	
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)
	Key size	2048
Signature (algorithm	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Authority Info Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://rootca.gov.vn/crt/vnrca256.p7b	
CRL Distribution Points (Non Critical)	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=https://rootca.gov.vn/crl/vnrca256.crl	
Basic Constaints (Critical)	Subject Type=End Entity Path Length Constraint=0	
Key Usage (Critical)	Digital Signature (80), Non-Repudiation (c0)	
Enhanced Key Usage (Critical)	Time Stamping (1.3.6.1.5.5.7.3.8)	

6.2. Cộng đồng người dùng và khả năng áp dụng

Chính sách của Cơ quan chứng nhận dấu thời gian hướng tới việc thực hiện các yêu cầu đối với dấu thời gian đủ điều kiện có thời hạn hiệu lực dài hạn (ETSI EN 319 122 [6]),

Tài liệu này không chỉ định bất kỳ giới hạn nào về khả năng áp dụng mã thông báo cho dấu thời gian điện tử (TST), được ban hành tuân thủ chính sách này.

Dịch vụ Chứng nhận Dấu thời gian đủ điều kiện cho phép chứng nhận ngày và giờ cung cấp chữ ký điện tử / dấu thời gian của mọi tài liệu được ký bằng chữ ký điện tử / tem

6.3. Sự tuân thủ

Hệ thống TSA được thiết kế theo mô hình của một hệ thống PKI hiện đại với đầy đủ các thành phần cần thiết, sử dụng sản phẩm TSA của hãng Ascertia là một trong các hãng hàng đầu về dịch vụ ký số, dịch vụ tin cậy trên thế giới hiện nay tuân thủ theo tiêu chuẩn

an toàn cao nhất cũng như các tiêu chuẩn của châu âu eIDAS về dịch vụ ký số từ xa, dịch vụ ký số nâng cao, ký cho lưu trữ điện tử lâu dài… và là đơn vị đầu tiên trên thế giới đạt chứng nhận bảo mật EN 419241- 1:2018 và EN 419241- 2:2019 cho Module SAM của máy chủ Server Signing của liên minh châu Âu.

7 Nghĩa vụ và trách nhiệm pháp lý

7.1. Nghĩa vụ

7.1.1. Nghĩa vụ chung

Nhà cung cấp dịch vụ TrustCA TSA hoạt động với chính sách và tuân thủ theo các yêu cầu trong bản CPS này.

Mọi thay đổi trong Chính sách này đều phải đảm bảo tuân thủ đúng quy định của pháp luật Việt Nam về dịch vụ chứng thực chữ ký số công cộng, phù hợp với tiêu chuẩn RFC 3647, và đảm bảo không ảnh hưởng đến quyền lợi của thuê bao.

Sự phê chuẩn được thực hiện bởi Tổng Giám Đốc Công ty Cổ phần Công nghệ SAVIS.

- Các thay đổi, cập nhật của quy chế chứng thực được ghi lại, công bố tại https://www.trustca.vn/repository/updates

TrustCA TSA sẽ tuân thủ kiểm toán. Ngoài ra TrustCA TSA thực hiện tự đánh giá hoạt động của hệ thống ít nhất mỗi năm một lần

7.1.2. Nghĩa vụ với thuê bao

TrustCA TSA đảm bảo cung cấp liên tục cho Dịch vụ chứng nhận dấu thời gian đủ điều kiện (24/7/365), ngoại trừ thời gian bảo trì kỹ thuật thường xuyên của hệ thống công nghệ.

Nhà cung cấp đảm bảo quyền truy cập công khai để nhận và kiểm tra mã thông báo dấu thời gian đủ điều kiện đã ban hành. Dịch vụ phát hành dấu thời gian điện tử đủ điều kiện có độ chính xác lên tới 0,5 giây và đảm bảo tính chính xác của người dùng, ngay cả trong nhiều kết nối cùng một lúc.

Ngoài ra, TrustCA TSA đảm bảo rằng:

- Sử dụng thiết bị công nghệ đáng tin cậy và an toàn (phần cứng và phần mềm) để cung cấp dịch vụ chứng nhận đủ điều kiện;
- Tiến hành các hoạt động theo pháp luật;
- Mã thông báo dấu thời gian điện tử được phát hành (TST) không chứa bất kỳ dữ liệu hỏng hoặc lỗi sai nào;
- Không vi phạm giấy phép, quyền sở hữu trí tuệ hoặc các quyền khác trong mã thông báo dấu thời gian điện tử đã ban hành (TST);
- Không cho phép sửa đổi dữ liệu kỹ thuật số sau khi phát hành mã thông báo dấu thời gian (TST), mà không thiết lập nó

7.1.3. Nghĩa vụ thuê bao sử dụng dịch vụ

Người dùng có nghĩa vụ kiểm tra tính hợp lệ của chữ ký điện tử của Cơ quan chứng nhận dấu thời gian và / hoặc Danh sách thu hồi chứng chỉ (CRL) khi trích xuất mã thông báo dấu thời gian (TST).

- Đường dẫn công bố thông tin chứng thư số bị thu hồi

https://rootca.gov.vn/crl/vnrca256.crl

7.1.4. Nghĩa vụ của các bên liên quan

Bên liên quan cần có kiến thức kỹ thuật tối thiểu cần thiết để sử dụng dịch vụ Chứng nhận Dấu thời gian đủ điều kiện. Nghĩa vụ chính của các bên có liên quan là kiểm tra chữ ký trên mã thông báo dấu thời gian điện tử (TST). Bên liên quan cần kiểm tra tính hợp lệ của Chứng thư cấp phát bởi Cơ quan chứng nhận dấu thời gian (TrustCA TSA), cũng như thời hạn hiệu lực của chứng thư này. Trong trường hợp kiểm tra dấu thời gian, sau khi hết thời hạn hiệu lực của Chứng thư cấp bởi của TrustCA TSA, các bên liên quan nên:

- Thực hiện kiểm tra Danh sách thu hồi chứng thư (CRL) của chứng thư cấp phát bởi Cơ quan chứng nhận dấu thời gian (TrustCA TSA);
- Kiểm tra khả năng ứng dụng của thuật toán băm đã sử dụng;
- Đảm bảo tính bảo mật của chữ ký điện tử đã sử dụng bằng cách kiểm tra sự kết hợp áp dụng của thuật toán băm không đối xứng và hàm băm.

7.2. Trách nhiệm pháp lý

Được qui định cụ thể khi chính thức cung cấp dịch vụ.

7.2.1. Bồi thường bởi chủ thể cuối cùng

Trong phạm vi của luật áp dụng, thỏa thuận chủ thể cuối cùng và các thỏa thuận khác yêu cầu chủ thể cuối cùng bồi thường cho TrustCA TSA và cho các tổ chức CA không phải là TrustCA TSA trong các trường hợp:

- Chủ thể cuối cùng xuyên tạc sự thật trong đơn đăng ký cấp chứng thư số.
- Chủ thể cuối cùng vi phạm tiết lộ những tài liệu trên đơn xin cấp chứng thư số, nếu những thông tin sai lệch hoặc bỏ sót do sự cẩu thả hay do cố ý để đánh lừa bất kỳ tổ chức nào.
- Chủ thể cuối cùng thiếu sót trong việc bảo vệ khóa riêng, hoặc trong những hành động cảnh báo cần thiết để chống lại việc tiết lộ, mất mát, sửa chữa

hoặc sử dụng trái phép khóa riêng của chủ thể cuối cùng hoặc sử dụng tên của chủ thể cuối cùng (bao gồm, không giới hạn bởi tên thường dùng, hoặc địa chỉ email) xâm phạm quyền sở hữu trí tuệ của bên thứ ba.

7.2.2. Bồi thường do RP

Trong phạm vi của luật áp dụng, thỏa thuận RP và các thỏa thuận khác yêu cầu RP bồi thường cho TrustCA TSA và thuê bao của TrustCA TSA về

- RP thiếu sót trong việc thực hiện các nghĩa vụ của RP;
- Sự tin tưởng của RP vào chứng thư số không phù hợp trong một số trường hợp; hoặc
- RP thiếu sót trong việc kiểm tra tình trạng của chứng thư số để xác định xem liệu chứng thư số đó đã hết hạn hay bị thu hồi hay chưa.

8 Các yêu cầu đối với Time Stamp Authority

8.1. Quản lý vòng đời khóa và chứng thư số

8.1.1. Khởi tạo cặp khóa TSA

TrustCA TSA sẽ tổ chức buổi lễ tạo khóa để tiến hành sinh cặp khóa vào HSM thông qua phần mềm TSA và tạo yêu cầu cấp chứng thư số gửi NEAC.

Sau khi nhận được yêu cầu xin cấp phát chứng thư số, NEAC sẽ kiểm tra lại thông tin yêu cầu. Sau khi được phê duyệt, NEAC sẽ tiến hành cấp chứng thư số từ yêu cầu trên và gửi lại cho nhà cung cấp dich vụ.

Sau khi nhận được chứng thư số do NEAC cấp, TrustCA TSA sẽ import chứng thư số đó vào trong hệ thống TrustCA TSA để hoàn thành quá trình khởi tạo chứng thư số.

8.1.2. Bảo vệ khóa riêng

8.1.2.1. Tiêu chuẩn đối với mô đun mã hóa

TrustCA TSA sử dụng HSM của hãng nCipher -Thales XC Base Network đạt chuẩn EN 419221- 5:2018/ EAL4+ AVAN_ VAN.5 mới nhất cho chuẩn an toàn quản lý khóa của nhà cung cấp dịch vụ eIDAS và Thông tư 16/2019/TT-BTTTT cho Quản lý mật mã trên thiết bị phần cứng phục vụ khởi tạo khoá mật mã TSA, sinh chữ ký TSA, xác nhận, lưu trữ và sao lưu / phục hồi khoá TSA..

8.1.2.2. Kiểm soát khóa riêng nhiều người dùng

TrustCA TSA áp dụng xác thực nhiều lớp sử dụng thẻ thông minh (xác thực n thẻ / 1 quyền) mỗi khi quản trị và khởi động hệ thống mật mã.

8.1.2.3. Quá trình đưa Private key vào môđun mã hóa

Quá trình tạo khóa sẽ được thực hiện qua các bước: khởi tạo kích hoạt thiết bị mã hóa phần cứng (token), thông qua phần mềm quản trị cho việc tạo khóa để thực hiện tạo cặp khóa trực tiếp vào thiết bị mã hóa. Hệ thống TrustCA TSA sử dụng các thuật toán RSA- 2048 cho việc tạo khóa và AES-256 cho việc mã hóa khóa bí mật.

Thiết bị mã hóa đạt tiêu chuẩn bảo mật EN 419221- 5:2018/ EAL4+ AVAN_ VAN.5

Khóa riêng chỉ có thể chuyển ra khỏi thiết bị mã hóa khi thực hiện quá trình sao lưu khóa riêng và không thể tồn tại bên ngoài thiết bị mã hóa ở bất cứ thời gian nào.

8.1.2.4. Lưu trữ khóa riêng trên môđun mã hóa

Quy trình lưu trữ khóa riêng vào môđun mã hóa được tiến hành theo hướng dẫn của nhà cung cấp thiết bị và tuân theo chuẩn do Bộ Thông tin và Truyền thông ban hành.

8.1.2.5. Phương pháp kích hoạt khóa riêng

Việc kích hoạt được thực hiện bởi mã số PIN. Khi không hoạt động, các khóa riêng phải được đặt trong môi trường mã hóa hoàn toàn

8.1.2.6. Phương pháp làm khóa riêng ngừng hoạt động

Các môđun mã hóa không được kích hoạt khi không có sự giám sát hoặc khi tự do truy cập. Sau khi sử dụng, chúng phải ngừng hoạt động, ví dụ sử dung một thủ tục hướng dẫn thoát ra bằng tay hoặc một chương trình tự ngừng hoạt động sau một khoảng thời gian. Khi không sử dụng, phần cứng môđun mã hóa sẽ được gỡ bỏ và lưu trữ, trừ khi chúng hoàn toàn nằm trong sử kiểm soát của chủ thể cuối cùng.

8.1.2.7. Phương pháp hủy bỏ khóa riêng

Các khóa riêng sẽ được hủy bỏ khi chúng không cần thiết, hoặc khi các chứng thư số tương ứng hết hạn hoặc bị thu hồi. Đối với phần mềm môđun mã hóa, việc phá hủy có thể thực hiện bằng cách ghi đè lên dữ liệu. Với Token, điều này được thực hiện bằng cách thực hiện một lệnh "zeroize". Sự phá hủy có tính chất vật lý sẽ không được áp dụng.

8.2. TIME-STAMPING

8.2.1. Time-stamp Token

Mỗi mã thông báo dấu thời gian điện tử (TST) do TrustCA TSA phát hành bao gồm một mã định danh duy nhất về chính sách của Cơ quan chứng nhận dấu thời gian.

Cấu hình yêu cầu / trả lời của hệ thống TrustCA TSA Cảnh tuân thủ các thông số kỹ thuật được mô tả ở trên và bao gồm các thuộc tính / tham số sau:

- Yêu cầu phát hành TST (TSQ) bao gồm:

Field	Attributes	Meaning/Value
Message Imprint	Thuật toán băm	OID của hàm băm SHA1, SHA-256
	Giá trị băm	Giá trị băm của dữ liệu
Nonce		Tùy chọn
Certificate Request		nếu đó là TRUE, Dịch vụ TSA sẽ từ chối các yêu cầu dấu thời gian không chứa trường cert certReq.
Extension		Không sử dụng

- TST trả lời yêu cầu (TSR) bao gồm:

Field	Attributes	Meaning/Value
Message Imprint	Thuật toán băm	OID của hàm băm SHA1, SHA-256
	Giá trị băm	Giá trị băm của dữ liệu
Serial Number		Serial number của chứng thư số
Thời gian khởi		Thời gian cung cấp chữ ký điện tử / tem

tạo		(Thời gian chứng nhận UTC)
Độ chính xác		500ms
Extension		Không sử dụng
Nonce		Chỉ khi có mặt trong yêu cầu
TSA		DN=[CN = TrustCA Qualified Timestamping CA, OU = TrustCA Time Stamping Authority, O = SAVIS TECHNOLOGY GROUP, S = Hà Nội, C = VN]
Extensions		Không sử dụng

8.2.2. Đồng bộ thời gian với UTC

TrustCA TSA luôn đồng bộ hóa tự động với nguồn thời gian UTC, dựa trên giao thức NTP, sau khi thiết lập tham chiếu tới nguồn thời gian quy chuẩn quốc gia do Tổng cục Tiêu chuẩn Đo lường Chất lượng (STAMEQ) quản lý

8.3. Kiểm soát vận hành, quản lý và thiết bị

8.3.1. Quản lý nhân sự

Tất cả các vấn đề liên quan đến quản lý nhân sự được mô tả trong mục *6.3 Quản lý nhân sự* tài liệu *Quy chế chứng thực dịch vụ Chứng thực chữ ký số công cộng TrustCA* theo các quy định về:

- Phẩm chất, kinh nghiệm và sự tin tưởng;
- Thủ tục kiểm tra lý lịch của nhân sự;
- Đào tạo nhân sự tham gia vào quản lý, vận hành hệ thống và tần suất đào tạo thường xuyên;
- Kỉ luật đối với những hành vi vi phạm;

8.3.2. Quản lý an ninh

TrustCA TSA triển khai và duy trì chính sách bảo mật thông tin. Tất cả nhân viên có nghĩa vụ tuân thủ các tiêu chuẩn của chính sách này. Chính sách bảo mật thông tin được xem xét và cập nhật một cách thường xuyên và trong trường hợp có phát sinh sự cố.

Tất cả các vấn đề liên quan đến quản lý bảo mật được mô tả trong mục *10.3 Bảo mật thông tin trong hoạt động TrustCA* tài liệu *Quy chế chứng thực dịch vụ Chứng thực chữ ký số công cộng TrustCA.*

8.3.3. Đánh giá rủi ro

Để đảm bảo cấp chất lượng và tính tin cậy của các dịch vụ được cung cấp, TrustCA TSA thường xuyên thực hiện các đánh giá rủi ro. Quy trình kiểm tra bảo mật được xác định trong khái niệm bảo mật của Nhà cung cấp được kiểm soát hàng quý để cung cấp hiệu quả kiểm soát.

Mô tả các quy trình và kế hoạch để đạt được tính liên tục và bảo mật cho các hoạt động của Nhà cung cấp được mô tả trong tài liệu Quy chế chứng thực dịch vụ Chứng thực chữ ký số công cộng TrustCA.

8.3.4. Kiểm soát hoạt động

TrustCA TSA thiết lập các chính sách và thủ tục kiểm soát đảm bảo có nhiều người tin tưởng thực hiện một công việc nhạy cảm như truy cập, điều khiển module phần cứng mã hóa.

Các chính sách và thủ tục kiểm soát này của TrustCA luôn đòi hỏi có ít nhất 2 người để thực hiện các công việc nhạy cảm.

Các đặc điểm và vai trò tin cậy của nhân viên và quản trị viên trong các hoạt động của Nhà cung cấp được mô tả trong tài liệu Quy chế chứng thực dịch vụ Chứng thực chữ ký số công cộng TrustCA.

8.3.5. Bảo mật vật lý

Việc tiến hành các hoạt động an toàn và đáng tin cậy của Cơ quan chứng nhận dấu thời gian (TrustCA TSA) được thực hiện bởi các cấp độ bảo mật khác nhau của quyền truy cập vật lý và logic vào hệ thống công nghệ.

Kiểm soát vật lý và kiểm soát truy cập tuân thủ theo mục *6.1.2 Truy cập vật lý* tài liệu *Quy chế chứng thực dịch vụ Chứng thực chữ ký số công cộng TrustCA.*

8.3.6. An ninh mạng

Dựa trên đánh giá rủi ro, cơ sở hạ tầng mạng được chia thành các khu vực, xem xét mối quan hệ chức năng, logic và vật lý giữa các hệ thống và dịch vụ đáng tin cậy. TrustCA TSA hạn chế quyền truy cập và liên lạc theo mức độ nhằm đảm bảo cho hoạt động bình thường của các dịch vụ chứng nhận. Các kết nối và dịch vụ liên quan đến các dịch vụ chứng nhận bị vô hiệu hóa. Các quy tắc cấp quyền truy cập được xem xét định kỳ.

Tất cả các thành phần của cơ sở hạ tầng quan trọng được được bảo vệ trong môi trường biệt lập.

Một mạng lưới quản trị được xây dựng và phân tách biệt lập với bởi mạng hạ tầng nhằm thực hiện tác vụ quản lý. Hệ thống trong mạng quản trị không được dùng để xử lý tác vụ khác.

Hạ tầng chạy thử và tìm lỗi được tách biệt khỏi các hạ tầng khác không có liên quan.

Kết nối với hệ thống tin cậy từ xa chỉ được thực hiện thông qua các kênh bảo mật, tách biệt với các kênh liên lạc khác và có hình thức định danh đầu cuối. Dữ liệu trên mạng lưới được bảo vệ, chống tiết lộ hoặc sửa đổi.

Kết nối Internet riêng biệt.

Các địa chỉ IP public để truy cập cũng thường xuyên được rò quét tìm các lỗ hổng bảo mật

Kiểm tra sự thâm nhập hệ thống được tiến hành trong các trường hợp sau: sau cài đặt ban đầu của hệ thống và sau cơ sở hạ tầng hoặc có sự thay đổi, nâng cấp các ứng dụng

8.4. Xử lý khi có sự cố và thảm họa

8.4.1. Các thủ tục kiểm soát sự cố và thảm họa

Các thông tin sau được backup đề phòng có sự cố và thảm họa: dữ liệu về đơn xin cấp chứng thư số, dữ liệu nhật ký, và các bản ghi chứng thư số được tạo ra. Khi có sự cố, các dữ liệu được phục hồi theo các thủ tục đã có.

8.4.2. Sự cố về máy tính, phần mềm và dữ liệu

Khi có các sự cố về máy tính, phần mềm và dữ liệu, các thủ tục xử lý sự cố được thực hiện. Mỗi sự cố sẽ có các quy trình xử lý khác nhau. Nếu sự cố nghiêm trọng, các thủ tục phục hồi sẽ được thực hiện

8.4.3. Thủ tục xử lý khi khóa bí mật bị làm mất/lộ

Khi khóa bí mật của TrustCA TSA nghi ngờ bị mất/lộ, CA sẽ thực hiện thủ tục xử lý khi khóa bị lộ. Nếu chứng thư số của TrustCA TSA bị thu hồi, các thủ tục sau sẽ được thực hiện:

- Trạng thái thu hồi chứng thư số của TrustCA TSA sẽ được công bố bởi RootCA.
- TrustCA TSA cố gắng thông báo cho toàn bộ người nhận trong hệ thống dừng sử dụng các dịch vụ cấp dấu thời gian do TrustCA TSA ban hành
- TrustCA TSA xin cấp chứng thư số mới từ RootCA và ban hành chứng thư số cho các thuê bao của mình để họ tiếp tục sử dụng.

8.4.4. Khả năng phục hồi hoạt động sau thảm họa

Luôn có hệ thống dự phòng và sẽ hoạt động khi có thảm họa xảy ra. Thời gian nhậm nhất để phục hồi là 8 giờ.