TCVN **TIÊU CHUẨN QUỐC GIA**

TCVN xxxx:2026

Xuất bản lần 1

GIAO DỊCH ĐIỆN TỬ - ỨNG DỤNG KÝ TRÊN MÁY CHỦ KÝ SỐ CHO MÔ HÌNH KÝ SỐ TỪ XA (REMOTE SIGNING)

Electronic transactions - Application of digital signature server-based signing for remote signing model

HÀ NỘI - 2026

Mục lục

Lời nói đầu

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

Giao dịch điện tử - Ứng dụng ký trên máy chủ ký số cho mô hình ký số từ xa (Remote signing)

Electronic transactions - Application of digital signature server-based signing for remote signing model

1 Phạm vi áp dụng

Tài liệu này quy định các yêu cầu và khuyến nghị về bảo mật đối với hệ thống dịch vụ tin cậy hỗ trợ ký số trên máy chủ (TW4S) tạo ra chữ ký số.

2 Tài liệu viện dẫn

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

TCVN 8709-1:2011 (ISO/IEC 15408-1:2009), “Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 1: Giới thiệu và mô hình tổng quát”.

TCVN 8709-2:2011 (ISO/IEC 15408-2:2008), “Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 2: Các thành phần chức năng an toàn”.

TCVN 8709-3:2011 (ISO/IEC 15408-3:2008), “Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 3: Các thành phần đảm bảo an toàn”.

TCVN 11295:2016 (ISO 19790:2012) về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu an toàn cho mô-đun mật mã (năm 2016).

Quy chuẩn kỹ thuật quốc gia QCVN 137:2025/BKHCN - Yêu cầu đối với dịch vụ chứng thực chữ ký số công cộng.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong TCVN 8709-1:2011 và các thuật ngữ sau:

3.1

Xác thực (authentication)

Cung cấp sự đảm bảo về danh tính của một chủ thể.

3.2

Yếu tố xác thực (authentication Factor)

Thông tin và/hoặc quy trình được sử dụng để xác thực hoặc kiểm chứng danh tính của một chủ thể.

3.3

Dữ liệu cần được ký xác nhận (data to be signed representation)

Dữ liệu được định dạng dùng để tính toán giá trị chữ ký số (ví dụ: giá trị băm).

3.4

Chữ ký số (digital signature)

Đơn vị dữ liệu được thêm vào, hoặc phép biến đổi mật mã của dữ liệu cho phép người nhận đơn vị dữ liệu chứng minh nguồn gốc và tính toàn vẹn của đơn vị dữ liệu, đồng thời bảo vệ chống lại sự giả mạo.

3.5

Hồ sơ bảo vệ (Protection Profile)

Một tập hợp các yêu cầu an toàn được xác định độc lập cho một dòng sản phẩm.

3.6

Thiết bị tạo chữ ký từ xa (remote signature creation device)

Thiết bị tạo chữ ký được sử dụng từ xa của người ký và áp dụng giao thức kích hoạt chữ ký để cung cấp quyền kiểm soát hoạt động ký thay mặt người ký, đồng thời đảm bảo với mức độ tin cậy cao đảm bảo các khóa ký được sử dụng dưới sự kiểm soát duy nhất của người ký.

3.7

Dữ liệu kích hoạt chữ ký (signature activation data)

Tập hợp dữ liệu được SAP thu thập, được sử dụng để kiểm soát với độ tin cậy cao một hoạt động ký số nhất định, được thực hiện bởi một mô-đun mật mã thay mặt người ký, và hoạt động này hoàn toàn nằm dưới sự kiểm soát của người ký.

Lưu ý 1 cho mục này: SAD có thể là kết quả của các hoạt động mã hóa (xem chi tiết trong mục 5.8)

3.8

Mô-đun kích hoạt chữ ký (signature activation module)

Phần mềm được cấu hình sử dụng SAD để đảm bảo với độ tin cậy cao rằng các khóa ký được sử dụng dưới sự kiểm soát duy nhất của người ký.

3.9

Giao thức kích hoạt chữ ký (signature activation protocol)

Giao thức thu thập SAD được sử dụng để kiểm soát hoạt động ký trên một tập hợp DTBS/R, sử dụng khóa ký của người ký.

3.10

Ứng dụng tạo chữ ký (signature creation application)

Ứng dụng tạo tài liệu có chữ ký, sử dụng chữ ký số được tạo bởi SCDev.

3.11

Dịch vụ tạo chữ ký (signature creation sevice)

Mô-đun mã hóa phần mềm và/hoặc phần cứng được cấu hình dùng để tạo chữ ký số.

3.12

Chính sách chữ ký (signature policy)

Chính sách tạo chữ ký, chính sách bổ sung chữ ký, chính sách xác thực chữ ký hoặc bất kỳ sự kết hợp nào của các chính sách đó, áp dụng cho cùng một chữ ký hoặc một tập hợp các chữ ký.

3.13

Người ký (signer)

Chủ thể (cá nhân hoặc pháp nhân) là người tạo ra chữ ký số.

3.14

Thành phần tương tác của người ký (signer’s interaction component)

Phần mềm và/hoặc thành phần phần cứng được người ký sử dụng để hỗ trợ SAP.

3.15

Khóa ký (signing key)

Khóa riêng của một cặp khóa mật mã bất đối xứng được sử dụng để tạo chữ ký số.

3.16

Tổ chức cung cấp dịch vụ tin cậy (trust service provider)

Một cá nhân hoặc pháp nhân cung cấp một hoặc nhiều dịch vụ tin cậy.

3.17

Hệ thống dịch vụ tin cậy hỗ trợ ký trên máy chủ (trustworthy system supporting server signing)

Hệ thống máy chủ-máy khách sử dụng khóa ký dưới sự kiểm soát của người ký để tạo chữ ký số.

4 Ký hiệu và chữ viết tắt

DTBS/R	Data To Be Signed Representation	Dữ liệu cần được ký xác nhận

EAL	Evaluation Assurance Level	Mức độ đảm bảo đánh giá
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission	Tổ chức Tiêu chuẩn hóa Quốc tế/ Ủy ban Kỹ thuật Điện Quốc tế
QSCD	Qualified Electronic Signature (or Electronic Seal)	Thiết bị tạo chữ ký điện tử (hoặc con dấu điện tử) đủ điều kiện
RA	Registration Authority	Tổ chức đăng ký
SAD	Signature Activation Data	Dữ liệu kích hoạt chữ ký
SAM	Signature Activation Module	Mô-đun kích hoạt chữ ký
SAP	Signature Activation Protocol	Giao thức kích hoạt chữ ký
SCA	Signature Creation Application	Ứng dụng tạo chữ ký
SCAL	Sole Control Assurance Level	Mức độ đảm bảo kiểm soát duy nhất
SCDev	Signature Creation Device	Thiết bị tạo chữ ký
SIC	Signer’s Interaction Component	Thành phần tương tác của người ký
SSA	Server Signing Application	Ứng dụng ký trên máy chủ
TSP	Trust Service Provider	Tổ chức cung cấp dịch vụ tin cậy
TW4S	Trustworthy System Supporting Server Signing	Hệ thống dịch vụ tin cậy

5 Mô tả các hệ thống dịch vụ tin cậy hỗ trợ ký trên máy chủ

5.1 Tổng quan

Điều khoản này mô tả các khái niệm khác nhau về việc ký trên máy chủ nhằm làm rõ cách thức thực hiện các yêu cầu bảo mật được nêu trong Điều 6.

5.2 Mục tiêu tạo chữ ký và ký trên máy chủ

Mục đích của TW4S là lấy Dữ liệu cần ký (DTBS/R) và tạo ra chữ ký số dưới sự kiểm soát của người ký.

5.3 Chữ ký gắn liền với cá nhân hoặc con dấu gắn liền với pháp nhân

Chữ ký số có thể được sử dụng để đại diện cho chữ ký điện tử hoặc con dấu điện tử.

Mức độ tin cậy trong việc kiểm soát khóa ký không nhất thiết phải giống nhau nếu chữ ký số được sử dụng để đại diện cho con dấu so với khi nó được sử dụng để đại diện cho chữ ký thông thường.

Chữ ký điện tử được tạo ra theo tiêu chuẩn này có thể được tạo ra dưới sự kiểm soát của cá nhân hoặc pháp nhân.

Trong tiêu chuẩn này, thuật ngữ "người ký" được sử dụng bao gồm cả cá nhân hoặc pháp nhân.

Thuật ngữ SCDev được sử dụng cho mục đích thuận tiện để bao gồm thiết bị tạo chữ ký hoặc thiết bị tạo con dấu.

5.4 Mức độ đảm bảo kiểm soát duy nhất

Tài liệu này xác định hai mức độ đảm bảo cho việc kiểm soát duy nhất:

— Mức độ đảm bảo kiểm soát duy nhất cấp 1 (SCAL1):

— Các khóa ký được sử dụng với mức độ tin cậy thấp, hoàn toàn nằm dưới sự kiểm soát của người ký.

— Việc người ký được ủy quyền sử dụng khóa của mình để ký được SSA thực thi và xác thực người ký.

— Mức độ đảm bảo kiểm soát duy nhất cấp 2 (SCAL2):

— Các khóa ký được sử dụng với độ tin cậy cao, hoàn toàn nằm dưới sự kiểm soát của người ký.

— Việc người ký được ủy quyền sử dụng khóa của mình để ký được SAM thực thi thông qua SAD do người ký cung cấp, sử dụng SAP, nhằm cho phép sử dụng khóa ký tương ứng.

Việc quyết định sử dụng mức độ đảm bảo kiểm soát duy nhất cấp 1 hay cấp 2 phụ thuộc vào chính sách chữ ký và các yêu cầu pháp lý hiện hành.

5.5 Ký trên máy chủ hàng loạt

Có thể ký một loạt tài liệu mà không yêu cầu người ký phải kiểm tra và phê duyệt rõ ràng từng tài liệu, hoặc có cơ hội kiểm tra chúng trước khi ký, chẳng hạn như cung cấp liên kết đến các tài liệu trong loạt đó thay vì phải chuyển từng tài liệu để kiểm tra và phê duyệt.

Điều này có nghĩa là người ký chỉ cần áp dụng các biện pháp kiểm soát duy nhất cho quá trình ký kết hàng loạt thay vì từng tài liệu riêng lẻ.

Vì tính hợp pháp của việc ký hàng loạt phụ thuộc vào môi trường pháp lý và ứng dụng, nên TW4S phải có các cấu hình cho phép hoặc không cho phép ký hàng loạt đối với chữ ký số.

5.6 Khóa ký và mô-đun mật mã

Để tạo chữ ký số ở cấp độ SCAL1 và đảm bảo tính linh hoạt cao, khóa ký (ví dụ: khóa riêng của cặp khóa bất đối xứng) không nhất thiết phải được tạo, lưu trữ và sử dụng bên trong một mô-đun mật mã (ví dụ: thiết bị bảo mật phần cứng hoặc thẻ thông minh). Khóa ký cũng có thể được lưu trữ trong một tệp và SCDev có thể là phần mềm sử dụng tệp đó.

Khi sử dụng các tập tin, cần phải triển khai các biện pháp bảo mật bên ngoài cụ thể, ngoài việc bảo vệ chính các tập tin đó khỏi bị can thiệp (xóa, sửa đổi).

Tuy nhiên, tiêu chuẩn này khuyến nghị rằng TW4S sử dụng các khóa ký được bảo vệ bởi môi trường chống giả mạo để tạo chữ ký số. Điều đó có nghĩa là SCDev phải là một mô-đun mật mã.

5.7 Xác thực người ký

5.7.1 Phương tiện nhận dạng điện tử

5.7.1.1 SCAL1

Việc đăng ký người ký và các đặc điểm cũng như yêu cầu thiết kế của phương tiện nhận dạng điện tử được xác định trong SRC_SA.1.1.

5.7.1.2 SCAL2

Việc đăng ký người ký và các đặc điểm cũng như yêu cầu thiết kế của phương tiện nhận dạng điện tử được xác định trong SRA_SAP.1.1.

5.7.2 Cơ chế xác thực

5.7.2.1 SCAL1

Các yêu cầu về cơ chế xác thực được định nghĩa trong SRC_SA.1.1.

5.7.2.2 SCAL2

Các yêu cầu về cơ chế xác thực được định nghĩa trong SRA_SAP.1.1.

5.7.3 Mục tiêu xác thực

5.7.3.1 SCAL1

— Người ký phải được xác thực thành công với SSA để được cấp quyền truy cập vào hoạt động ký điện tử, và

— Khóa ký của người ký phải được SSA liên kết với yếu tố xác thực của người ký.

5.7.3.2 SCAL2

— SAD phải được thiết lập, tính toán hoặc là kết quả của một tương tác bảo mật giữa SAM và SIC thông qua SSA, để ủy quyền cho hoạt động ký kết trong SCDev và

— SAD phải được truyền đến SAM thông qua SSA để ủy quyền cho hoạt động ký kết trong SCDev cho DTBS/R chuyên dụng.

5.7.4 Ủy quyền xác thực cho bên thứ ba

5.7.4.1 Tổng quan

Tổ chức cung cấp dịch vụ tin cậy (TSP) có thể ủy quyền quy trình xác thực cho bên thứ ba (ví dụ: tổ chức cung cấp định danh).

5.7.4.2 SCAL1

Tổ chức cung cấp dịch vụ tin cậy (TSP) phải đảm bảo rằng quy trình xác thực được ủy quyền cho bên ngoài đáp ứng các yêu cầu được quy định trong SRC_SA.1.1.

5.7.4.3 SCAL2

Tổ chức cung cấp dịch vụ tin cậy (TSP) phải đảm bảo rằng quy trình xác thực được ủy quyền cho bên ngoài đáp ứng các yêu cầu được quy định trong SRA_SAP.1.1.

Tổ chức cung cấp dịch vụ tin cậy (TSP) phải đảm bảo rằng:

— Bên thứ ba đáp ứng đầy đủ tất cả các yêu cầu liên quan của tiêu chuẩn này và các yêu cầu đăng ký theo quy định pháp luật hiện hành, hoặc

— Quá trình xác thực được ủy quyền cho bên thứ ba sử dụng phương tiện nhận dạng điện tử được cấp theo một chương trình đã được thông báo phù hợp với các yêu cầu pháp lý hiện hành.

5.8 Dữ liệu kích hoạt chữ ký

Để đạt được SCAL2, việc sử dụng SAD để đảm bảo quyền kiểm soát khóa của người ký phải được SAM thực thi. Việc kích hoạt chữ ký tại SCAL2 yêu cầu đáp ứng một số điều kiện như xác thực người ký và tính xác thực của yêu cầu thao tác ký từ người ký (chi tiết được nêu trong mục 5.7). Cả hai thuộc tính đều có thể được cung cấp trực tiếp bởi SAD. Tuy nhiên, ví dụ, cũng có thể thực hiện xác thực người ký trước khi tạo SAD, chẳng hạn như bằng cách sử dụng ủy quyền xác thực. SAD có thể là một tập hợp dữ liệu hoặc là kết quả của các hoạt động mã hóa (chi tiết được nêu trong SRA_SAP.2) từ đó có thể suy ra cùng một thông tin. SAD góp phần xác thực trực tiếp hoặc gián tiếp người ký.

Khi quá trình xác thực người ký diễn ra trước khi thu thập SAD, SAD phải chứa các mục để xác định người ký được đối chiếu bởi một nguồn đã biết. Nguồn đối chiếu này có thể đến từ SIC hoặc từ một tổ chức cung cấp định danh điện tử dịch vụ tin cậy. Nguồn đối chiếu phải được xác thực.

5.9 Giao thức kích hoạt chữ ký

Hệ thống SAP phải được thiết kế để cho phép sử dụng an toàn khóa ký để tạo chữ ký số do mô-đun mật mã thực hiện thay mặt người ký.

SAP là một giao thức trong đó người ký (thông qua SIC) và TW4S giao tiếp với nhau để tạo ra SAD.

Thiết kế của hệ thống SAP phải bao gồm tối thiểu các bước xác minh sau:

— Xác thực người ký khi sử dụng khóa ký,

— xác thực yêu cầu chữ ký với SAD cụ thể,

— Khóa ký đã chọn hợp lệ và đang hoạt động.

— Chuyển giao an toàn tất cả các thành phần của SAD.

Khi khóa ký không được sử dụng để ký xác nhận quyền sở hữu nhằm lấy chứng chỉ, hệ thống SAP phải bao gồm bước xác minh sau:

— Sự hiện diện của chứng chỉ hợp lệ liên kết với khóa ký.

5.10 Thành phần tương tác của người ký

SIC là một phần mềm và/hoặc phần cứng, được vận hành trên môi trường của người ký dưới sự kiểm soát hoàn toàn của người ký.

Việc sử dụng thành phần này là cần thiết trong quy trình SAP và để tạo chữ ký số bởi SCDev.

SIC luôn tham gia vào SAP để xác thực người ký hoặc tạo SAD:

— SIC có thể trực tiếp tạo SAD, hoặc

— Mã SIC có thể được sử dụng để xác thực người ký, và thông tin xác nhận người ký phải được sử dụng trong quá trình tạo SAD.

Thành phần này có thể là (hoặc sự kết hợp của):

— một ứng dụng được thực thi bởi trình duyệt (ví dụ: yêu cầu HTTP POST qua TLS),

— một ứng dụng được thực thi bởi thiết bị di động (ví dụ: điện thoại thông minh, máy tính bảng),

— một thành phần bảo mật của điện thoại di động (ví dụ: thẻ SIM nhận tin nhắn SMS),

— một thiết bị mã hóa thuộc sở hữu của người ký (ví dụ: thông qua VNeID, eToken, FIDO-Token),

— […]

SIC đảm bảo mối liên hệ giữa người ký và thao tác ký tên trong hệ thống SAP.

5.11 Mô-đun kích hoạt chữ ký

SAM là một phần mềm sử dụng SAD để đảm bảo với độ tin cậy cao rằng các khóa ký được sử dụng dưới sự kiểm soát duy nhất của người ký đối với SCAL2. SAM phải được sử dụng trong môi trường được bảo vệ chống can thiệp trái phép. Nếu SAM không được sử dụng trong cùng một môi trường chống giả mạo với SCDev, thì cần có một kênh bảo mật giữa hai môi trường chống giả mạo này.

5.12 Môi trường

Có ba môi trường khác nhau được xác định.

5.12.1 Môi trường được bảo vệ chống giả mạo

Môi trường chống giả mạo được vận hành bên trong môi trường được bảo vệ bởi TSP và được cách ly khỏi truy cập internet trực tiếp. Điều này đảm bảo tính toàn vẹn của mã được thực thi trong môi trường này. Mã này bảo vệ việc sử dụng các khóa ký và đảm bảo việc kích hoạt chữ ký phải nằm dưới sự kiểm soát của người ký. Môi trường được bảo vệ chống giả mạo cũng bảo vệ các liên kết giữa khóa ký và người ký (liên kết được tạo và kiểm tra khi cần thiết để tạo chữ ký).

Đối với SCAL1, phải tạo và sử dụng các khóa riêng tư hoặc khóa bí mật trong môi trường được bảo vệ chống giả mạo.

Đối với SCAL2, các khóa riêng tư hoặc khóa bí mật cần được tạo ra và sử dụng trong môi trường được bảo vệ chống giả mạo. Ngoài ra, phần mềm của SAM cũng cần được sử dụng trong môi trường được bảo vệ chống giả mạo.

5.12.2 Môi trường được bảo vệ bởi TSP

Môi trường được bảo vệ bởi TSP được kiểm tra theo các yêu cầu về vận hành an toàn của hệ thống ký trên máy chủ. Môi trường này bảo vệ chống lại các cuộc tấn công từ internet và xử lý các kết nối internet đến/từ môi trường bên ngoài (ví dụ: người ký, SCA, RA).

Môi trường này có thể lưu trữ dưới dạng được bảo vệ, khóa ký và liên kết giữa khóa và người ký.

TSP bảo vệ môi trường này nhằm đáp ứng các yêu cầu SAD và SAP và đặt ra các nghĩa vụ đối với môi trường RA (liên quan đến việc đăng ký).

Môi trường này cũng phải đáp ứng các yêu cầu đăng ký chứng chỉ để chứng minh quyền kiểm soát duy nhất (cần thiết cho RA).

5.12.3 Môi trường của người ký

Môi trường của người ký là môi trường cục bộ đối với người ký.

Bên ký kết chịu trách nhiệm bảo vệ môi trường của mình. Khi bên ký kết sử dụng môi trường do bên thứ ba cung cấp, thì bên thứ ba chịu trách nhiệm bảo vệ môi trường của bên ký kết.

Môi trường ký kết bao gồm các yếu tố chung có thể được sử dụng để chuẩn bị tài liệu cần ký và định dạng chữ ký tài liệu, cũng như mã SIC.

Mã SIC được người ký sử dụng để tạo liên kết giữa người ký và toàn bộ quy trình ký điện tử được kích hoạt thông qua hệ thống SAP.

Không có yêu cầu chứng nhận trực tiếp nào đối với SIC liên quan đến tiêu chuẩn này. Tuy nhiên, trong thiết kế và triển khai SIC, cần phải tính đến các yêu cầu về truyền/tính toán SAD và sự tương tác của SIC với SAM thông qua SAP, bao gồm cả việc xác thực người ký.

5.13 Mô hình chức năng

5.13.1 Tổng quan

Điều khoản này trình bày kiến trúc khái niệm của TW4S nhằm giới thiệu phạm vi, các thành phần và cơ chế kích hoạt. Mô hình này không đại diện cho bất kỳ kiến trúc vật lý nào, vốn trên thực tế sẽ sử dụng, ví dụ, nhiều máy chủ và thiết bị để chia sẻ tải hoặc dự phòng.

Môi trường của người ký không được TW4S biết đến. Môi trường này cần được bảo vệ, ví dụ như bằng cách chỉ cài đặt phần mềm dịch vụ tin cậy và sử dụng phần mềm bảo vệ chống lại phần mềm độc hại.

Tổ chức cung cấp dịch vụ tin cậy (TSP) bảo vệ môi trường của TW4S. TW4S được vận hành theo chính sách bảo mật bao gồm các yêu cầu bảo mật chung về vật lý, nhân sự, quy trình và tài liệu, cũng như bất kỳ yêu cầu cụ thể nào đối với các TSP cung cấp dịch vụ tạo chữ ký.

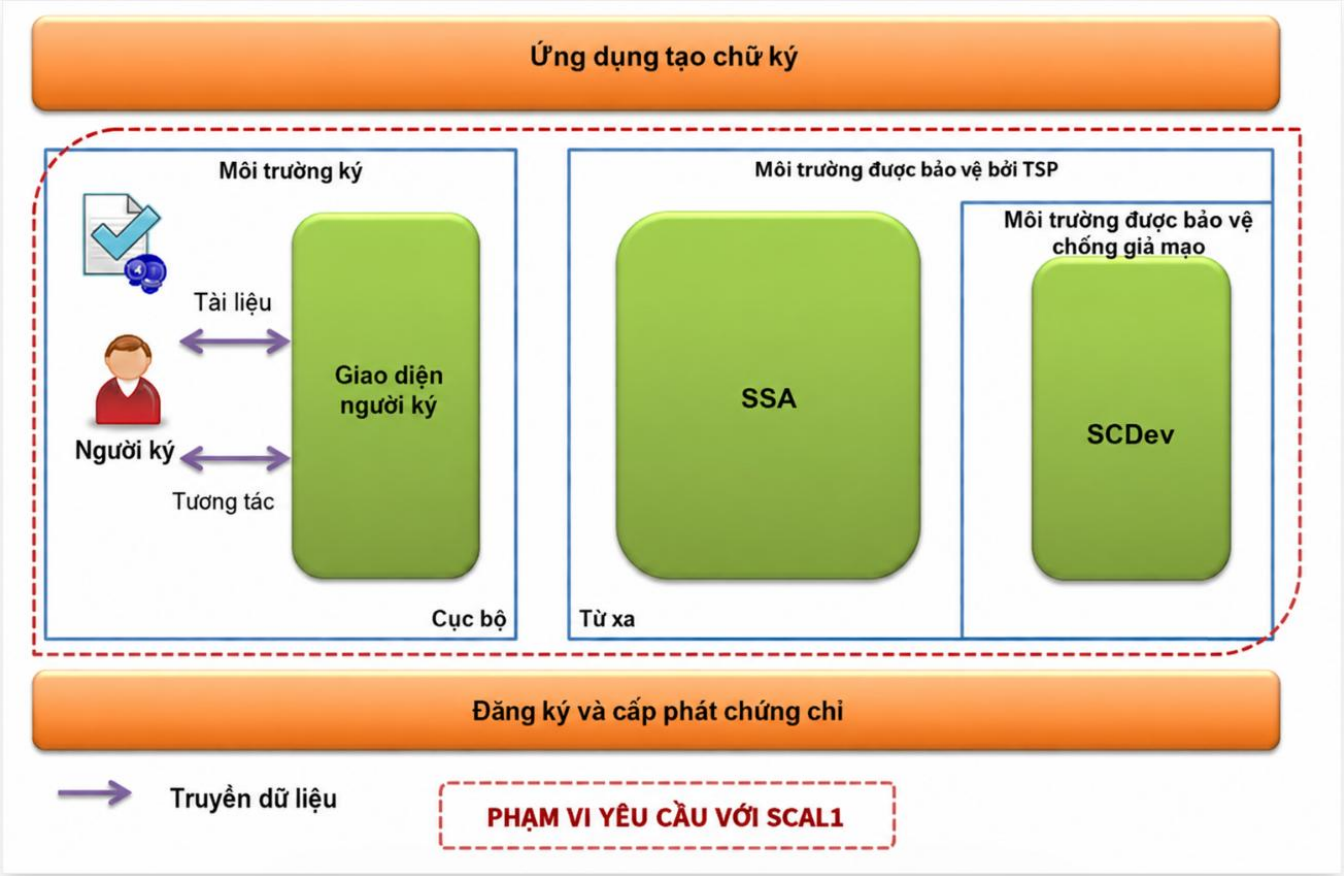
Đối với SCAL2, khóa ký và SAM được bảo vệ bởi một môi trường chống giả mạo.

5.13.2 Phạm vi yêu cầu

Thiết bị TW4S cung cấp khả năng quản lý từ xa an toàn khóa ký của người ký và tạo chữ ký số thông qua khóa ký được quản lý từ xa đó.

Tiêu chuẩn này không đặt ra bất kỳ hạn chế nào về cách thức hệ thống máy chủ và hệ thống ký có thể được chia thành một hoặc nhiều thành phần. Ứng dụng tạo chữ ký (SCA) nằm ngoài phạm vi (xem Hình

1) của tiêu chuẩn này và các yêu cầu đối với hệ thống dịch vụ tin cậy cho TSP liên quan đến việc cấp chứng chỉ cũng nằm ngoài phạm vi (xem CEN/TS 419261).



Hình 1 — Phạm vi yêu cầu

5.13.3 Cơ chế kích hoạt chữ ký

5.13.3.1 Tổng quan

Điều khoản này trình bày một số mô hình được đề xuất để kích hoạt chữ ký nhằm tạo ra chữ ký số. Bất kỳ kiến trúc nào khác tuân thủ Điều khoản 6 đều có thể được triển khai.

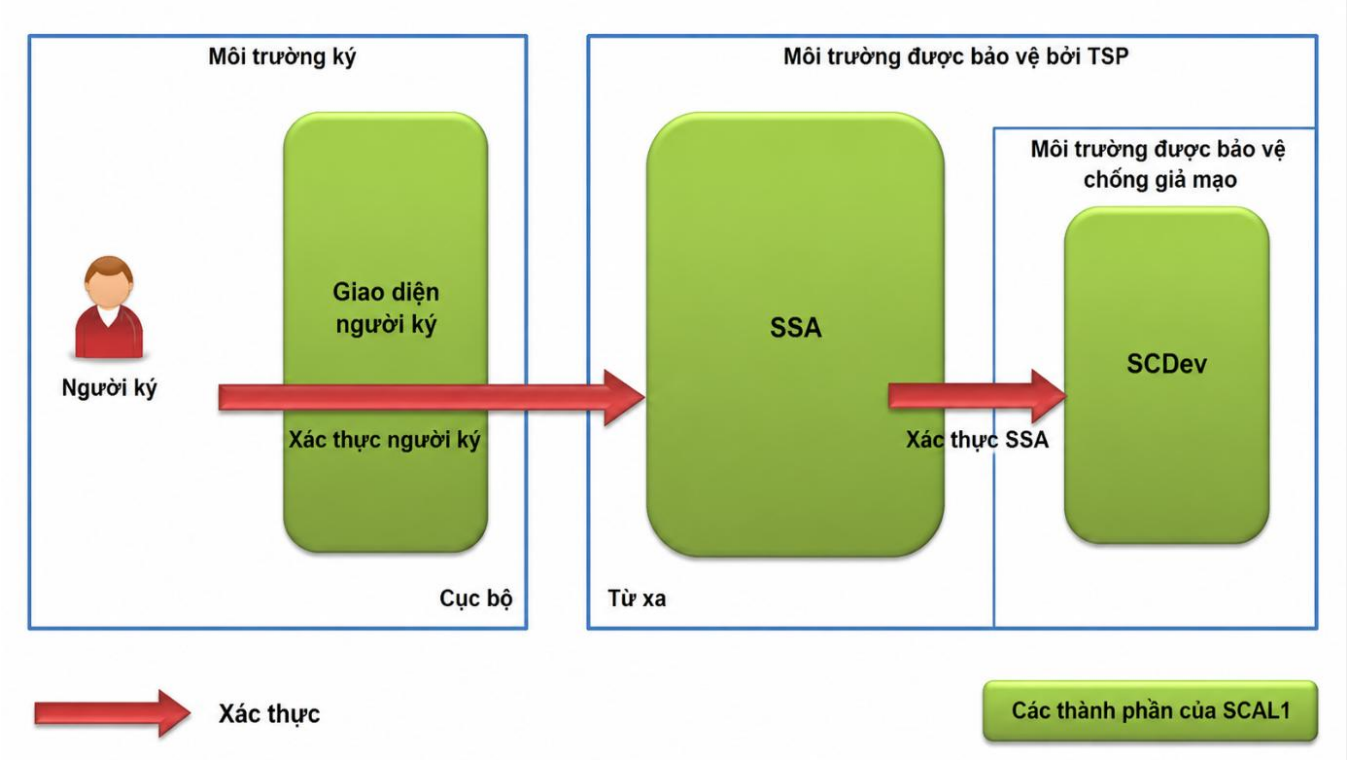
TW4S thường được sử dụng bởi một nhóm người ký, mỗi người ký sở hữu một hoặc nhiều khóa ký và TW4S có thể bao gồm một hoặc nhiều SCDev để thực hiện các thao tác ký.

Khóa ký có thể được lưu trữ an toàn bên ngoài SCDev và được tải động, miễn là các biện pháp kiểm soát được áp dụng để đảm bảo tính bảo mật tương tự đối với khóa ký. Các cơ chế tải/dỡ khóa được sử dụng để bảo vệ khóa ký nằm ngoài phạm vi của tiêu chuẩn này.

5.13.3.2 Kích hoạt chữ ký cho SCAL1

Tính bảo mật và toàn vẹn của khóa ký được đảm bảo bởi SCDev. SCDev có thể được kích hoạt bởi SSA. Việc kích hoạt có thể duy trì trong một khoảng thời gian nhất định và/hoặc cho một số lượng chữ ký nhất định.

Việc kích hoạt khóa ký yêu cầu người ký phải được SSA xác thực (xem Hình 2). Khi quá trình xác thực người ký thành công, khóa ký tương ứng CÓ THỂ được sử dụng để thực hiện thao tác ký thay mặt người ký trong một khoảng thời gian nhất định và/hoặc một số lượng thao tác ký nhất định. Điều này cho phép SSA được sử dụng cho mục đích ký hàng loạt/theo lô.



Hình 2 — Hệ thống kích hoạt chữ ký với SCAL1

Kiến trúc này có thể được sử dụng để tạo ra giá trị chữ ký số (ví dụ: mã băm được mã hóa bằng khóa riêng của người ký) với mức độ đảm bảo kiểm soát thấp.

5.13.3.3 Kích hoạt chữ ký cho SCAL2

Tính bảo mật và toàn vẹn của khóa ký được đảm bảo bởi SCDev từ xa .

Thiết bị SCDev từ xa được điều khiển bởi SSA.

SCDev từ xa tham gia vào SAP và đảm bảo rằng hoạt động ký điện tử được thực hiện dưới sự kiểm soát của người ký hợp pháp.

Giao diện SSA thông qua một kênh bảo mật sẽ kết nối với SAM của SCDev từ xa để xác minh SAD nhằm kích hoạt khóa ký tương ứng (xem Hình 3).

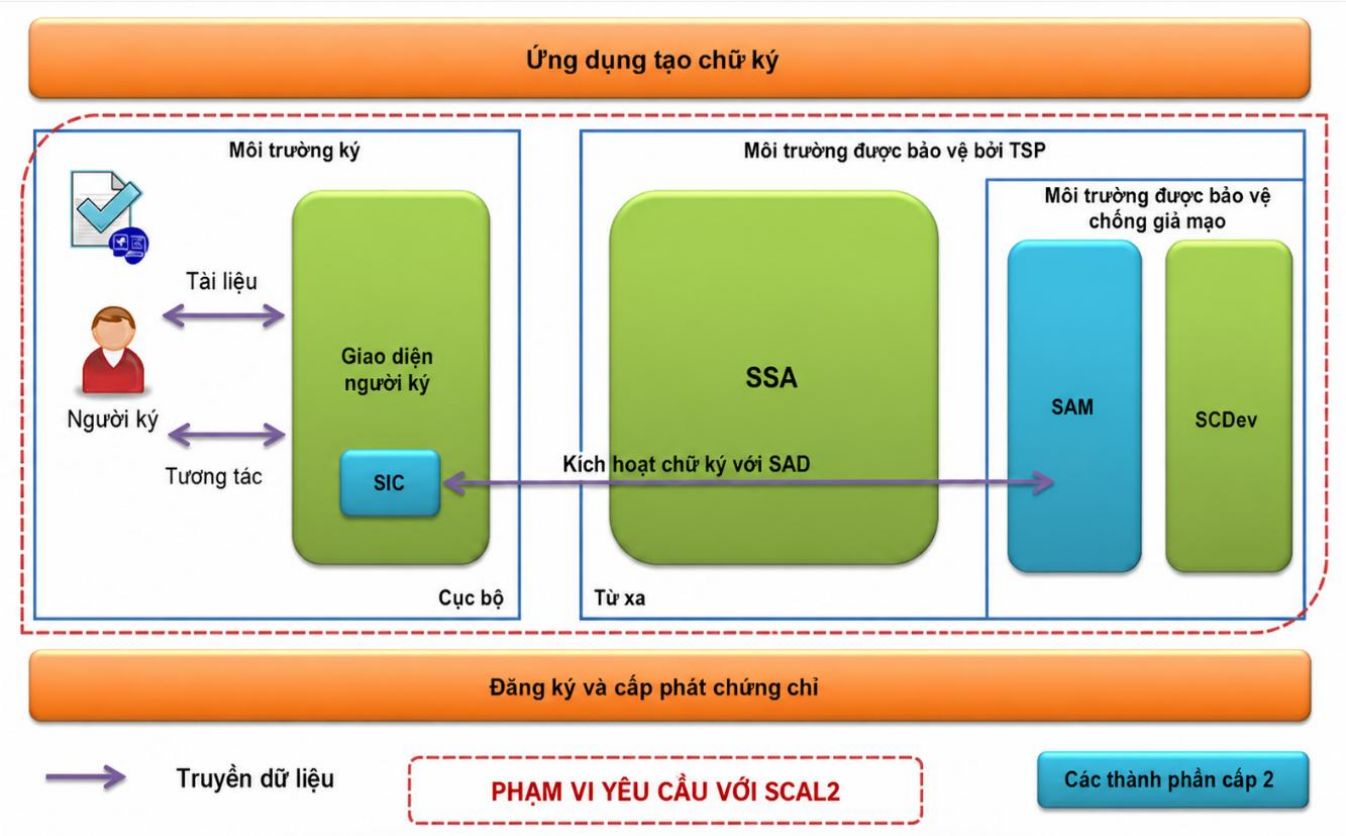
Việc xác thực người ký có thể được duy trì trong một khoảng thời gian nhất định và/hoặc cho một số lượng chữ ký nhất định. Tuy nhiên, việc tính toán SAD phải được thực hiện cho mỗi thao tác ký. SAD có thể được liên kết với một tập hợp DTBS/ R, điều này cho phép SSA được sử dụng cho mục đích ký hàng loạt/theo lô.

Việc xác thực người ký có thể được thực hiện bằng cách sử dụng SIC, mã này được dùng để tạo liên kết giữa người ký và chữ ký như một phần của SAD.

Việc sử dụng SAD thuộc trách nhiệm của SAM:

— Nếu SAD được tạo bởi SIC thì phải được chuyển một cách an toàn từ SIC sang SAM để xác minh.

— Nếu SAD không được tạo bởi SIC thì phải được tạo trong/trong quá trình xác thực người ký thành công bằng SIC và được chuyển một cách an toàn đến SAM để xác minh.



Hình 3 — Hệ thống kích hoạt chữ ký với SCAL2

Kiến trúc này có thể được sử dụng để tạo ra giá trị chữ ký số (ví dụ: hàm băm được mã hóa bằng khóa riêng của người ký) với mức độ đảm bảo kiểm soát cao hơn.

5.13.4 Các thành phần TW4S

Các bộ phận cốt lõi của TW4S mà tiêu chuẩn này quy định các yêu cầu là tập hợp các thành phần chức năng:

— Thiết lập khóa ký – để tạo khóa ký trong SCDev và gán chúng cho những người ký được ủy quyền sử dụng.

— Quản lý khóa ký – để xóa, sao lưu và khôi phục khóa ký trong SCDev. — Xác thực người ký – để ủy quyền cho người ký sử dụng khóa ký.

— Tạo chữ ký số – để kết nối người ký được ủy quyền nhằm tạo chữ ký số trong SCDev.

Để nâng cao mức độ đảm bảo, cần bổ sung thêm các thành phần bắt buộc để đạt được chứng nhận SCAL2:

— SIC – để tạo liên kết giữa người ký và thao tác ký trong SAP. SIC có thể tạo ra SAD trong môi trường của người ký.

— SAM – được bảo vệ bởi môi trường chống giả mạo và chịu trách nhiệm thực thi SAP. SAM cung cấp một tập hợp các thành phần:

— Tạo SAD – để tạo SAD trong môi trường được bảo vệ chống giả mạo khi SAD không được tạo bởi SIC.

— Kích hoạt khóa ký – để quản lý quá trình xác minh SAD và kích hoạt các khóa ký.

— Tạo khóa ký – để quản lý các yếu tố xác thực gắn liền với khóa ký.

6 Yêu cầu bảo mật

6.1 Tổng quan

Điều khoản này mô tả tất cả các yêu cầu áp dụng cho một hệ thống ký trên máy chủ để được coi là TW4S.

Các yêu cầu trong mục 6.4 áp dụng cho TW4S hỗ trợ mức độ đảm bảo kiểm soát duy nhất cấp 2.

6.2 Yêu cầu an toàn chung (SRG)

6.2.1 Quản lý (SRG_M)

6.2.1.1 Tổng quan

Giả định rằng Tổ chức cung cấp dịch vụ tin cậy (TSP) cung cấp dịch vụ tạo chữ ký vận hành TW4S trong một môi trường có chính sách bảo mật bao gồm các yêu cầu bảo mật chung về vật lý, nhân sự, quy trình và tài liệu, cũng như bất kỳ yêu cầu cụ thể nào đối với các TSP cung cấp dịch vụ tạo chữ ký.

Ví dụ, định nghĩa về các yêu cầu có thể được tham chiếu trong quy chuẩn kỹ thuật quốc gia QCVN 137:2025/BKHCN.

6.2.1.2 Quản lý hệ thống và an toàn (SRG_M.1)

Một TSP cần quản lý bảo mật của mình để vận hành TW4S, hệ thống cung cấp dịch vụ tạo chữ ký số.

SRG_M.1.1 TW4S phải hỗ trợ các vai trò với các quyền hạn khác nhau.

SRG_M.1.2 Tối thiểu, TW4S phải hỗ trợ các vai trò sau:

Nhân sự bảo mật: chịu trách nhiệm tổng thể về việc quản lý và thực thi các chính sách, quy trình an toàn, đồng thời có quyền truy cập vào các thông tin liên quan đến an toàn.

Quản trị viên hệ thống: được phép cài đặt, cấu hình và bảo trì TW4S nhưng chỉ được phép truy cập hạn chế vào các thông tin liên quan đến bảo mật.

Người vận hành hệ thống: chịu trách nhiệm vận hành hệ thống TW4S hàng ngày và được phép thực hiện sao lưu và phục hồi hệ thống.

Các nhân sự kiểm toán hệ thống: được phép xem các bản lưu trữ và nhật ký kiểm toán của TW4S nhằm mục đích kiểm toán hoạt động của hệ thống theo chính sách bảo mật.

Các nhân viên bảo mật và quản trị viên hệ thống là những người dùng hệ thống có quyền truy cập đặc biệt.

Các nhà điều hành hệ thống và kiểm toán viên hệ thống có vai trò đặc quyền nhưng không thể quản trị hoặc cấu hình TW4S.

SRG_M.1.3 Tối thiểu, TW4S phải hỗ trợ các vai trò không có đặc quyền sau:

Người ký: được ủy quyền sử dụng TW4S bằng cách chuyển tiếp SAD như một phần của SAP để ký tài liệu hoặc DTBS/R, mà cũng có thể được chuyển tiếp thông qua SAP.

SCA: được ủy quyền gửi yêu cầu DTBS/R đến TW4S để người ký xác nhận.

RA: được ủy quyền gửi chứng chỉ khóa công khai đến TW4S để đáp lại yêu cầu ký chứng chỉ.

SRG_M.1.4 Một người dùng có quyền đặc quyền không được phép đảm nhiệm tất cả các vai trò đặc quyền và không nên đảm nhiệm nhiều hơn một vai trò đặc quyền.

SRG_M.1.5 Người dùng được liên kết với các vai trò có đặc quyền không được liên kết với các vai trò không có đặc quyền.

Người dùng không có vai trò đặc quyền không được phép đảm nhận vai trò đặc quyền.

SRG_M.1.6 TW4S phải có khả năng đảm bảo rằng người dùng được ủy quyền đảm nhận vai trò Nhân viên bảo mật không được ủy quyền đảm nhận vai trò Kiểm toán viên Hệ thống.

SRG_M.1.7 TW4S phải có khả năng đảm bảo rằng người dùng được ủy quyền đảm nhận vai trò Quản trị viên Hệ thống và/hoặc vai trò Người vận hành Hệ thống không được ủy quyền đảm nhận vai trò Kiểm toán viên Hệ thống và/hoặc vai trò Nhân sự bảo mật.

SRG_M.1.8 Các cá nhân thuộc nhóm người dùng hệ thống có đặc quyền phải là những người được chỉ định và đào tạo.

SRG_M.1.9 Chỉ những người dùng hệ thống có đặc quyền mới được phép truy cập vật lý vào phần cứng và quản trị TW4S.

SRG_M.1.10 Chỉ những người dùng hệ thống có đặc quyền mới được phép quản trị TW4S thông qua tất cả các ứng dụng và giao diện liên quan.

6.2.2 Hệ thống và hoạt động (SRG_SO)

6.2.2.1 Quản lý vận hành (SRG_SO.1)

TSP vận hành hệ thống TW4S cần đảm bảo các chức năng quản lý vận hành của mình được bảo mật đầy đủ.

SRG_SO.1.1 Các nhà sản xuất TW4S phải đảm bảo cung cấp hướng dẫn để cho phép TW4S được: — vận hành đúng cách và an toàn;

— được triển khai theo cách giảm thiểu tối đa rủi ro lỗi hệ thống;

— được bảo vệ chống lại virus và phần mềm độc hại để đảm bảo tính toàn vẹn của hệ thống và thông tin mà chúng xử lý.

SRG_SO.1.2 Các nhà sản xuất TW4S phải cung cấp tài liệu hệ thống bao gồm trách nhiệm của bốn vai trò đặc quyền được đề cập trong SRG_M.1.2. Tài liệu nên bao gồm:

— Hướng dẫn cài đặt;

— Hướng dẫn quản lý;

— Hướng dẫn sử dụng.

6.2.2.2 Đồng bộ hóa thời gian (SRG_SO.2)

Việc tạo chữ ký và xác minh sau đó có liên quan đến thời gian, do đó cần đảm bảo rằng TW4S được đồng bộ hóa phù hợp với một nguồn thời gian chuẩn. Yêu cầu này độc lập với bất kỳ yêu cầu đóng dấu thời gian nào mà TSP có thể thiết lập.

SRG_SO.2.1 Các nhà sản xuất TW4S phải nêu rõ độ chính xác về thời gian của TW4S và cách thức đảm bảo điều này.

SRG_SO.2.2 Để đảm bảo độ chính xác về thời gian của các sự kiện được kiểm toán, nên sử dụng nguồn thời gian được đồng bộ hóa phù hợp với nguồn thời gian chuẩn.

SRG_SO.2.3 Để kiểm tra xem chứng chỉ đã hết hạn hay chưa, phải sử dụng nguồn thời gian được đồng bộ hóa phù hợp với UTC.

6.2.3 Nhận dạng và xác thực (SRG_IA)

6.2.3.1 Tổng quan

Các chức năng Nhận dạng và Xác thực giới hạn quyền truy cập và sử dụng TW4S chỉ dành cho những người được ủy quyền. Điều này áp dụng cho tất cả các thành phần quản lý của TSP. Việc Nhận dạng và Xác thực CÓ THỂ được cung cấp bởi phần mềm hệ điều hành cơ bản hoặc trực tiếp bởi chính thành phần đó.

6.2.3.2 Xác thực cho các vai trò có đặc quyền và không có đặc quyền khác ngoài người ký (SRG_IA.1) LƯU Ý Việc xác thực người ký được quy định bởi SRC_SA.

SRG_IA.1.1 TW4S phải yêu cầu mỗi người dùng phải tự nhận dạng và được xác thực thành công trước khi cho phép bất kỳ hành động nào thay mặt người dùng đó hoặc vai trò mà người dùng đó đảm nhận.

SRG_IA.1.2 Việc xác thực lại là bắt buộc sau khi đăng xuất.

SRG_IA.1.3 Sự kết hợp của dữ liệu xác thực, nếu được sử dụng, phải không thể dự đoán được.

SRG_IA.1.4 Đối với người dùng có đặc quyền, cần phải triển khai các cơ chế để giảm nguy cơ phiên người dùng đã được xác thực bị chiếm đoạt nếu thiết bị nhập liệu của người dùng bị bỏ quên, ví dụ như bằng cách chấm dứt phiên người dùng sau một khoảng thời gian không hoạt động nhất định.

6.2.3.3 Lỗi xác thực (SRG_IA.2)

SRG_IA.2.1 Nếu số lần xác thực không thành công từ cùng một người dùng đạt đến số lần tối đa cho phép, TW4S phải ngăn chặn các lần xác thực người dùng tiếp theo trong một khoảng thời gian nhất định hoặc cho đến khi người quản trị mở khóa người dùng.

6.2.4 Kiểm soát truy cập hệ thống (SRG_SA)

6.2.4.1 Tổng quan

Các chức năng kiểm soát truy cập hệ thống hạn chế việc sử dụng các đối tượng của TW4S chỉ dành cho những người được ủy quyền. Điều này không áp dụng cho kiểm soát truy cập người ký mà áp dụng cho kiểm soát truy cập người dùng có đặc quyền đối với tất cả các đối tượng nhạy cảm của TW4S (xem SRC_SA để biết kiểm soát truy cập người ký).

Việc kiểm soát truy cập hệ thống có thểđược cung cấp bởi phần mềm hệ điều hành cơ bản hoặc trực tiếp bởi chính thành phần đó. Quyền truy cập vào các đối tượng TW4S cụ thể được xác định bởi chủ sở hữu đối tượng dựa trên danh tính của người cố gắng truy cập và:

a) quyền truy cập vào đối tượng được cấp cho chủ thể hoặc;

b) Các đặc quyền mà đối tượng được hưởng.

6.2.4.2 Quản lý quyền (SRG_SA.1)

SRG_SA.1.1 TW4S PHẢI cung cấp khả năng kiểm soát và hạn chế quyền truy cập của các cá nhân được xác định vào hệ thống hoặc các đối tượng người dùng mà họ sở hữu hoặc chịu trách nhiệm.

SRG_SA.1.2 TW4S PHẢI đảm bảo cung cấp quyền truy cập vào thông tin dư thừa nhạy cảm.

6.2.5 Quản lý khóa (SRG_KM)

6.2.5.1 Tổng quan

Một hệ thống TW4S có thể sử dụng các khóa mật mã để cung cấp tính toàn vẹn, bảo mật và chức năng xác thực trong các hệ thống con của chính nó và giữa các hệ thống con. Do đó, việc sử dụng, tiết lộ, sửa đổi hoặc thay thế trái phép các khóa này sẽ dẫn đến mất an toàn trong hệ thống TW4S. Điều cần thiết là các khóa này phải được quản lý an toàn trong suốt vòng đời của chúng.

Do các mối đe dọa khác nhau tác động đến khóa TW4S, tùy thuộc vào nơi và cách chúng được sử dụng, việc phân loại khóa theo mức độ rủi ro (tức là độ nhạy cảm) là rất quan trọng. Theo tiêu chuẩn này, khóa được chia thành các loại sau:

1) Khóa ký của người ký – các khóa được người ký liên quan sử dụng để tạo chữ ký điện tử;

2) Khóa cơ sở hạ tầng – các khóa được TW4S sử dụng cho các quy trình như thỏa thuận khóa, xác thực hệ thống con, ký nhật ký kiểm toán, mã hóa dữ liệu được truyền hoặc lưu trữ, v.v. Các khóa phiên ngắn hạn cũng được phân loại là khóa cơ sở hạ tầng;

3) Khóa điều khiển – các khóa được sử dụng bởi nhân viên quản lý hoặc sử dụng TW4S và những người có khả năng sử dụng các khóa này cho mục đích xác thực, ký kết hoặc bảo mật.

Về yêu cầu bảo mật, khóa ký của người ký phải được coi là rất nhạy cảm. Do đó, các biện pháp đối phó để quản lý rủi ro tiềm ẩn nên được áp dụng cả về số lượng và hiệu quả. Khóa cơ sở hạ tầng cũng được coi là rất nhạy cảm nhưng do đặc tính phân tán của chúng nên chúng ít nhạy cảm hơn so với khóa ký của người ký. Các khóa ít nhạy cảm nhất được TSP sử dụng được coi là những khóa được nhân viên sử dụng để kiểm soát TW4S vì chúng được sử dụng bởi những cá nhân dịch vụ tin cậy và có thời gian sử dụng ngắn hơn. Khóa phiên, được sử dụng cho các giao dịch đơn lẻ/ngắn hạn, được coi là thông tin nhạy cảm nhưng có yêu cầu bảo mật thấp hơn so với các loại đã đề cập ở trên.

Khóa cơ sở hạ tầng và khóa điều khiển có thể là khóa riêng tư hoặc khóa bí mật.

6.2.5.2 Tạo khóa (SRG_KM.1)

SRG_KM.1.1 Khóa riêng tư hoặc khóa bí mật nên được tạo và sử dụng trong SCDev.

SCDev đã sử dụng nên:

— là một hệ thống dịch vụ tin cậy, được đảm bảo đạt chuẩn EAL 4 trở lên, được bổ sung bởi AVA_VAN.5 theo tiêu chuẩn quốc gia TCVN 8709-3:2011, hoặc các tiêu chí đánh giá an toàn công nghệ thông tin tương đương được công nhận trong nước hoặc quốc tế. Đích an toàn hoặc hồ sơ bảo vệ này phải đáp ứng các yêu cầu của tài liệu này, dựa trên phân tích rủi ro và có tính đến các biện pháp an toàn vật lý và các biện pháp an toàn phi kỹ thuật khác; hoặc

— Đáp ứng các yêu cầu được xác định trong tiêu chuẩn quốc gia TCVN 11295:2016 hoặc QCVN 137:2025/BKHCN (FIPS PUB 140-2 mức 3).

SRG_KM.1.2 SCDev phải hỗ trợ các thuật toán mã hóa và độ dài khóa tương ứng với mức độ bảo mật phù hợp, đáp ứng các nhu cầu bảo mật đã được xác định trong quá trình thiết kế hệ thống.

Trong trường hợp cần các dịch vụ bảo mật hoặc bảo vệ tính toàn vẹn (ví dụ: sao lưu khóa ký), chỉ được sử dụng các thuật toán mã hóa và tham số thuật toán có độ mạnh tương đương hoặc cao hơn.

SRG_KM.1.3 Khi các khóa riêng tư hoặc khóa bí mật (bao gồm khóa ký của người ký, Khóa Cơ sở hạ tầng và Khóa Điều khiển) được lưu giữ bên ngoài SCDev, các khóa này phải được bảo vệ để đảm bảo tính bảo mật và toàn vẹn của chúng.

SRG_KM.1.4 SCDev phải được khởi tạo, trước khi tạo hoặc chứa bất kỳ khóa ký nào, bằng các cơ chế kỹ thuật yêu cầu ít nhất hai toán tử trong SCDev.

6.2.5.3 Lưu trữ, sao lưu và phục hồi khóa (SRG_KM.2)

SRG_KM.2.1 Tất cả các khóa riêng tư hoặc khóa bí mật (bao gồm khóa ký của người ký, Khóa Cơ sở hạ tầng và Khóa Điều khiển) phải được lưu trữ an toàn, tức là không bao giờ được lưu trữ ở trạng thái không được bảo vệ.

SRG_KM.2.2 Nếu bất kỳ khóa riêng tư hoặc khóa bí mật nào (bao gồm khóa ký của người ký, Khóa Cơ sở hạ tầng và Khóa Điều khiển) được xuất ra từ SCDev đó phải được bảo vệ để đảm bảo tính bảo mật và toàn vẹn của nó ở mức độ bảo mật tương đương hoặc cao hơn so với bên trong SCDev.

Trong trường hợp khóa riêng/khóa bí mật được bảo vệ bằng mã hóa, chỉ được sử dụng các thuật toán mã hóa và tham số thuật toán có độ mạnh tương đương hoặc cao hơn.

SRG_KM.2.3 TW4S phải đảm bảo rằng việc sao lưu, lưu trữ và khôi phục các khóa riêng tư hoặc khóa bí mật (bao gồm khóa ký của người ký, Khóa Cơ sở hạ tầng và Khóa Điều khiển) chỉ được thực hiện bởi nhân viên được ủy quyền. Các khóa chính được sử dụng để bảo vệ cả khóa người dùng và khóa làm việc phải được sao lưu, lưu trữ và tải lại dưới sự kiểm soát kép tối thiểu. Các khóa chính đó CHỈ được lưu giữ bên ngoài SCDev dưới dạng được bảo vệ.

6.2.5.4 Cách sử dụng khóa (SRG_KM.3)

SRG_KM.3.1 Khóa riêng tư hoặc khóa bí mật (bao gồm khóa ký của người ký, Khóa Cơ sở hạ tầng và Khóa Điều khiển) chỉ được sử dụng cho mục đích đã định.

SRG_KM.3.2 Khóa riêng tư hoặc khóa bí mật (bao gồm khóa ký của người ký, Khóa cơ sở hạ tầng và Khóa điều khiển) KHÔNG ĐƯỢC chia sẻ trừ khi cần thiết để đáp ứng mục đích sử dụng.

SRG_KM.3.3 Các biện pháp kiểm soát truy cập phải được thiết lập để bảo vệ quyền truy cập và sử dụng các khóa (bao gồm khóa ký của người ký, Khóa Cơ sở hạ tầng và Khóa Kiểm soát).

SRG_KM.3.4 Khóa ký chỉ được liên kết với một người ký và chỉ một chứng chỉ khóa công khai. 6.2.5.5 Phân phối khóa (SRG_KM.4)

SRG_KM.4.1 Khóa riêng tư hoặc khóa bí mật (bao gồm Khóa Cơ sở hạ tầng và Khóa Điều khiển) phải được truyền tải một cách an toàn khi cần phải truyền tải.

SRG_KM.4.2 Tất cả các khóa được sử dụng để bảo vệ các khóa riêng tư/bí mật khác trong quá trình truyền tải phải mạnh (ít nhất) bằng các khóa được truyền tải.

6.2.5.6 Gia hạn/cập nhật/thay đổi khóa (SRG_KM.5)

SRG_KM.5.1 Các khóa cơ sở hạ tầng và điều khiển nên được thay đổi thường xuyên, với tần suất dựa trên đánh giá rủi ro.

SRG_KM.5.2 Nếu bất kỳ thuật toán khóa hoặc độ dài nào được coi là không phù hợp, các khóa dựa trên các thuật toán đó phải được thay đổi ngay lập tức.

SRG_KM.5.3 Nếu bất kỳ khóa nào bị xâm phạm hoặc nghi ngờ bị xâm phạm, chúng nên được thay đổi ngay lập tức.

6.2.5.7 Lưu trữ khóa (SRG_KM.6)

SRG_KM.6.1 Khóa ký không được lưu trữ.

6.2.5.8 Xóa khóa (SRG_KM.7)

SRG_KM.7.1 Khóa ký phải bị hủy sau khi chứng chỉ khóa công khai hết hạn hoặc nếu khóa ký không còn hữu ích đối với người ký.

SRG_KM.7.2 Nếu liên kết giữa khóa ký và người ký không được duy trì sau khi phiên ký kết kết thúc, thì khóa ký phải bị hủy bỏ khi phiên ký kết kết thúc.

SRG_KM.7.3 Cơ chế và quy trình hủy khóa ký nên đảm bảo rằng tất cả các bản sao lưu của khóa ký đã bị hủy cũng bị hủy và không có thông tin còn sót lại nào có thể được sử dụng để khôi phục khóa ký.

6.2.6 Kiểm toán (SRG_AA)

6.2.6.1 Tạo dữ liệu kiểm toán (SRG_AA.1)

Mỗi dịch vụ đều có các yêu cầu kiểm toán cụ thể bổ sung mà phải được đáp ứng ngoài các yêu cầu chung này.

SRG_AA.1.1 Tối thiểu, các sự kiện sau phải được ghi lại:

— Các sự kiện quan trọng về môi trường và quản lý chính của TW4S (phát sinh, sử dụng và hủy bỏ);

— Các sự kiện ký kết của người dùng (ví dụ: ký kết thành công bằng khóa ký của người ký và quản lý yêu cầu DTBS/R);

— Xác thực người dùng trong quá trình SAP;

— Quản lý SAD của người ký tên bởi TW4S;

— Khởi động và tắt chức năng tạo dữ liệu kiểm toán;

— thay đổi các tham số kiểm toán.

Các sự kiện ký kết của người dùng phải bao gồm chứng chỉ liên kết với khóa ký.

Tất cả các lần truy cập vào TW4S đều nên được ghi lại.

SRG_AA.1.2 Tổ chức cung cấp dịch vụ tin cậy (TSP) phải chỉ rõ những việc cần làm (tức là các hành động được thực hiện) trong trường hợp không thể truyền thông tin kiểm toán đến bất kỳ kho lưu trữ bên ngoài nào.

6.2.6.2 Đảm bảo tính khả dụng của dữ liệu kiểm toán (SRG_AA.2)

SRG_AA.2.1 TW4S phải duy trì dữ liệu kiểm toán và đảm bảo thực hiện các biện pháp để lưu trữ tất cả dữ liệu kiểm toán.

SRG_AA.2.2 Chức năng kiểm toán chỉ được phép thêm thông tin.

SRG_AA.2.3 TW4S phải bảo vệ các bản ghi kiểm toán được lưu trữ trong nhật ký kiểm toán khỏi bị xóa trái phép.

SRG_AA.2.4 Bản ghi kiểm toán có thể bị xóa khi được lưu trữ vào bộ nhớ ngoài.

6.2.6.3 Tham số dữ liệu kiểm toán (SRG_AA.3)

SRG_AA.3.1 Tất cả các bản ghi kiểm toán (bao gồm cả việc ghi nhật ký kiểm toán dành riêng cho dịch vụ) phải chứa các tham số sau:

— Ngày và giờ diễn ra sự kiện;

— Loại sự kiện;

— Danh tính của chủ thể (ví dụ: người dùng, quản trị viên, quy trình) chịu trách nhiệm cho hành động đó;

— Sự thành công hay thất bại của sự kiện được kiểm toán.

6.2.6.4 Xem xét kiểm toán có thể lựa chọn (SRG_AA.4)

SRG_AA.4.1 TW4S phải cho phép tìm kiếm các sự kiện trong nhật ký kiểm toán dựa trên ngày xảy ra sự kiện, loại sự kiện và/hoặc danh tính của người dùng.

SRG_AA.4.2 Hồ sơ kiểm toán phải được định dạng sao cho có thể xử lý và trình bày theo cách phù hợp để các kiểm toán viên hệ thống có thể hiểu được thông tin.

6.2.6.5 Rà soát kiểm toán hạn chế (SRG_AA.5)

Theo mặc định, SRG_AA.5.1 TW4S phải từ chối tất cả quyền truy cập đọc của người dùng vào các bản ghi kiểm toán, ngoại trừ những người dùng đã được cấp quyền truy cập đọc rõ ràng (ví dụ: những người có vai trò Kiểm toán viên Hệ thống).

6.2.6.6 Tạo cảnh báo (SRG_AA.6)

SRG_AA.6.1 TW4S phải tạo ra cảnh báo thông báo kịp thời về các sự kiện bất thường có thể ảnh hưởng đến khả năng đáp ứng các yêu cầu bảo mật được xác định trong tiêu chuẩn này của hệ thống máy chủ ký.

Cần phải triển khai một cơ chế phát ra cảnh báo mỗi khi phát hiện sự kiện bất thường. Cảnh báo này nên kích hoạt thông báo đến các nhân viên quản trị có liên quan.

Cảnh báo cũng có thể kích hoạt các hành động tiếp theo để phản ứng lại các cuộc tấn công tiềm tàng, chẳng hạn như chặn đứng con đường tấn công.

Ví dụ về các sự kiện bất thường liên quan đến hoạt động của người dùng có thể là (nhưng không giới hạn):

— Các hành động của người dùng ngoài giờ sử dụng thông thường.

— Các thao tác của người dùng được thực hiện với tốc độ bất thường (nhằm phát hiện sự can thiệp không phải của con người).

— Hành động của người dùng bỏ qua các hoạt động tiêu chuẩn trong các quy trình đã được xác định.

— Phiên người dùng trùng lặp.

6.2.6.7 Đảm bảo tính toàn vẹn dữ liệu kiểm toán (SRG_AA.7)

SRG_AA.7.1 TW4S phải đảm bảo tính toàn vẹn của dữ liệu kiểm toán.

SRG_AA.7.2 TW4S phải cung cấp một chức năng để xác minh tính toàn vẹn của dữ liệu kiểm toán.

6.2.6.8 Đảm bảo thời gian kiểm toán (SRG_AA.8)

SRG_AA.8.1 Để đảm bảo tính chính xác về thời gian của các sự kiện được kiểm toán, yêu cầu SRG_SO.2.2 được áp dụng.

6.2.7 Lưu trữ (SRG_AR)

6.2.7.1 Tạo dữ liệu lưu trữ (SRG_AR.1)

SRG_AR.1.1 TSP nên có khả năng tạo bản lưu trữ trên phương tiện lưu trữ ngoài. Phương tiện lưu trữ phải phù hợp cho việc lưu trữ và xử lý tiếp theo, và phải có khả năng cung cấp bằng chứng pháp lý cần thiết để hỗ trợ chữ ký số.

SRG_AR.1.2 Tất cả nhật ký kiểm toán phải được lưu trữ.

SRG_AR.1.3 Mỗi mục lưu trữ phải bao gồm thời gian diễn ra việc lưu trữ.

SRG_AR.1.4 Tệp lưu trữ không được bao gồm bất kỳ tham số bảo mật nhạy cảm nào, chẳng hạn như mật khẩu người dùng TW4S.

6.2.7.2 Tính toàn vẹn của dữ liệu lưu trữ (SRG_AR.2)

SRG_AR.2.1 Việc sửa đổi trái phép từng mục trong kho lưu trữ phải được ngăn chặn. Phải có cơ chế xác minh tính toàn vẹn để phát hiện các sửa đổi trái phép.

6.2.8 Sao lưu và phục hồi (SRG_BK)

6.2.8.1 Tổng quan

Điều khoản này chỉ bao gồm thông tin hệ thống, thông tin đối tượng và tất cả dữ liệu khác cần thiết để khôi phục hệ thống sau sự cố hoặc thảm họa. Điều khoản này không bao gồm việc sao lưu và phục hồi khóa, các yêu cầu bảo mật đối với việc này được quy định trong điều khoản SRG_KM.2.

6.2.8.2 Tính toàn vẹn và bảo mật của thông tin sao lưu (SRG_BK.1)

SRG_BK.1.1 Các bản sao lưu phải được bảo vệ khỏi sự sửa đổi bằng một cơ chế cho phép xác minh tính toàn vẹn của thông tin sao lưu.

SRG_BK.1.2 Các tham số bảo mật nhạy cảm và các thông tin bí mật khác phải được lưu trữ dưới dạng được bảo vệ để đảm bảo tính bảo mật và toàn vẹn.

6.2.8.3 Khôi phục (SRG_BK.2)

SRG_BK.2.1 Thiết bị TW4S phải bao gồm chức năng phục hồi có khả năng khôi phục trạng thái hệ thống từ bản sao lưu.

SRG_BK.2.2 Người dùng được liên kết với một vai trò có đủ đặc quyền phải có khả năng gọi chức năng khôi phục theo yêu cầu từ bản sao lưu.

6.3 Yêu cầu bảo mật của các thành phần cốt lõi (SRC)

6.3.1 Thiết lập khóa ký (SRC_SKS) - Khóa mật mã (SRC_SKS.1)

SRC_SKS.1.1 Các tham số thuật toán được sử dụng để tạo chữ ký bởi các hệ thống dịch vụ tin cậy phải được chọn sao cho chúng có thể tồn tại trong suốt thời gian hiệu lực của chứng chỉ người ký.

SRC_SKS.1.2 TW4S phải liên kết các khóa ký của người ký với chứng chỉ khóa công khai tương ứng của người ký.

SRC_SKS.1.3 Khóa ký của người ký có thể được tạo trước (tức là không liên kết với chứng chỉ khóa công khai).

SRC_SKS.1.4 Không nên sử dụng khóa ký trước khi chứng chỉ khóa công khai của nó được liên kết bởi TW4S.

SRC_SKS.1.5 TW4S phải bảo vệ tính toàn vẹn của các liên kết giữa khóa ký của người ký và chứng chỉ khóa công khai.

6.3.2 Xác thực người ký (SRC_SA)

6.3.2.1 Xác thực người ký cho SCAL1 (SRC_SA.1)

SRC_SA.1.1 Việc đăng ký người ký phải được thực hiện theo quy định tại Phụ lục A, mục A.1, đối với mức độ đảm bảo thấp hoặc cao hơn.

Các đặc tính và thiết kế của phương tiện nhận dạng điện tử phải tuân theo quy định tại Phụ lục A, mục A.2.1, đối với mức độ đảm bảo thấp hoặc cao hơn.

Cơ chế xác thực phải được quy định trong Phụ lục A, mục A.2.2, đối với mức độ đảm bảo thấp hoặc cao hơn.

SRC_SA.1.2 SSA phải yêu cầu mỗi người ký phải được xác định và xác thực thành công trước khi cho phép bất kỳ hành động nào có thể ảnh hưởng đến quyền kiểm soát duy nhất đối với bất kỳ khóa ký nào.

SRC_SA.1.3 Các giao thức đang sử dụng phải ngăn chặn các cuộc tấn công trung gian, tấn công phát lại và nói chung là bất kỳ hình thức tấn công nào mà người dùng độc hại có thể sử dụng thông tin xác thực không thuộc về họ.

SRC_SA.1.4 Kiểm soát truy cập phải đảm bảo rằng người ký không có quyền truy cập vào các đối tượng hệ thống nhạy cảm và bất kỳ chức năng nào cho phép người dùng kiểm soát khóa ký của người khác.

SRC_SA.1.5 TW4S phải đảm bảo rằng DTBS/R được cung cấp dưới sự kiểm soát của người ký chỉ được ký bằng khóa ký thuộc về người ký này.

6.3.2.2 Xử lý lỗi xác thực (SRC_SA.2)

SRC_SA.2.1 Đối với một người ký cụ thể, TW4S phải phát hiện khi nào xảy ra một số lần xác thực không thành công liên tiếp được xác định trước.

SRC_SA.2.2 Đối với một người ký cụ thể, khi đạt đến số lần xác thực không thành công được xác định, TW4S phải chặn quyền truy cập của người dùng này trong một khoảng thời gian hợp lý hoặc cho đến khi một người có vai trò quản trị mở khóa người dùng.

6.3.2.3 Ủy quyền xác thực người ký cho hệ thống bên ngoài (SRC_SA.3)

SRC_SA.3.1 Nếu việc xác thực người ký được ủy quyền cho một hệ thống bên ngoài, TSP phải đảm bảo rằng các yêu cầu được quy định trong Điều khoản SRC_SA.1 và SRC_SA.2 được hệ thống bên ngoài đáp ứng.

6.3.3 Tạo chữ ký số (SRC_DSC) - Thao tác mã hóa (SRC_DSC.1)

SRC_DSC.1.1 Các tham số thuật toán được sử dụng để tạo chữ ký bởi các hệ thống dịch vụ tin cậy phải được lựa chọn sao cho chúng có thể tồn tại trong suốt thời gian hiệu lực của chứng chỉ người ký.

6.4 Các yêu cầu bảo mật bổ sung cho SCAL2 (SRA)

6.4.1 Tổng quan

Các yêu cầu sau đây chỉ áp dụng cho TW4S triển khai mức độ đảm bảo kiểm soát duy nhất cấp 2. SAM xác thực trực tiếp hoặc gián tiếp người ký.

SAD được thu thập dưới sự kiểm soát hoàn toàn của người ký, với mức độ tin cậy cao, đảm bảo rằng khóa được xác định được người ký đã được xác thực sử dụng cho một (tập hợp) DTBS/R cụ thể.

6.4.2 Giao thức kích hoạt chữ ký và dữ liệu kích hoạt chữ ký (SRA_SAP)

6.4.2.1 Khả năng chống lại mối đe dọa (SRA_SAP.1)

SRA_SAP.1.1 Việc đăng ký của người ký phải được thực hiện theo quy định tại Phụ lục A, điều khoản phụ A.1, đối với mức độ đảm bảo trung bình hoặc cao hơn.

Các đặc điểm và thiết kế của phương tiện nhận dạng điện tử phải tuân theo quy định tại Phụ lục A, tiểu khoản A.2.1, đối với mức độ đảm bảo trung bình hoặc cao hơn.

Cơ chế xác thực phải được quy định trong Phụ lục A, tiểu khoản A.2.2, đối với mức độ đảm bảo trung bình hoặc cao hơn.

SRA_SAP.1.2 Các biện pháp kiểm soát phải được cung cấp, theo đánh giá rủi ro, để chống lại các mối đe dọa sau đây đối với SAD và việc sử dụng SAD: đoán mật khẩu trực tuyến, đoán mật khẩu ngoại tuyến, sao chép thông tin đăng nhập, lừa đảo trực tuyến (phishing), nghe lén, phát lại, chiếm đoạt phiên, tấn công trung gian (man-in-the-middle), đánh cắp thông tin đăng nhập, tấn công giả mạo và mạo danh.

SRA_SAP.1.3 SAP phải cung cấp các cơ chế mã hóa mạnh mẽ để bảo vệ các yếu tố xác thực khỏi sự xâm phạm của các mối đe dọa từ giao thức cũng như các cuộc tấn công mạo danh bên thứ ba dịch vụ tin cậy.

SRA_SAP.1.4 SAP phải được bảo vệ chống lại các cuộc tấn công phát lại, vượt qua và giả mạo giữa người ký và SCDev từ xa (ví dụ: bằng nonce, dấu thời gian hoặc mã thông báo phiên).

SRA_SAP.1.5 SAM phải được sử dụng trong môi trường được bảo vệ chống giả mạo, trong đó: — là một hệ thống dịch vụ tin cậy được đảm bảo đạt mức EAL 4 trở lên theo tiêu chuẩn TCVN 8709-3:2011, hoặc các tiêu chí đánh giá an toàn công nghệ thông tin được công nhận quốc gia hoặc quốc tế tương đương. Điều này phải hướng đến đích an toàn hoặc hồ sơ bảo vệ đáp ứng các yêu cầu của tài liệu này, dựa trên phân tích rủi ro và có tính đến các biện pháp an toàn vật lý và các biện pháp an toàn phi kỹ thuật khác; hoặc

SRA_SAP.1.6 Hệ thống SAP phải được thiết kế sao cho có thể giả định rằng SAD luôn được bảo vệ một cách dịch vụ tin cậy chống lại việc sao chép hoặc giả mạo bởi kẻ tấn công có tiềm năng tấn công cao.

SRA_SAP.1.7 SAP phải được thiết kế sao cho người ký luôn có thể bảo vệ một cách dịch vụ tin cậy việc kích hoạt khóa ký bởi SAD trước kẻ tấn công có tiềm năng tấn công cao.

6.4.2.2 Quản lý SAD (SRA_SAP.2)

SRA_SAP.2.1 SAD có thể là một tập hợp dữ liệu hoặc là kết quả của các hoạt động mã hóa sử dụng các tham số bắt buộc được liệt kê bên dưới.

SRA_SAP.2.2 SAD có thể được thu thập hoặc tạo ra trong môi trường của người ký bởi SIC hoặc từ xa bằng cách sử dụng SIC dưới sự kiểm soát của người ký.

SRA_SAP.2.3 SAD phải liên kết với mức độ tin cậy cao ít nhất các tham số sau: — một DTBS/R nhất định hoặc một tập hợp các DTBS/R,

— các mục để xác định người ký đã được xác thực, và

— Khóa ký mặc định hoặc đã chọn.

Nếu được hỗ trợ, việc vô hiệu hóa sử dụng nhiều hơn một DTBS/R sẽ khả thi trong những trường hợp không được pháp luật cho phép.

SRA_SAP.2.4 SAD chỉ được sử dụng để kích hoạt khóa ký nếu quá trình xác thực người ký thành công (ví dụ: bằng cách tính toán SAD sau khi xác thực thành công, hoặc bằng các phương tiện mã hóa khác).

SRA_SAP.2.5 SAD phải được chuyển đến SAM trong SAP.

SRA_SAP.2.6 SAD phải:

— được thu thập theo cách nằm dưới sự kiểm soát của người ký với mức độ tin cậy cao.

— được bảo vệ để đảm bảo mọi khóa được lưu trữ trong thiết bị đều an toàn và

— Bảo vệ mọi bí mật được sử dụng (một lần hoặc lâu dài) như được định nghĩa trong SRA_SAP.1.4 SRA_SAP.2.7. SAP phải được thiết kế sao cho nếu SAD được SAM nhận được, có thể giả định rằng SAD đã được gửi dưới sự kiểm soát duy nhất của người ký bằng các phương tiện mà người ký đang sở hữu.

SRA_SAP.2.8 SAD phải được xác minh sao cho khả năng các hoạt động như suy đoán, nghe lén, phát lại hoặc thao túng thông tin liên lạc bởi kẻ tấn công có tiềm năng tấn công cao có thể phá vỡ quá trình xác thực để kích hoạt chữ ký là cực kỳ thấp.

6.4.3 Quản lý khóa ký (SRA_SKM)

6.4.3.1 Tạo khóa ký (SRA_SKM.1)

SRA_SKM.1.1 Khóa ký của người ký phải được tạo và sử dụng trong SCDev mà:

— là một hệ thống dịch vụ tin cậy được đảm bảo đạt mức EAL 4 trở lên, được bổ sung bởi AVA_VAN.5 theo tiêu chuẩn TCVN 8709-3:2011, hoặc các tiêu chí đánh giá an toàn công nghệ thông tin tương đương được công nhận trong nước hoặc quốc tế. Điều này phải hướng đến đích an toàn hoặc hồ sơ bảo vệ đáp ứng các yêu cầu của tài liệu này, dựa trên phân tích rủi ro và có tính đến các biện pháp an toàn vật lý và các biện pháp an toàn phi kỹ thuật khác; hoặc

— Đáp ứng các yêu cầu được xác định trong tiêu chuẩn quốc gia TCVN 11295:2016 hoặc QCVN 137:2025/BKHCN (FIPS PUB 140-2 mức 3).

SCDev này phải được dành riêng để hỗ trợ các chức năng mã hóa cần thiết cho dịch vụ tạo chữ ký (tức là bao gồm tạo số ngẫu nhiên và thậm chí có thể cả mã hóa để hỗ trợ việc ký trên máy chủ).

SRA_SKM.1.3 Khi SCDev được sử dụng để tạo khóa ký khác với SCDev được sử dụng cho các thao tác ký, việc truyền khóa ký phải tuân thủ yêu cầu SRG_KM.4.1.

SRA_SKM.1.4 SCDev có thể chứa nhiều khóa ký cho cùng một người ký hoặc cho những người ký khác nhau.

Trong đó có nhiều khóa ký cho cùng một người ký hoặc cho những người ký khác nhau.

Trong SCDev, việc tách biệt quyền kiểm soát việc sử dụng các khóa phải được đảm bảo.

SRA_SKM.1.5 Khóa ký của người ký phải được liên kết với người ký với mức độ tin cậy cao thông qua phương tiện do SAP cung cấp.

Khóa ký của người ký SRA_SKM.1.6 không được sử dụng trước khi người ký được liên kết bởi TW4S.

SRA_SKM.1.7 TW4S có thể hỗ trợ một số cơ chế SAP và SAD khác nhau để kích hoạt khóa ký. Tuy nhiên, một khóa ký CHỈ được liên kết với một cơ chế SAD và SAP duy nhất.

6.4.3.2 Kích hoạt khóa ký (SRA_SKM.2)

SRA_SKM.2.1 TW4S phải yêu cầu người ký xuất trình SAD cho SAM để được xác thực và kích hoạt khóa ký.

SRA_SKM.2.2 SAP phải quản lý việc truyền SAD đến SAM theo cách đảm bảo rằng khóa ký nằm dưới sự kiểm soát của người ký với mức độ tin cậy cao.

SRA_SKM.2.3 Khóa ký của người ký chỉ được kích hoạt để sử dụng trong SCDev từ xa.

SRA_SKM.2.4 Khóa ký của người ký phải được kích hoạt bằng SAD được tạo ra với các yếu tố xác thực của người ký với tham chiếu khóa chính xác.

SRA_SKM.2.5 Khóa ký đã kích hoạt chỉ được sử dụng để ký các DTBS/R được SAP ủy quyền. SRA_SKM.2.6 Trường hợp DTBS/R cho SAD đến từ SCA, nguồn phải được xác thực. SRA_SKM.2.7 Người dùng có đặc quyền không được phép sử dụng khóa ký được cấp cho người ký.

SRA_SKM.2.8 Sau khi kích hoạt khóa ký và tạo chữ ký số, SAD của người ký không được lưu trữ ở bất kỳ đâu mà không được bảo vệ bởi TW4S.

Phụ lục A

(Quy định)

Yêu cầu đối với phương tiện nhận dạng điện tử, đặc điểm và thiết kế

A.1 Đăng ký

A.1.1 Ứng dụng và đăng ký

Mức độ đảm bảo	Các yếu tố cần thiết
Thấp	1. Đảm bảo người đăng ký nắm rõ các điều khoản và điều kiện liên quan đến việc sử dụng phương tiện nhận dạng điện tử. 2. Đảm bảo người đăng ký nắm rõ các biện pháp phòng ngừa an toàn được khuyến nghị liên quan đến phương tiện nhận dạng điện tử. 3. Thu thập các thông tin nhận dạng cần thiết để xác minh danh tính.
Trung bình	Tương tự mức độ đảm bảo thấp.
Cao	Tương tự mức độ đảm bảo thấp.

A.1.2 **Xác minh và chứng thực** danh tính (cá nhân)

Mức độ đảm bảo	Các yếu tố cần thiết
Thấp	1. Có thể giả định rằng người đó đang sở hữu bằng chứng được công nhận bởi cơ quan có thẩm quyền nơi nộp đơn xin cấp giấy tờ tùy thân điện tử và bằng chứng đó chứng minh danh tính được yêu cầu. 2. Có thể giả định rằng bằng chứng là xác thực, hoặc tồn tại theo một nguồn dịch vụ tin cậy và bằng chứng đó có vẻ hợp lệ. 3. Một nguồn tin dịch vụ tin cậy xác nhận rằng danh tính được khẳng định là có thật và có thể giả định rằng người khẳng định danh tính đó là cùng một người.
Trung bình	Bằng chứng được kiểm tra để xác định tính xác thực; hoặc, theo một nguồn dịch vụ tin cậy, nó được biết là tồn tại và liên quan đến một người có thật. và Các biện pháp đã được thực hiện để giảm thiểu rủi ro danh tính của người đó không phải là danh tính đã khai báo, chẳng hạn như tính đến rủi ro mất mát, bị đánh cắp, bị tạm đình chỉ, bị thu hồi hoặc hết hạn của bằng chứng; hoặc 2. Giấy tờ tùy thân được xuất trình trong quá trình đăng ký tại cơ quan có thẩm quyền nơi giấy tờ đó được cấp và giấy tờ đó có vẻ liên quan đến người xuất trình. Và

	Các biện pháp đã được thực hiện để giảm thiểu rủi ro danh tính của người đó không trùng khớp với danh tính đã khai báo, chẳng hạn như tính đến rủi ro mất mát, bị đánh cắp, bị tạm đình chỉ, bị thu hồi hoặc hết hạn giấy tờ; hoặc 3. Trường hợp các thủ tục đã được một tổ chức công hoặc tư nhân trong nước sử dụng trước đây cho mục đích khác với việc cấp phương tiện nhận dạng điện tử cung cấp sự đảm bảo tương đương với những quy định nêu trong mục A.1.2 về mức độ đảm bảo trung bình, thì tổ chức chịu trách nhiệm đăng ký không cần phải lặp lại các thủ tục trước đó, với điều kiện sự đảm bảo tương đương đó được xác nhận bởi một cơ quan đánh giá sự phù hợp tuân thủ các yêu cầu quy định hiện hành (xem ghi chú) hoặc bởi một cơ quan tương đương; hoặc 4. Trường hợp phương tiện nhận dạng điện tử được cấp dựa trên phương tiện nhận dạng điện tử hợp lệ đã được thông báo có mức độ đảm bảo trung bình hoặc cao, và có tính đến rủi ro thay đổi dữ liệu nhận dạng cá nhân, thì không cần phải lặp lại quy trình xác minh và chứng thực danh tính. Trường hợp phương tiện nhận dạng điện tử được sử dụng làm cơ sở chưa được thông báo, mức độ đảm bảo trung bình hoặc cao phải được xác nhận bởi một cơ quan đánh giá sự phù hợp tuân thủ các yêu cầu quy định hiện hành (xem ghi chú) hoặc bởi một cơ quan tương đương.
Cao	Phải đáp ứng được một trong hai yêu cầu của điểm 1 hoặc điểm 2: 1. Mức độ trung bình, cộng thêm một trong các phương án được liệt kê trong các điểm (a) đến (c) phải được đáp ứng: (a) Trường hợp người đó đã được xác minh là có bằng chứng nhận dạng bằng ảnh hoặc sinh trắc học được công nhận bởi cơ quan có thẩm quyền nơi nộp đơn xin phương tiện nhận dạng điện tử và bằng chứng đó thể hiện danh tính được yêu cầu, thì bằng chứng đó phải được kiểm tra để xác định xem nó có hợp lệ theo nguồn có thẩm quyền hay không; và người nộp đơn được xác định là người có danh tính được yêu cầu thông qua việc so sánh một hoặc nhiều đặc điểm thể chất của người đó với nguồn có thẩm quyền; hoặc (b) Trường hợp các thủ tục đã được một tổ chức công hoặc tư nhân trong nước sử dụng trước đây cho mục đích khác với việc cấp phương tiện nhận dạng điện tử cung cấp sự đảm bảo tương đương với những quy định nêu trong mục A.1.2 đối với mức độ đảm bảo cao, thì tổ chức chịu trách nhiệm đăng ký không cần phải lặp lại các thủ tục trước đó, với điều kiện sự đảm bảo tương đương đó được xác nhận bởi một cơ quan đánh giá sự phù hợp tuân thủ các yêu cầu quy định hiện hành

	(xem ghi chú) hoặc bởi một cơ quan tương đương và các bước được thực hiện để chứng minh rằng kết quả của các thủ tục trước đó vẫn còn hiệu lực; hoặc (c) Trường hợp phương tiện nhận dạng điện tử được cấp trên cơ sở phương tiện nhận dạng điện tử đã được thông báo hợp lệ với mức độ đảm bảo cao, và có tính đến rủi ro thay đổi dữ liệu nhận dạng cá nhân, thì không cần phải lặp lại quy trình xác minh và chứng thực danh tính. Trường hợp phương tiện nhận dạng điện tử được sử dụng làm cơ sở chưa được thông báo, thì mức độ đảm bảo cao phải được xác nhận bởi một cơ quan đánh giá sự phù hợp tuân thủ các yêu cầu quy định hiện hành (xem ghi chú) hoặc bởi một cơ quan tương đương và phải thực hiện các bước để chứng minh rằng kết quả của quy trình cấp phương tiện nhận dạng điện tử đã được thông báo trước đó vẫn còn hiệu lực. hoặc 2. Trường hợp người nộp đơn không xuất trình bất kỳ giấy tờ tùy thân có ảnh hoặc sinh trắc học nào được công nhận, thì các thủ tục tương tự được sử dụng bởi tổ chức chịu trách nhiệm đăng ký để thu thập giấy tờ tùy thân có ảnh hoặc sinh trắc học được công nhận đó sẽ được áp dụng.

A.1.3 Xác minh và chứng thực danh tính (pháp nhân)

Mức độ đảm bảo	Các yếu tố cần thiết
Thấp	1. Danh tính được tuyên bố của pháp nhân được chứng minh dựa trên bằng chứng được công nhận bởi cơ quan có thẩm quyền nơi nộp đơn xin cấp giấy tờ tùy thân điện tử. 2. Bằng chứng có vẻ hợp lệ và có thể được coi là xác thực, hoặc tồn tại theo một nguồn có thẩm quyền, trong đó việc đưa một pháp nhân vào nguồn có thẩm quyền là tự nguyện và được điều chỉnh bởi một thỏa thuận giữa pháp nhân đó và nguồn có thẩm quyền. 3. Không có nguồn thông tin dịch vụ tin cậy nào xác nhận rằng pháp nhân đó đang ở trong tình trạng pháp lý nào ngăn cản nó hoạt động với tư cách là pháp nhân đó.
Trung bình	Mức độ thấp, cộng thêm một trong các phương án được liệt kê trong điểm 1 đến 3 phải được đáp ứng: 1. Danh tính được tuyên bố của pháp nhân được chứng minh dựa trên bằng chứng được công nhận bởi cơ quan có thẩm quyền nơi nộp đơn xin cấp giấy tờ tùy thân điện tử, bao gồm tên, hình thức pháp lý và (nếu có) số đăng ký của pháp nhân, và bằng chứng đó được kiểm tra để xác định xem có phải là bằng chứng xác thực hay không, hoặc có được biết đến theo nguồn thông tin dịch vụ tin cậy hay không,

	trong trường hợp việc pháp nhân được đưa vào nguồn thông tin dịch vụ tin cậy là cần thiết để pháp nhân hoạt động trong lĩnh vực của mình và các biện pháp đã được thực hiện để giảm thiểu rủi ro danh tính của pháp nhân không trùng khớp với danh tính được tuyên bố, chẳng hạn như xem xét rủi ro mất mát, bị đánh cắp, bị tạm đình chỉ, bị thu hồi hoặc hết hạn giấy tờ; hoặc 2. Trường hợp các thủ tục đã được một tổ chức công hoặc tư nhân trong nước sử dụng trước đây cho mục đích khác với việc cấp phương tiện nhận dạng điện tử cung cấp sự đảm bảo tương đương với những quy định nêu trong mục A.1.3 về mức độ đảm bảo trung bình, thì tổ chức chịu trách nhiệm đăng ký không cần phải lặp lại các thủ tục trước đó, với điều kiện sự đảm bảo tương đương đó được xác nhận bởi một cơ quan đánh giá sự phù hợp tuân thủ các yêu cầu quy định hiện hành (xem ghi chú) hoặc bởi một cơ quan tương đương; hoặc 3. Trường hợp phương tiện nhận dạng điện tử được cấp dựa trên phương tiện nhận dạng điện tử hợp lệ đã được thông báo có mức độ đảm bảo trung bình hoặc cao, thì không cần phải lặp lại quy trình xác minh và chứng thực danh tính. Trường hợp phương tiện nhận dạng điện tử được sử dụng làm cơ sở chưa được thông báo, thì mức độ đảm bảo trung bình hoặc cao phải được xác nhận bởi một cơ quan đánh giá sự phù hợp tuân thủ các yêu cầu quy định hiện hành (xem ghi chú) hoặc bởi một cơ quan tương đương.
Cao	Mức độ trung bình, cộng thêm một trong các phương án được liệt kê trong điểm 1 đến 3 phải được đáp ứng: 1. Danh tính được khẳng định của pháp nhân được chứng minh dựa trên bằng chứng được công nhận bởi cơ quan có thẩm quyền nơi nộp đơn xin cấp giấy tờ định danh điện tử, bao gồm tên, hình thức pháp lý và ít nhất một mã định danh duy nhất đại diện cho pháp nhân được sử dụng trong bối cảnh quốc gia, và bằng chứng này được kiểm tra để xác định tính hợp lệ theo nguồn có thẩm quyền; hoặc 2. Trường hợp các thủ tục đã được một tổ chức công hoặc tư nhân trong nước sử dụng trước đây cho mục đích khác với việc cấp phương tiện nhận dạng điện tử cung cấp sự đảm bảo tương đương với những quy định nêu trong mục A.1.3 đối với mức độ đảm bảo cao, thì tổ chức chịu trách nhiệm đăng ký không cần phải lặp lại các thủ tục trước đó, với điều kiện sự đảm bảo tương đương đó được xác nhận bởi một cơ quan đánh giá sự phù hợp tuân thủ các yêu cầu quy định hiện hành (xem ghi chú) hoặc bởi một cơ quan tương đương và các bước được thực hiện để chứng minh rằng kết quả của thủ tục trước đó vẫn còn hiệu lực; hoặc

	3. Trường hợp phương tiện nhận dạng điện tử được cấp dựa trên phương tiện nhận dạng điện tử đã được thông báo hợp lệ với mức độ đảm bảo cao, thì không cần phải lặp lại quy trình xác minh và chứng thực danh tính. Trường hợp phương tiện nhận dạng điện tử được sử dụng làm cơ sở chưa được thông báo, thì mức độ đảm bảo cao phải được xác nhận bởi một cơ quan đánh giá sự phù hợp tuân thủ các yêu cầu quy định hiện hành (xem ghi chú) hoặc bởi một cơ quan tương đương và phải thực hiện các bước để chứng minh rằng kết quả của quy trình cấp phương tiện nhận dạng điện tử đã được thông báo trước đó vẫn còn hiệu lực.

A.1.4 Mối liên hệ giữa các phương tiện nhận dạng điện tử của cá nhân và pháp nhân

Trong trường hợp áp dụng, đối với sự ràng buộc giữa phương tiện nhận dạng điện tử của một cá nhân và phương tiện nhận dạng điện tử của một pháp nhân ('ràng buộc'), các điều kiện sau đây phải được áp dụng:

a) Việc tạm ngừng và/hoặc hủy bỏ ràng buộc là hoàn toàn có thể. Vòng đời của ràng buộc (ví dụ: kích hoạt, tạm ngừng, gia hạn, hủy bỏ) sẽ được quản lý theo các thủ tục được công nhận trên toàn quốc.

b) Cá nhân có phương tiện nhận dạng điện tử được liên kết với phương tiện nhận dạng điện tử của pháp nhân có thể ủy quyền việc thực hiện liên kết đó cho một cá nhân khác trên cơ sở các thủ tục được quốc gia công nhận. Tuy nhiên, cá nhân ủy quyền vẫn phải chịu trách nhiệm.

c) Việc ràng buộc sẽ được thực hiện theo cách sau:

Mức độ đảm bảo	Các yếu tố cần thiết
Thấp	1. Việc xác minh danh tính của cá nhân hành động thay mặt pháp nhân được xác nhận là đã thực hiện ở mức độ thấp hoặc cao hơn. 2. Việc ràng buộc được thiết lập trên cơ sở các thủ tục được công nhận trên toàn quốc. 3. Không có nguồn thông tin dịch vụ tin cậy nào xác nhận rằng cá nhân đó đang ở trong tình trạng pháp lý nào cản trở việc người đó hành động thay mặt cho pháp nhân.
Trung bình	Điểm 3 của cấp độ thấp, cộng thêm: 1. Việc xác minh danh tính của cá nhân hành động thay mặt pháp nhân được xác nhận là đã được thực hiện ở mức độ trung bình hoặc cao. 2. Việc ràng buộc được thiết lập trên cơ sở các thủ tục được công nhận trên toàn quốc, dẫn đến việc đăng ký ràng buộc trong một nguồn có thẩm quyền. 3. Việc ràng buộc đã được xác minh dựa trên thông tin từ một nguồn dịch vụ tin cậy.

Cao	Điểm 3 ở mức độ thấp và điểm 2 ở mức độ trung bình, cộng thêm: 1. Việc xác minh danh tính của cá nhân hành động thay mặt pháp nhân được xác nhận là đã được thực hiện ở mức độ cao. 2. Việc ràng buộc đã được xác minh dựa trên mã định danh duy nhất đại diện cho pháp nhân được sử dụng trong bối cảnh quốc gia; và dựa trên thông tin duy nhất đại diện cho cá nhân từ một nguồn có thẩm quyền.

A.2 Phương tiện nhận dạng điện tử và xác thực

A.2.1 Đặc điểm và thiết kế của phương tiện nhận dạng điện tử

Mức độ đảm bảo	Các yếu tố cần thiết
Thấp	1. Phương tiện nhận dạng điện tử sử dụng ít nhất một yếu tố xác thực. 2. Phương tiện nhận dạng điện tử được thiết kế sao cho bên phát hành thực hiện các bước hợp lý để kiểm tra xem nó chỉ được sử dụng dưới sự kiểm soát hoặc sở hữu của người được cấp quyền sở hữu.
Trung bình	1. Phương tiện nhận dạng điện tử sử dụng ít nhất hai yếu tố xác thực từ các danh mục khác nhau. 2. Phương tiện nhận dạng điện tử được thiết kế sao cho có thể giả định rằng nó chỉ được sử dụng khi nằm dưới sự kiểm soát hoặc sở hữu của người sở hữu nó.
Cao	Mức độ trung bình, cộng thêm: 1. Phương tiện nhận dạng điện tử bảo vệ chống lại việc sao chép và giả mạo, cũng như chống lại những kẻ tấn công có tiềm năng gây hại cao. 2. Phương tiện nhận dạng điện tử được thiết kế sao cho người sở hữu có thể bảo vệ nó một cách dịch vụ tin cậy khỏi việc người khác sử dụng.

A.2.2 Cơ chế xác thực

Bảng sau đây trình bày các yêu cầu cho từng cấp độ đảm bảo liên quan đến cơ chế xác thực, thông qua đó cá nhân hoặc pháp nhân sử dụng phương tiện nhận dạng điện tử để xác nhận danh tính của mình với bên tin cậy.

Mức độ đảm bảo	Các yếu tố cần thiết
Thấp	1. Việc công bố dữ liệu nhận dạng cá nhân phải được thực hiện sau khi xác minh dịch vụ tin cậy về phương tiện nhận dạng điện tử và tính hợp lệ của nó. 2. Trường hợp dữ liệu nhận dạng cá nhân được lưu trữ như một phần của cơ chế xác thực, thông tin đó được bảo mật để tránh mất mát và xâm phạm, bao gồm cả việc phân tích ngoại tuyến. 3. Cơ chế xác thực thực hiện các biện pháp kiểm soát an toàn để xác minh phương tiện nhận dạng điện tử, do đó, các hoạt động như đoán mò, nghe lén, phát lại hoặc

	thao túng thông tin liên lạc bởi kẻ tấn công có tiềm năng tấn công cơ bản nâng cao khó có thể phá vỡ cơ chế xác thực.
Trung bình	Mức độ thấp, bao gồm thêm: 1. Việc công bố dữ liệu nhận dạng cá nhân được thực hiện sau khi xác minh dịch vụ tin cậy các phương tiện nhận dạng điện tử và tính hợp lệ của chúng thông qua xác thực động. 2. Cơ chế xác thực thực hiện các biện pháp kiểm soát an toàn để xác minh phương tiện nhận dạng điện tử, sao cho khả năng các hoạt động như đoán mò, nghe lén, phát lại hoặc thao túng thông tin liên lạc bởi kẻ tấn công có tiềm năng tấn công trung bình có thể phá vỡ cơ chế xác thực là rất thấp.
Cao	Mức độ trung bình, bao gồm thêm: Cơ chế xác thực thực hiện các biện pháp kiểm soát an toàn để xác minh phương tiện nhận dạng điện tử, do đó, các hoạt động như đoán mò, nghe lén, phát lại hoặc thao túng thông tin liên lạc bởi kẻ tấn công có tiềm năng tấn công cao khó có thể phá vỡ cơ chế xác thực.

Thư mục tài liệu tham khảo

TCVN xxxx:2026 được xây dựng dựa trên cơ sở tham khảo tiêu chuẩn EN 419241-1: “Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements” của Ủy ban Tiêu chuẩn hóa Châu Âu, phiên bản 1.0, ngày 30/4/2018.