CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM

ĐỘC LẬP – TỰ DO – HẠNH PHÚC

TỔ CHỨC CUNG CẤP DỊCH VỤ

CHỨNG THỰC CHỮ KÝ SỐ CÔNG CỘNG (CA2)

Quy chế chứng thực

Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2

(CA2 Remote signing – CA2 Mobile Sign)

Phiên bản V1.0

CÔNG TY CỔ PHẦN CÔNG NGHỆ THẺ NACENCOMM

Hà Nội, 2021

Công ty cổ phần công nghệ thẻ Nacencomm
Digitally signed by Công ty cổ phần công nghệ thẻ Nacencomm
DN: C=VN, S=MST:0103930279, L="Tầng 5 số 2 Chùa Bộc, phường Trung Tự, Quận Đống Đa, thành phố Hà Nội, Việt Nam", O=Công ty cổ phần công nghệ thẻ Nacencomm, OU=Cổ BH, CN=Công ty cổ phần công nghệ thẻ Nacencomm, E=ketoanthue@cavn.vn
Reason: I am the author of this document
Location: your signing location here
Date: 2021.12.30 12:05:21 +07'00'
Foxit PDF Editor Version: 11.2.0

MỤC LỤC

1. GIỚI THIỆU VỀ CHÍNH SÁCH VÀ QUY TRÌNH QUY CHẾ DỊCH VỤ 9

1.1. TỔNG QUAN 9
1.2. TÊN VÀ DẤU HIỆU NHẬN DIỆN TÀI LIỆU 9
1.3. CÁC THÀNH PHẦN TRONG HỆ THỐNG DỊCH VỤ 10
1.3.1. Trung tâm chứng thực điện tử quốc gia (NEAC) - Bộ TTTT 10
1.3.2. Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign) 10
1.3.3. RA và các đại lý CA2 11
1.3.4. Thuê bao (bên ký) 11
1.3.5. Bên nhận 11
1.3.6. Bên cung cấp hệ thống ứng dụng nghiệp vụ 12
1.3.7. Các bên khác 12
1.4. MỤC ĐÍCH SỬ DỤNG CHỨNG THƯ SỐ 12
1.4.1. Các trường hợp sử dụng chứng thư số hợp lệ 12
1.4.2. Các trường hợp không được sử dụng chứng thư số 12
1.5. QUẢN LÝ QUY CHẾ CHỨNG THỰC 12
1.5.1. Tổ chức 12
1.5.2. Người liên hệ 13
1.5.3. Người quyết định sự phù hợp của Quy chế vận hành Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign) 13
1.5.4. Các thủ tục phê chuẩn Quy chế vận hành Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign) 13
1.6. ĐỊNH NGHĨA VÀ VIẾT TẮT 14
1.6.1. Thuật ngữ 14
1.6.2. Từ viết tắt 17

2. TRÁCH NHIỆM LƯU TRỮ VÀ CÔNG BỐ THÔNG TIN 18

2.1. LƯU TRỮ 18
2.2. CÔNG BỐ THÔNG TIN CỦA CA2 MOBILE SIGN 18
2.3. THỜI GIAN, TẦN SUẤT CÔNG BỐ THÔNG TIN 19
2.4. KIỂM SOÁT TRUY NHẬP THÔNG TIN 20

3. NHẬN DẠNG VÀ XÁC THỰC YÊU CẦU XIN CẤP CHỨNG THƯ SỐ 20

3.1. ĐẶT TÊN TRONG CHỨNG THƯ SỐ 20
3.2. XÁC MINH ĐỀ NGHỊ CẤP CHỨNG THƯ SỐ 21
3.3. XÁC MINH ĐỀ NGHỊ THAY ĐỔI CẶP KHÓA 23
3.4. XÁC MINH ĐỀ NGHỊ THU HỒI CHỨNG THƯ SỐ 24

4. CÁC YÊU CẦU ĐỐI VỚI VÒNG ĐỜI HOẠT ĐỘNG CỦA CHỨNG THƯ SỐ THUÊ BAO 24

4. 1. YÊU CẦU CẤP CHỨNG THƯ SỐ 24
4.2. XỬ LÝ YÊU CẦU CẤP CHỨNG THƯ SỐ 24

4.3. CẤP CHỨNG THƯ SỐ 25
4.4. XÁC NHẬN VÀ CÔNG BỐ CÔNG KHAI CHỨNG THƯ SỐ 25
4.5. SỬ DỤNG CẶP KHÓA VÀ CHỨNG THƯ SỐ 26
4.6. GIA HẠN CHỨNG THƯ SỐ 26
4.7. THAY ĐỔI CẶP KHÓA CỦA THUÊ BAO 27
4.8. THAY ĐỔI THÔNG TIN CHỨNG THƯ SỐ 28
4.9. TẠM DỪNG VÀ THU HỒI CHỨNG THƯ SỐ 29
4.10. KIỂM TRA TRẠNG THÁI CHỨNG THƯ SỐ 29
4.11. CHẤM DỨT DỊCH VỤ CỦA THUÊ BAO 29
4.12. LƯU TRỮ VÀ PHỤC HỒI KHÓA BÍ MẬT CỦA THUÊ BAO 30

5. KIỂM SOÁT, QUẢN LÝ VÀ VẬN HÀNH 30

5.1. KIỂM SOÁT AN TOÀN, AN NINH VẬT LÝ 31
5.1.1. Nơi đặt hệ thống và kết cấu 33
5.1.2. Kiểm soát ra vào 33
5.1.3. Kiểm soát truy cập 33
5.1.4. Điều hòa nhiệt độ và nguồn điện 34
5.1.5. Hư hại do nước 35
5.1.6. Phòng cháy chữa cháy 35
5.1.7. Chống nhiễu điện từ 35
5.1.8. Chống chịu lũ lụt, động đất 35
5.2. QUY TRÌNH KIỂM SOÁT 36
5.3. KIỂM SOÁT NHÂN SỰ 37
5.3.1. Yêu cầu và thủ tục về trình độ chuyên môn, kinh nghiệm 39
5.3.2. Thủ tục kiểm tra năng lực 39
5.3.4. Các vai trò yêu cầu tin cậy cao trong hệ thống 40
5.3.5. Định danh và xác nhận danh tính đối với từng vai trò trong hệ thống 41
5.3.6. Yêu cầu đào tạo 42
5.3.7. Tần suất đào tạo và yêu cầu cập nhật chuyên môn 43
5.3.8. Xử phạt đối với những hành động trái phép 43
5.3.9. Yêu cầu phân tách nhiệm vụ 43
5.3.10. Tài liệu 44
5.4. CÁC QUY TRÌNH GHI NHẬT KÝ HỆ THỐNG 44
5.4.1. Các loại sự kiện được ghi lại 45
5.4.2 Tần suất xử lý bản ghi log 45
5.4.3 Bảo vệ bản ghi log và đảm bảo tính khả dụng 45
5.5. LƯU TRỮ CÁC BẢN GHI 46
5.6. THAY ĐỔI KHÓA 46
5.7. XỬ LÝ SỰ CỐ, THẢM HỌA VÀ PHỤC HỒI 46
5.7.1. Xử lý sự cố thảm họa 48
5.7.2. Tài nguyên máy tính, phần mềm, và /hoặc dữ liệu gặp sự cố 48
5.7.3. Thủ tục khi khóa mật mã bị can thiệp 48

5.7.4. Khả năng duy trì hoạt động kinh doanh sau thảm họa *48*
5.8. DỪNG HOẠT ĐỘNG 48

6. ĐẢM BẢO AN TOÀN AN NINH VỀ KỸ THUẬT 49

6.1. TẠO VÀ PHÂN PHỐI CẶP KHÓA 49
6.1.1. Sinh khóa ký *49*
6.1.2. Liên kết phương thức định danh điện tử *51*
6.1.3. Liên kết chứng thư số *53*
6.1.4. Cung cấp định danh danh tính điện tử *53*
6.2. KIỂM SOÁT VÀ BẢO VỆ KHÓA BÍ MẬT 54
6.3. CÁC VẤN ĐỀ KHÁC LIÊN QUAN ĐẾN QUẢN LÝ CẶP KHÓA 54
6.4. KÍCH HOẠT DỮ LIỆU 56
6.5. KIỂM SOÁT AN NINH MÁY TÍNH 65
6.6. KIỂM SOÁT AN NINH QUY TRÌNH SỬ DỤNG 67
6.7. GIÁM SÁT AN NINH HỆ THỐNG MẠNG 67
6.9. AN NINH AN TOÀN VẬN HÀNH HỆ THỐNG 71
6.10. ĐỒNG BỘ HÓA THỜI GIAN HỆ THỐNG 72
6.11. KIỂM SOÁT AN NINH AN TOÀN VÒNG ĐỜI 72
6.12. AN NINH AN TOÀN HỆ THỐNG MẬT MÃ 73
6.13. DẤU THỜI GIAN (TIME-STAMPING) 74

7. ĐỊNH DẠNG CHỨNG THƯ SỐ, DANH SÁCH THU HỒI CHỨNG THƯ SỐ (CRL), GIAO THỨC KIỂM TRA TRẠNG THÁI CHỨNG THƯ SỐ TRỰC TUYẾN (OCSP) 74

7.1. ĐỊNH DẠNG CỦA CHỨNG THƯ SỐ 74
7.2. ĐỊNH DẠNG DANH SÁCH THU HỒI CHỨNG THƯ SỐ (CRL) 74
7.3. ĐỊNH DẠNG GIAO THỨC KIỂM TRA TRẠNG THÁI CHỨNG THƯ SỐ TRỰC TUYẾN (OCSP) 75

8. KIỂM ĐỊNH TÍNH TUÂN THỦ VÀ CÁC ĐÁNH GIÁ KHÁC 76

8.1. TẦN SUẤT VÀ CÁC TÌNH HUỐNG KIỂM TRA KỸ THUẬT 76
8.2. ĐƠN VỊ, NGƯỜI THỰC HIỆN KIỂM TRA KỸ THUẬT 77
8.3. CÁC NỘI DUNG KIỂM TRA KỸ THUẬT 77
8.4. XỬ LÝ KHI PHÁT HIỆN SAI SÓT 78
8.5. CÔNG BỐ KẾT QUẢ KIỂM TRA KỸ THUẬT 78
8.6. TẦN SUẤT VÀ CÁC TRƯỜNG HỢP ĐÁNH GIÁ 78
8.7. DANH TÍNH VÀ KHẢ NĂNG CỦA ĐƠN VỊ, NGƯỜI KIỂM TRA 78
8.8. LƯU TRỮ KẾT QUẢ 79
8.9. THU THẬP BẰNG CHỨNG 79

9. CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC 81

9.1. PHÍ/GIÁ 81
9.1.1. Phí cấp phát, gia hạn, tạm dừng, khôi phục, thu hồi chứng thư số ký số từ xa và chữ ký số từ xa *81*
9.1.2. Phí truy cập danh bạ chứng thư chữ ký số từ xa *81*
9.1.3. Phí truy cập thông tin trạng thái thu hồi (Dịch vụ xác minh hiệu lực của chứng thư số) *81*

91.4. Phí những dịch vụ khác như là thông tin về chính sách *81*
9.1.5. Phí duy trì hệ thống kiểm tra trạng thái chữ ký số *81*
9.1.6. Chính sách hoàn phí *82*
9.2. TRÁCH NHIỆM TÀI CHÍNH 82
9.2.1. Bảo lãnh Ngân hàng theo Nghị định 130/2018/NĐ-CP *82*
9.2.2. Bảo hiểm dịch vụ *82*
9.2.3. Trách nhiệm bồi thường thiệt hại cho thuê bao *82*
9.2.4. Trách nhiệm bồi thường của bên khác *82*
9.3. BẢO MẬT CÁC THÔNG TIN NGHIỆP VỤ 83
9.4. BẢO MẬT THÔNG TIN CÁ NHÂN 83
9.5. QUYỀN SỞ HỮU TRÍ TUỆ 84
9.6. TUYÊN BỐ VÀ CAM KẾT 84
9.7. TỪ CHỐI TRÁCH NHIỆM 84
9.8. GIỚI HẠN TRÁCH NHIỆM 84
9.9. BỒI THƯỜNG THIỆT HẠI 84
9.10. HIỆU LỰC CỦA QUY CHẾ CHỨNG THỰC 84
9.11. THÔNG BÁO VÀ TRAO ĐỔI THÔNG TIN VỚI CÁC BÊN THAM GIA 85
9.12. BỔ SUNG VÀ SỬA ĐỔI 85
9.13. THỦ TỤC GIẢI QUYẾT TRANH CHẤP 85
9.14. HỆ THỐNG PHÁP LÝ ĐIỀU CHỈNH 85
9.15. PHÙ HỢP VỚI PHÁP LUẬT HIỆN HÀNH 85
9.16. CÁC ĐIỀU KHOẢN CHUNG 85
9.17. CÁC ĐIỀU KHOẢN KHÁC 88

10. TỔ CHỨC NỘI BỘ 89

10.1. ĐÁNH GIÁ RỦI RO 89
10.2. QUẢN LÝ VÀ THEO DÕI SỰ CỐ 90
10.3. CHÍNH SÁCH BẢO MẬT THÔNG TIN 92
10.4. QUẢN LÝ TÀI SẢN 93
10.5. SAO LƯU DỰ PHÒNG 94
10.6. SỬ DỤNG CÁC PHƯƠNG TIỆN VẬN HÀNH KHÁC NHAU 94
10.7. HỦY RÁC 94

11. YÊU CẦU KỸ THUẬT APP CA2 GIAO TIẾP KÝ CHỮ KÝ SỐ TỪ XA 95

11.1. GIAO DIỆN (LƯỢC ĐỒ CÁC THÀNH PHẦN THEO KIẾN TRÚC VN HIỆN TẠI) 95
11.2. YÊU CẦU VỀ TẠO CHỮ KÝ SỐ ADES 96

Sử dụng bản quy chế này

Bản quy chế này được cung cấp cho các bên sử dụng Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign). Xem và phân phối tài liệu không bị giới hạn. Sử dụng lại nội dung trong tài liệu này phải được sự đồng ý bằng văn bản của CA2.

Bản quyền

Bản quyền thuộc Công ty Cổ phần Công nghệ thẻ Nacencomm

Tóm tắt

Bộ TTTT ngày 05 tháng 12 năm 2019 đã ban hành thông tư 16/2019/TT-BTTTT tạo điều kiện ứng dụng chữ ký số từ xa. Vô cùng thuận lợi cho người dân, chỉ cần sử dụng điện thoại thông minh, máy tính bảng thân thiện để ký số. Quy định của Bộ TTTT đưa ra các yêu cầu về cơ chế và thủ tục để người ký kiểm soát được dữ liệu và quyền ký đảm bảo tính chống chối bỏ theo quy định của pháp luật.

CA2 là tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng được tin tưởng sử dụng hơn 10 năm qua, là đơn vị cung cấp dịch vụ chứng thực chữ ký số công cộng thứ 2 được Bộ TTTT cấp phép từ đầu năm 2010. Với dịch vụ chữ ký số và chứng thực chữ ký số từ xa, CA2 áp dụng các quy chế, quy trình, thủ tục và giải pháp công nghệ đặc thù đảm tính an toàn, tin cậy và sự kiểm soát tuyệt đối của người ký.

Tài liệu cung cấp nội dung chính sách và quy chế vận hành Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign) tuân theo quy định của Thông tư 16/2019/TT-BTTTT ngày 05/12/2019 "Quy định danh mục tiêu chuẩn bắt buộc về chữ ký số và dịch vụ chứng thực chữ ký số từ xa" của Bộ Thông tin - Truyền thông; Mẫu quy chế quy định tại Thông tư 31/2020/TT-BTTTT; Bộ tiêu tiêu chí quy chế vận hành cung cấp dịch dịch vụ chữ ký số và chứng thực chữ ký số từ xa ETSI TS 119 431-1; ETSI TS 119 431-2; Cẩm nang NEAC-VCDC và Quy chế dịch vụ chứng thực chữ ký số công cộng CA2 (CA2 CP/CPS v1.4). Tham khảo bộ ISO 27000., và Quy định của Châu Âu số 910/2014.

Hướng dẫn chi tiết quy chế vận hành dịch vụ đối với CA2 Remote signing, và quy trình & thủ tục đăng ký, sử dụng dịch vụ của thuê bao, bên tích hợp ứng dụng nghiệp vụ và bên nhận.

Phương án kỹ thuật, giải pháp công nghệ thực hiện kết nối an toàn với bên tích hợp và cung cấp hệ thống ứng dụng nghiệp vụ áp dụng chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign).

CA2 khuyến nghị bên tích hợp ứng dụng, thuê bao, người nhận sử dụng dịch vụ có hiểu biết về khóa công khai, chứng thư số, chữ ký số từ xa; các quyền, nghĩa vụ và trách nhiệm của CA2, thuê bao CA2 Mobile Sign và các bên tham gia trước khi đăng ký và sử dụng dịch vụ.

Bên chấp nhận chữ ký số của thuê bao (người ký) chịu trách nhiệm cho quyết định về việc chấp nhận hay không chấp nhận chữ ký số của thuê bao. CA2 khuyến cáo bên nhận kiểm tra tính hợp lệ của chữ ký số và thông tin cung cấp trong chứng thực chữ ký số, trong chữ ký số, bằng cách kiểm tra với hệ thống xác thực trạng thái chứng thực chữ ký số trực tuyến kiểm tra tính hợp lệ chữ ký số của người ký, do CA2 cung cấp hoặc sử dụng công cụ chuẩn, trước khi chấp nhận chữ ký số qua công cụ của CA2, công cụ chuẩn hoặc hệ thống ứng dụng nghiệp vụ. Quy trình kiểm tra này được mặc mặc định thực hiện một cách tự động. Bên nhận có thể đề nghị để được hỗ trợ kiểm tra theo yêu yêu cầu.

Các quy định của tài liệu này có thể được sửa đổi theo thời gian vào ngày hoặc sau ngày có hiệu lực của văn bản.

Căn cứ:

- Nghị định 130/2018/NĐ-CP ngày 27/09/2018 “Quy định chi tiết thi hành luật giao dịch điện tử về chữ ký số và dịch vụ chứng thực chữ ký số”;
- Thông tư 16/2019/TT-BTTTT ngày 05/12/2019 “Quy định danh mục tiêu chuẩn bắt buộc về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa”;
- Mẫu quy định tại Thông tư 31/2020/TT-BTTTT ngày 30/10/2020 “Ban hành Quy chế chứng thực của tổ chức cung cấp dịch vụ chứng thực chữ ký số Quốc gia”;
- Bộ tiêu chí về quy chế vận hành dịch vụ chữ ký số và chứng thực chữ ký số từ xa ETSI TS 119 431-1;
- Tham chiếu các bộ tiêu chí ETSI TS 119 431-2; ETSI TS 119 432; EN 419 241-1:2018; EN 419 241-2:2019; EN 419 221-221-5:2018
- Hướng dẫn của NEAC về dịch dịch chữ ký số và chứng thực chữ ký số từ xa;
- Quy chế chứng thực chữ ký số công cộng CA2, phiên bản 1.4.

- Hệ thống quản lý an ninh thông tin ISO/IEC 27001:2013 của CA2;
- Quy chế chính sách bảo đảm an toàn, an ninh cấp độ;
- Quy định Châu Âu số 910/2014.

1. GIỚI THIỆU VỀ CHÍNH SÁCH VÀ QUY TRÌNH QUY CHẾ DỊCH VỤ

1.1. Tổng quan

Tài liệu cung cấp nội dung chính sách và quy chế vận hành Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign) tuân theo quy định của Thông tư 16/2019/TT-BTTTT ngày 05/12/2019 "Quy định danh mục tiêu chuẩn bắt buộc về chữ ký số và dịch vụ chứng thực chữ ký số theo mô hình ký số trên thiết bị di động và ký số từ xa" của Bộ Thông tin và Truyền thông; Mẫu quy định tại Thông tư 31/2020/TT-BTTTT; ETSI TS 119 431-1; ETSI TS 119 431-2; Cẩm nang NEAC-VCDC và CA2 CP/CPS v1.4.

CA2 cung cấp dịch vụ Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign) cho các tổ chức, doanh nghiệp và cá nhân để thực hiện giao dịch trong môi trường mạng mở an toàn và có giá trị pháp lý theo quy định của pháp luật Việt Nam trong việc sử dụng chữ ký số phục vụ chống chối bỏ, xác thực và toàn vẹn các tài liệu và giao dịch điện tử.

Tài liệu này mô tả tập hợp các quy định và thủ tục cấp phát và quản lý dịch vụ đối với hệ thống CA2 và thủ tục quy định đăng ký, sử dụng chứng thư số đối với thuê bao của CA2, bên cung cấp ứng dụng nghiệp vụ và bên nhận. Tài liệu quy định các quy trình thủ tục đăng ký, cấp, quản lý, tạm dừng, thu hồi và cấp lại chứng thư số, ký số trong Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign). Là tài liệu pháp lý ràng buộc tất cả các bên tham gia sử dụng và xác nhận chứng thư số CA2 Remote Signing; điều chỉnh quyền, nghĩa vụ và trách nhiệm các bên trong tài liệu này.

Quy chế này cũng công bố các thuật toán ký số, tham số, sinh khóa cũng như các thuật toán và tham số áp dụng cho Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign).

Quy chế được công bố 24/7 trên cổng thông tin điện tử của Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign).

1.2. Tên và dấu hiệu nhận diện tài liệu

Tên tài liệu: Quy chế chứng thực Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign).

Phiên bản: v1.0

Ngày tạo: 31/05/2021

OID: 1.3.6.1.5.5.7.2.1

1.3. Các thành phần trong hệ thống dịch vụ

Các bên tham gia vào hệ thống Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign) bao gồm:

Trung tâm chứng thực điện tử quốc gia (NEAC) - Bộ TTTT

Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign)

RA và đại lý CA2

Thuê bao (Bên ký)

Bên nhận

Bên cung cấp hệ thống ứng dụng nghiệp vụ

1.3.1. Trung tâm chứng thực điện tử quốc gia (NEAC) - Bộ TTTT

NEAC RootCA là cấp cao nhất trong hạ tầng chứng thực chữ ký số công cộng Việt Nam.

Cấp chứng thư số cho các hệ thống chứng thực chữ ký số công cộng theo giấy phép của Bộ Thông tin và Truyền thông.

Thiết lập các thông số kỹ thuật để vận hành cơ sở hạ tầng khóa công khai cho xác thực chữ ký số công cộng.

Kiểm tra kỹ thuật, điều phối các hoạt động xử lý sự cố liên quan đến dịch vụ chứng thực chữ ký số công cộng.

Thu thập, tổ chức, phân tích, thống kê và tổng hợp số liệu về dịch vụ chứng thực chữ ký số công cộng.

1.3.2. Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign)

Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign), thuộc Công ty Cổ phần Công nghệ thẻ NACENCOMM.

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng CA2, thuộc công ty Cổ phần Công nghệ thẻ NACENCOMM.

Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng CA2 là đơn vị được Bộ Thông tin và Truyền thông cấp phép cung cấp dịch vụ. Giấy phép số: 375/GP-BTTTT ngày 31/08/2020.

Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign) là đơn vị được Bộ Thông tin và Truyền thông cấp pháp cung cấp dịch vụ. Giấy phép số ...

CA2 Remote signing cung cấp Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign) cho các tổ chức, doanh nghiệp và cá nhân để thực hiện giao dịch trong môi trường mạng mở an toàn và có giá trị pháp lý theo quy định của pháp luật Việt Nam.

CA2 Remote signing triển khai mô hình PKI có mức độ tin cậy cao, áp dụng kiến trúc Offline RootCA. Core CA và các thành phần lõi cung cấp dịch vụ ủy thác ký số từ xa được cấp chứng nhận bởi các tổ chức quốc tế uy tín.

Dịch vụ ký số và chứng thực chữ ký số từ xa CA2 Mobile Sign vận hành tuân thủ theo hệ thống quy chế, bao gồm:

- Hệ thống quản lý an ninh thông tin ISO/IEC 27001:2013
- Quy chế chính sách đảm bảo an toàn, an ninh cấp độ
- Quy chế chứng thực Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign).
- Quy chế chứng thực chữ ký số công cộng CA2 CP/CPS phiên bản mới nhất
- Quy chế dịch vụ cấp dấu thời gian số CA2 TSA TP/TPS
- Hệ thống quy trình nghiệp vụ liên quan
- Những văn bản khác có liên quan theo quy định của pháp luật.

1.3.3. RA và các đại lý CA2

RA, đại lý CA2 là đơn vị ký với CA2 một hợp đồng ủy quyền tham gia thẩm định đăng ký và cung cấp dịch vụ theo quy định của pháp luật. Quyền và nghĩa vụ của hai bên được quy định trong hợp đồng hợp tác giữa hai bên.

1.3.4. Thuê bao (bên ký)

Là các tổ chức, cá nhân, doanh nghiệp, cá nhân thuộc tổ chức doanh nghiệp sử dụng Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign). Quyền và nghĩa vụ của hai bên được quy định trong hợp đồng cung cấp dịch vụ giữa hai bên.

1.3.5. Bên nhận

Là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký là thuê bao CA2 Remote signing, kiểm tra chữ ký số của người ký để đảm bảo tính chống chối bỏ

của người ký đối với thông điệp dữ liệu nhận được theo quy định của pháp luật và tiến hành các hoạt động, giao dịch có liên quan.

1.3.6. Bên cung cấp hệ thống ứng dụng nghiệp vụ

Là tổ chức, cá nhân cung cấp hệ thống, ứng dụng có sử dụng tích hợp chữ ký số từ xa hỗ trợ cho các nghiệp vụ của người sử dụng để đảm bảo an ninh an toàn và giá trị pháp lý của các nghiệp vụ, thông điệp, tài liệu, văn bản... theo quy định của pháp luật đối với giá trị pháp lý của chữ ký số tương tự như chữ ký tay.

1.3.7. Các bên khác

Đối với một số hoạt động nhất định, liên quan đến Luật Giao dich điện tử, các nghị định và thông tư liên quan, CA2 Remote signing có thể liên quan đến các bên bên ngoài. Các quan hệ liên quan đến các hoạt động này sẽ được quy định trong thỏa thuận. Thỏa thuận này sẽ quy định các quyền và nghĩa vụ của các bên bên ngoài liên quan đến hoạt động cung cấp dịch vụ.

CA2 Remote signing có thể ký hợp đồng với các nhà thầu phụ và nhà cung cấp dịch vụ, chẳng hạn như các trung tâm dữ liệu chuyên biệt, để đặt máy chủ và thiết bị dự phòng tin cậy và an toàn, nhà cung cấp hệ thống và dịch vụ đám mây, nhà cung cấp dịch vụ nhận dạng tự động, dịch vụ CNTT và các nhà cung cấp khác. Khi làm việc với nhà thầu phụ và nhà cung cấp. CA2 Remote signing yêu cầu họ tuân thủ nghiêm ngặt các quy trình, phù hợp với bản Chính sách và Quy chế này.

1.4. Mục đích sử dụng chứng thư số

1.4.1. Các trường hợp sử dụng chứng thư số hợp lệ

Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign) chỉ được sử dụng theo đúng phạm vi quy định trong hợp đồng giữa CA2 và thuê bao và theo quy định của pháp luật.

1.4.2. Các trường hợp không được sử dụng chứng thư số

Nghiêm cấm việc sử dụng Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign) trái với quy định trong hợp đồng giữa CA2 và thuê bao và trái với quy định của pháp luật.

1.5. Quản lý quy chế chứng thực

1.5.1. Tổ chức

- Công ty Cổ phần Công nghệ thẻ NACENCOMM
- Trung tâm chứng thực số công cộng CA2

- Dịch vụ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign)
- Địa chỉ: Tầng 3 Tòa nhà Bohemia số 25 Nguyễn Huy Tưởng, phường Thanh Xuân Trung, Quận Thanh Xuân, thành phố Hà Nội.
- Website: www.cavn.vn

1.5.2. Người liên hệ

- Điện thoại: (84-4) 3576 5146
- Đường dây nóng: 1900 54 54 07
- Email: support@cavn.vn
- Ông: Đặng Vũ Hồng Quang
- Mobile: 0903 275027
- Email: quangdvh@cavn.vn
- Địa chỉ: Tầng 3 Tòa nhà Bohemia số 25 Nguyễn Huy Tưởng, phường Thanh Xuân Trung, Quận Thanh Xuân, thành phố Hà Nội.
- Website: www.cavn.vn

1.5.3. Người quyết định sự phù hợp của Quy chế vận hành Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign)

- Ông Hoàng Quốc Khánh
- Mobile: 0913234 234
- Email: khanh@cavn.vn

1.5.4. Các thủ tục phê chuẩn Quy chế vận hành Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign)

CA2 có quy định cụ thể về quy trình cập nhật, sửa đổi và ban hành Quy chế chứng thực Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign). Bao gồm nhưng không giới hạn như dưới đây:

- Từng phiên bản của Quy chế được xây dựng và rà soát bởi những nhân sự có chuyên môn cao.
- Quy chế chỉ có hiệu lực ban hành đưa vào sử dụng sau khi được phê duyệt bởi ban lãnh đạo có thẩm quyền
- Bản Quy chế có hiệu lực được công bố công khai tại cổng điện tử www.cavn.vn
- Bản Quy chế và bất cứ cập nhật phải được thông báo ngay cho toàn thể Công ty và các bên liên quan.

- CA2 tổ chức hệ thống nhân sự chuyên trách cho việc rà soát, trình phê duyệt và thẩm định phê duyệt Quy chế trước khi công bố.
- Quy chế dựa trên các yêu cầu được nêu trong ETSI TS 119 431-2 và trong ETSI TS 119 431-1, CA2 Remote Signing thực hiện đánh giá rủi ro để đánh giá các yêu cầu cung cấp dịch vụ và xác định các yêu cầu bảo mật như được mô tả trong tài liệu này;
- Quy chế phải được rà soát để đảm bảo sát thực với hệ thống triển khai thực tế. Việc rà soát trên sẽ được thực hiện định kỳ hàng năm.

1.6. Định nghĩa và viết tắt

1.6.1. Thuật ngữ

Các khái niệm, thuật ngữ được sử dụng trong Quy chế vận hành Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign) được giải thích như dưới đây:

Chứng thư số: Hay còn gọi là chứng thư số chứng thực khóa công khai, là một dạng chứng thực kỹ thuật số do Tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng CA2 cấp cho một khóa công khai bằng cách ràng buộc khóa công khai của thuê bao với các thông tin định danh danh tính của thuê bao có khóa riêng là một cặp với khóa công khai được chứng thực này.

Chứng thư số ký số từ xa: Chứng thư chứng thực cho khóa công khai của thuê bao sử dụng dịch vụ ủy thác ký số từ xa. Chứng thư số giúp xác thực danh tính của người ký từ xa bào gồm các thông tin định danh như: Thông tin định danh thuê bao, mã định danh điện thoại thông minh thuê bao sở hữu, mã định danh khóa ký, mã định danh duy nhất toàn cầu. Chứng thư số này đảm bảo tính toàn vẹn và xác thực đối với danh tính của người ký số từ xa.

Ký số: Là việc đưa khóa bí mật vào một chương trình phần mềm để tự động tạo và gắn chữ ký số vào thông điệp dữ liệu.

Chữ ký số: Là một dạng chữ ký kỹ thuật số được tạo ra bằng sự biến đổi một thông điệp dữ liệu sử dụng hệ thống mật mã không đối xứng. Theo đó người có được thông điệp dữ liệu ban đầu và khóa công khai của người ký có thể xác định được chính xác:

- Việc biến đổi nêu trên được tạo ra bằng đúng khóa bí mật tương ứng với khóa công khai trong cùng một cặp khóa;
- Sự toàn vẹn nội dung của thông điệp dữ liệu kể từ khi thực hiện việc biến đổi nêu trên.

CA2 Remote Singing: Dịch vụ ký số và chứng thực chữ ký số từ xa CA2, dịch vụ ủy thác ký số từ xa được Bộ Thông tin Truyền thông cấp phép. Dịch vụ ký số từ xa CA2 Remote Signing đảm bảo chỉ duy nhất người ký kiểm soát khóa ký và kích hoạt ký số ở mức độ kiểm soát cao nhất SCAL2 theo quy định eIDAS của Châu Âu.

Thuê bao: Là tổ chức, cá nhân, cá nhân thuộc tổ chức đăng ký, chấp nhận sử dụng dịch vụ ký số và chứng thực chữ ký số từ xa CA2 Remote Signing.

Người ký: Là tổ chức, cá nhân, cá nhân thuộc tổ chức đăng ký, chấp nhận sử dụng dịch vụ ký số và chứng thực chữ ký số từ xa CA2 Remote Signing.

Thuê bao ký số từ xa: Là tổ chức, cá nhân, cá nhân thuộc tổ chức đăng ký, chấp nhận sử dụng dịch vụ ký số và chứng thực chữ ký số từ xa CA2 Remote Signing.

Chữ ký số từ xa: Là chữ ký số mà thuê bao ủy thác cho CA2 Remote Signing quản lý khóa ký của người ký, dưới sự kiểm soát duy nhất của người ký về việc kích hoạt khóa ký để có ký chữ ký số của thuê bao.

Bên ký: Là thuê bao CA2 Mobile Sign dùng khóa bí mật của mình để ký số vào thông điệp dữ liệu dưới tên của mình.

Bên nhận: Là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký, sử dụng chứng thư số của người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan.

Tổ chức cung cấp dịch vụ chứng thực chữ ký số từ xa: Là tổ chức cung cấp dịch vụ chứng thực chữ ký số thực hiện hoạt động cung cấp dịch vụ chứng thực khóa công khai chữ ký số của thuê bao ký số từ xa.

Khóa mật mã tạo chữ ký: Khóa riêng cùng cặp với khoá công khai nằm trong chứng thư số chứng thực khóa công khai và được sử dụng để ký số.

Danh sách thu hồi chứng thư số (Certificate Revocation List - CRL): Một cơ sở dữ liệu hoặc một danh sách các chứng thư số do CA2 thu hồi hay hủy bỏ trước thời hạn so với thời hạn hiệu lực của chứng thư số.

Sinh khóa (Key Generation): là quá trình tạo một cặp khóa mật mã phi đối xứng bao gồm khóa riêng và khóa công khai.

Cặp khóa (Key Pair): Hai khóa liên kết với nhau một cách chính xác (một khóa riêng và tương ứng với nó là một khóa công khai), có đặc điểm là: (i) một khóa có thể được sử dụng để mã hóa các thông tin và chỉ có thể được giải mã bằng chiếc khóa cùng cặp còn lại; (ii) Nếu biết một khóa cũng không thể có khả năng biết được một khóa còn lại.

Kiểm tra trạng thái trực tuyến (Online Certificate Status Protocol): trạng thái thời gian thực được kiểm tra trực tuyến về thời hạn hiệu lực của chứng thư số. Kiểm tra trạng thái trực tuyến liên quan tới một CRL bao gồm việc kiểm tra CRL công bố mới nhất.

Khóa riêng (Private Key): Một khóa bí mật của người giữ chứng thư số, được sử dụng để ký chữ ký số và giải mã thông tin hoặc tài liệu được mã hóa bởi khóa công khai tương ứng.

Khóa công khai (Public Key): Một khóa công khai thuộc sở hữu của người giữ khoá riêng cùng cặp với khoá công khai này. Khoá công khai được phát tán để người nhận xác thực người "ký" điện tử (người giữ khóa bí mật cùng cặp với khoá công khai này) và người gửi sử dụng khoá công khai này để mã hoá dữ liệu trước khi gửi đi, chỉ có người nhận giữ khóa bí mật cùng cặp với khoá công khai này mới giải mã được

Cơ sở hạ tầng khóa công khai (Public Key Infrastructure - PKI): Tập hợp các kiến trúc, tổ chức, kỹ thuật, nguyên tắc thực hiện, thủ tục để hỗ trợ trong việc thực hiện và điều hành chứng thư số dựa trên hệ thống mã hóa khóa công khai.

Tổ chức đăng ký (Registration Authority - RA): là một tổ chức được CA2 ký hợp đồng đại diện có quyền tiếp nhận và giải quyết các đơn xin cấp chứng thư số và xác minh nhận dạng các chủ thể cuối cùng cũng như chứng thực các thông tin có trong đơn xin chứng thư số tuân theo những điều khoản theo Quy chế này và các thỏa thuận có liên quan.

Danh bạ chứng thư số (Repository): Hệ thống trực tuyến do CA2 phát hành duy trì để lưu trữ và phục hồi các chứng thư số hoặc các thông tin liên quan tới thuê bao chứng thư số, bao gồm các thông tin về thời hạn hiệu lực và sự thu hồi chứng thư số.

Tạm dừng chứng thư số: Là làm mất hiệu lực của chứng thư số một cách tạm thời từ một thời điểm xác định.

Thu hồi chứng thư số: Là làm mất hiệu lực của chứng thư số một cách vĩnh viễn từ một thời điểm xác định.

HSM chuyên dụng: Thiết bị mật mã phần cứng chuyên dụng đạt mức an toàn bảo mật EAL4+, đạt chứng chỉ EN 419 221-5 trở lên.

SAM chuyên dụng: Mô-đun kích hoạt chữ ký số chuyên dụng được cấp chứng chỉ EN 419 241-2, vận hành bên trong HSM chuyên dụng.

SIC Thành phần tương tác người ký: Giao diện tương tác người ký, với giao diện kỹ thuật tuân thủ SCAL2 do SAM chuyên dụng thực hiện.

Dữ liệu kích hoạt ký số SAD: Bộ dữ liệu kích hoạt chữ ký số, SAD được ký số bởi người ký để phục vụ xác thực kích hoạt khóa ký, bộ dữ liệu SAD bao gồm nhưng không giới hạn: mã định danh thuê bao, mã định danh điện thoại thông minh thuê bao sở hữu, mã định danh khóa ký, mã định danh duy nhất toàn cầu, mã định danh phiên, chuỗi định danh dữ liệu yêu cầu ký số.

Dữ liệu yêu cầu ký số DTBS/R: Chuỗi định danh duy nhất của thông điệp yêu cầu ký số.

Định danh danh tính của thuê bao: Chứng thư chữ ký số từ xa của thuê bao, bao gồm định danh thiết bị di động do thuê bao sở hữu và các thông tin định danh khác khẳng định danh tính của thuê bao.

1.6.2. Từ viết tắt

API	Application Programming Interface
CA	Certification Authority
CRL	Certificate Revocation List
PIN	Personal Identification Standard
PKI	Public Key Infrastructure
RA	Registration Authority
HSM	Hardware Security Module
CM	Cryptographic Module
CC	Common Criteria
drQSCD	Distributed Remote QSCD
DTBS/R	Data To Be Signed / Representation
EAL	Evaluation Assurance Level
JWT	Json Web Token

OTP	One Time Password
FIPS	Federal Information Processing Standards
QSCD	Qualified Signature Creation Device
RSA	Rivest, Shamir, Adleman
SCAL2	Sole Control Assurance Level 2
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SIC	Signer’s Interaction Component

2. TRÁCH NHIỆM LƯU TRỮ VÀ CÔNG BỐ THÔNG TIN

2.1. Lưu trữ

Tổ chức cung cấp dịch vụ chữ ký số và chứng thực chữ ký từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign) có trách nhiệm lưu trữ thông tin, bao gồm:

- Lưu trữ và sử dụng thông tin của thuê bao một cách bí mật, an toàn và chỉ được sử dụng thông tin này vào mục đích liên quan đến chứng thư số.
- Lưu trữ đầy đủ, chính xác và cập nhật thông tin của thuê bao phục vụ việc cấp chứng thư số trong suốt thời gian chứng thư số có hiệu lực và trong thời gian ít nhất 05 năm, kể từ khi chứng thư số hết hiệu lực.
- Lưu trữ đầy đủ, chính xác và cập nhật danh sách các chứng thư số có hiệu lực, đang tạm dừng và đã hết hiệu lực và cho phép, hướng dẫn người sử dụng Internet truy nhập trực tuyến 24 giờ trong ngày và 7 ngày trong tuần.
- Lưu trữ toàn bộ thông tin liên quan đến việc tạm đình chỉ hoặc thu hồi giấy phép và các cơ sở dữ liệu về thuê bao, chứng thư số trong thời gian ít nhất 05 (năm) năm, kể từ khi giấy phép bị tạm đình chỉ hoặc thu hồi.

2.2. Công bố thông tin của CA2 Remote signging

Công bố sẽ thực hiện tại website CA2 http://www.cavn.vn và có phương án tốt nhất để thông báo thành công đến các bên liên quan đảm bảo cập nhật kịp thời.

Thông tin bao gồm các phiên bản của Quy chế về điều khoản, điều kiện và phương thức sử dụng khóa ký chữ ký số từ xa. Hệ thống danh bạ chứng thực khóa công khai chữ ký số từ xa bị thu hồi.

Kênh cung cấp cấp thông tin công bố luôn được đảm bảo sẵn sàng truy cập cho các bên liên quan và không có bất kỳ giới hạn truy cập.

Trường hợp sự cố nghiêm trọng vượt giới hạn kiểm soát CA2 sẽ áp dụng quy trình ứng cứu để đảm bảo kênh thông tin trực tuyến được cung cấp phù hợp trong phạm vi thời gian gián đoạn tối thiểu được cho phép.

Chứng thư số khóa công khai của người ký sẽ được công bố ngay sau khi hoàn thành việc thẩm định sau cấp và có xác nhận của thuê bao.

CA2 sẽ thực hiện công bố công khai thông tin và hệ thống danh bạ về chữ ký số và chứng thực chữ ký số từ xa của thuê bao ngay sau khi hoàn thành thủ tục cho thuê bao.

Hệ thống kênh công bố thông tin bao gồm nhưng không giới hạn:

1) Chứng thư số của NEAC Root_CA - Bộ TTTT;

2) Chứng thư số của CA2;

3) Chứng thư số của thuê bao;

4) Danh sách Chứng thư số bị thu hồi (CRL);

5) Dịch vụ kiểm tra trạng thái chứng thư số trực tuyến (OCSP);

6) Quy chế chứng thực Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign);

7) Các thông tin liên quan khác.

2.3. Thời gian, tần suất công bố thông tin

1) CA2 thực hiện công bố bản Quy chế chứng thực Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign) mới hoặc sửa đổi ngay sau khi được phê duyệt.

2) CA2 có trách nhiệm duy trì 24 giờ trong ngày và 7 ngày trong tuần trên trang tin điện tử của mình những thông tin sau:

- Quy chế chứng thực Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign).
- Danh sách chữ ký số từ xa có hiệu lực, bị tạm dừng, bị thu hồi của thuê bao.
- Trạng thái trực tuyến chứng thư số.
- Những thông tin cần thiết khác .

3) Thời gian cập nhật thông tin công bố:

- Bản Quy chế và các văn bản, tài liệu liên quan sẽ được cập nhật ngay sau khi được ký duyệt ban hành.

- Chứng thư số được cập nhật ngay sau khi hoàn thành thủ tục cấp.

- CRL được cập nhật tự động theo khung giờ 2 tiếng.

- CRL được cập nhật ngay sau khi hoàn thành các công việc hủy, tạm dừng, thu hồi chữ ký số từ xa.

2.4. Kiểm soát truy nhập thông tin

CA2 sẽ không áp đặt bất kỳ sự kiểm soát truy cập nào đối với:

(1) Quy chế chứng thực Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign);

(2) Danh bạ chứng thực khóa công khai chữ ký số từ xa;

(3) Danh sách chứng thư số bị thu hồi CRL.

3. NHẬN DẠNG VÀ XÁC THỰC YÊU CẦU XIN CẤP CHỨNG THƯ SỐ

3.1. Đặt tên trong chứng thư số

Ngoài những trường hợp ngoại lệ được chỉ ra trong chính sách chứng thư số, quy chế chứng thực, tên trong chứng thư số do CA2 cấp phải được kiểm tra tính xác thực.

3.1.1 Quy định các kiểu tên

- VID Stamp: Đặt tên theo quyết định thành lập hoặc giấy đăng ký kinh doanh hoặc tài liệu tương đương khác của tổ chức.
- VID Sign: Đặt tên theo Chứng minh nhân dân, căn cước công dân, hộ chiếu hoặc chứng thực cá nhân hợp pháp.
- VID Web: Đặt tên theo tên miền website đăng ký hợp lệ của đơn vị đăng ký sử dụng dịch vụ CA2.

3.1.2 Quy định yêu cầu đối với tên

- Tên trong chứng thư số do CA2 ban hành cho phép xác định được nhận dạng của đối tượng sở hữu của chứng thư số.

3.1.3 Quy định cú pháp định dạng tên

- CA2 không đặt tên khác với quy định tại "Quy định các kiểu tên"

3.1.4 Quy định tính duy nhất của tên

- VID Stamp: Bao gồm tên tổ chức và trường mã số thuế hoặc mã số tổ chức hợp lệ

- VID Sign: Bao gồm tên cá nhân và trường số chứng minh nhân dân, hoặc số hộ chiếu, hoặc số chứng thực cá nhân hợp pháp.
- VID Web: Tên miền hợp lệ.

3.2. Xác minh đề nghị cấp chứng thư số

3.2.1 Phương pháp chứng minh sở hữu khóa riêng

- Thuê bao phải được chứng minh thuê bao thực sự sở hữu khóa riêng tương ứng với khóa công khai được đề nghị cấp chứng thư số.
- Các phương pháp chứng minh thuê bao thực sự sở hữu khóa riêng:
  - Tệp tin đề nghị cấp chứng thư số mã hóa theo chuẩn PKCS #10 chứa khóa công khai và các thông tin định danh của thuê bao được ký bởi khóa riêng của thuê bao đó sinh từ HSM EN 419 221-5. HSM EN 419 221-5 ký số từ xa (CA2 Remote Signing) tuân thủ các tiêu chuẩn theo mô hình ký số từ xa quy định tại Thông tư TT16/2019/TT-BTTTT do thuê bao thực hiện;
  - Hoặc thuê bao ủy quyền cho CA2, CA2 sinh khóa theo ủy quyền của thuê bao sử dụng HSM EN 419 221-5. HSM EN 419 221-5 ký số từ xa (CA2 Remote Signing) tuân thủ các tiêu chuẩn theo mô hình ký số từ xa quy định tại Thông tư TT16/2019/TT-BTTTT. Theo quy trình, CA2 đảm bảo quyền sở hữu khóa riêng của thuê bao và bàn giao an toàn tránh các rủi ro trong quá trình giao nhận.

3.2.2 Thẩm định xác thực thông tin tổ chức

- Hồ sơ đề nghị cấp chứng thư số của tổ chức có thể được thực hiện qua phương thức điện tử.
- CA2 sẽ thực hiện tối thiểu các bước thẩm định bao gồm: Thẩm định hồ sơ đáp ứng theo yêu cầu của pháp luật; Xác thực chéo với cổng thông tin điện tử của cơ quan quản lý Nhà nước; Xác nhận qua điện thoại hoặc email
- Với đề nghị là tên miền website, ngoài những bước thẩm định trên CA2 sẽ thực hiện xác thực quyền sở hữu sử dụng tên miền của tổ chức đề nghị.
- Các thông tin cần có đối với tổ chức đề nghị cấp chứng thư số như sau:
  - Tên tổ chức
  - Mã số thuế/Mã số tổ chức hợp lệ
  - Địa chỉ theo Giấy phép đăng ký kinh doanh
  - Email hợp lệ

- Số điện thoại hợp lệ
- Bản sao hợp lệ quyết định thành lập, quyết định quy định chức năng, nhiệm vụ, quyền hạn hoặc văn bản xác nhận chức danh của người có thẩm quyền của cơ quan, nhà nước
- Thông tin về website, tên miền của tổ chức (sử dụng cho chứng thư SSL)
- Thông tin về người đại diện pháp luật của tổ chức

3.2.3 Thẩm định xác thực đối với cá nhân đại diện cho tổ chức

- Hồ sơ đề nghị cấp chứng thư số của cá nhân đại diện cho tổ chức có thể được thực hiện qua phương thức điện tử.
- CA2 sẽ thực hiện tối thiểu các bước thẩm định bao gồm: Thẩm định hồ sơ đáp ứng theo yêu cầu của pháp luật; Xác thực chéo với cổng thông tin điện tử của cơ quan quản lý Nhà Nước; Xác nhận qua điện thoại hoặc email.
- Các thông tin cần có đối với cá nhân đại diện cho tổ chức đề nghị cấp chứng thư số như sau:
    - Tên cá nhân
    - Thuộc tổ chức
    - Số CMND/Căn cước công dân/Hộ chiếu của người đại diện theo pháp luật của tổ chức
    - Địa chỉ theo CMND
    - Số điện thoại hợp lệ
    - Thư điện tử hợp lệ
    - Văn bản của tổ chức đề nghị cấp chữ ký số cho người có thẩm quyền và chức danh
    - Bản sao từ sổ gốc/Bản sao có chứng thực/Bản sao xuất trình bản chính để đối chiếu của một trong các loại giấy tờ: CMND/Hộ chiếu/Căn cước công dân
    - Thông tin sở hữu tên miền (sử dụng cho chứng thư SSL)

3.2.4 Thẩm định và xác thực đối với tên miền hợp lệ

- Hồ sơ đề nghị cấp chứng thư số của cá nhân có thể được thực hiện qua phương thức điện tử.

- CA2 sẽ thực hiện tối thiểu các bước thẩm định bao gồm: Thẩm định hồ sơ đáp ứng theo yêu cầu của pháp luật; Xác nhận qua điện thoại hoặc email.
- Các thông tin cần có đối với cá nhân đề nghị cấp chứng thư số như sau:
    - Tên cá nhân
    - Số CMND/Căn cước công dân/Hộ chiếu của người đại diện theo pháp luật của tổ chức
    - Địa chỉ theo CMND/Căn cước công dân
    - Địa chỉ thường trú
    - Số điện thoại hợp lệ
    - Thư điện tử hợp lệ
    - Bản sao từ sổ gốc/Bản sao có chứng thực/Bản sao xuất trình bản chính để đối chiếu của một trong các loại giấy tờ: CMND/Hộ chiếu/Căn cước công dân.
    - Thông tin sở hữu tên miền (sử dụng cho chứng thư SSL)

3.2.5 Xác thực với cơ quan quản lý nhà nước

CA2 sẽ thực hiện thẩm định chéo với cổng thông tin điện tử của Tổng Cục Thuế, Bộ Kế hoạch đầu tư, CMND/CCCD của cơ quan Công an

3.2.6. Tiêu chuẩn tích hợp

CA2 áp dụng theo danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số liên quan đến chuẩn kỹ thuật tích hợp.

3.3. Xác minh đề nghị thay đổi cặp khóa

Thuê bao phải có đơn xin thay đổi cặp khóa

CA2 sẽ thực hiện thẩm định trực tiếp với thuê bao, hồ sơ thuê bao và phía yêu cầu thay đổi để đảm bảo đúng đối tượng và gắn trách nhiệm trước khi CA2 thực hiện thu hồi chứng thư số của thuê bao xin thay đổi cặp khóa

3.3.1 Thực hiện thay đổi khóa

Quy trình thủ tục thay đổi cặp khóa được thực hiện tuân theo như các thủ tục cấp chứng thư số lần đầu Mục 3.2

3.3.2 Thực hiện thay đổi khóa khi thuê bao đã bị thu hồi

Thuê bao đã bị thu hồi không thuộc diện xem xét thay đổi cặp khóa

3.4. Xác minh đề nghị thu hồi chứng thư số

Trước khi thực hiện thu hồi một chứng thư số, CA2 tiến hành xác minh trực tiếp với thuê bao, hồ sơ thuê bao và phía yêu cầu thu hồi để đảm bảo đúng đối tượng và gắn trách nhiệm trước khi CA2 thực hiện chính thức thu hồi.

Việc thu hồi chỉ được thực hiện khi có xác nhận của thuê bao bằng văn bản

4. CÁC YÊU CẦU ĐỐI VỚI VÒNG ĐỜI HOẠT ĐỘNG CỦA CHỨNG THƯ SỐ THUÊ BAO

4. 1. Yêu cầu cấp chứng thư số

4.1.1 Đối tượng đề nghị cấp chứng thư số

Bất cứ cá nhân hay tổ chức nào đều có quyền đăng ký yêu cầu CA2 cung cấp dịch vụ

4.2.2 Hồ sơ đề nghị cấp chứng thư số

- Thuê bao phải hoàn thành Đơn yêu cầu cấp Chứng thư số CA2 và cung cấp đầy đủ, chính xác thông tin theo mẫu của CA2
- Cung cấp hồ sơ theo yêu cầu của CA2 và tham gia quá trình thẩm định thông tin thuê bao
- Ký hợp đồng sử dụng dịch vụ giữa hai bên, thực hiện các quyền lợi và nghĩa vụ theo như hợp đồng ký kết

4.2. Xử lý yêu cầu cấp chứng thư số

4.2.1 Thực hiện chức năng thẩm định

CA2 và RA, đại lý sẽ tổ chức thẩm định theo quy định tại Mục 3.2

4.2.2. Chấp thuận hoặc từ chối

CA2 hoặc RA, đại lý sẽ chấp thuận đăng ký đề nghị cấp chứng thư số thuê bao CA2, nếu việc thẩm định các thông tin như yêu cầu tại Mục 3.2 thành công, và thuê bao thanh toán theo quy định.

CA2 hoặc RA, đại lý sẽ từ chối nếu:

- Việc thẩm định không thể hoàn thành
- Thuê bao không hoàn thành hồ sơ theo như yêu cầu
- Thuê bao không thực hiện theo khung thời gian quy định
- Thuê bao không thanh toán theo quy định

4.2.3 Thời gian xử lý:

Trong vòng 5 ngày làm việc CA2 sẽ trả lời về việc chấp nhận đơn yêu cầu cấp chứng thư số CA2 và việc cấp phát chứng thư số CA2. CA2 sẽ cố gắng phản hồi nhanh nhất đến tất cả các đơn yêu cầu cấp chứng thư số CA2

4.3. Cấp chứng thư số

Bước 1: Thuê bao gửi hồ sơ đến thẩm định (CA Service online)

+ Nhập thông tin hồ sơ; Thẩm định hồ sơ…

+ CA Service online xử lý hồ sơ

Bước 2: RA Kiểm tra/ khởi tạo thông tin Thuê bao gửi đến SCA

+ SCA tạo Thông tin sử dụng cho khách hàng đến Thuê bao

+ Hệ thống sinh ID và gửi ID cho khách hàng

Bước 3: CA Service online gửi thông tin sử dụng cho khách hàng đến Thuê bao

Bước 4: Thuê bao cài đặt APP xác thực

+ Thuê bao cài đặt App trên mobile, kích hoạt thiết bị và nhập ID CA Service online cung cấp

Bước 5: Thuê bao gửi thông tin APP xác thực yêu cầu cấp CTS cho CA Service online

Bước 6: SAM gửi yêu cầu xác thực đến APP xác thực

Bước 7: APP xác thực gửi yêu cầu xác thực Thuê bao

Bước 8: Thuê bao nhập mã xác thực trên APP xác thực PIN/ Vân tay xác thực và thiết lập mã pin.

Bước 9: APP xác thực sinh khoá và gửi khoá xác thực đến SAM

Bước 10: SAM xác thực khoá và gửi yêu cầu sinh khóa ký đến HSM

Bước 11: HSM gửi yêu cầu tạo request đến CA offline

Bước 12: CA offline gửi Certificate Signing Requests - CSR đến App xác thực và sau khi CA Service online sinh CTS thì CA offline gửi tới SCA để cập nhật chứng thư số

Bước 13: RA gửi CTS đến cho APP xác thực sinh thông báo tới Thuê bao

Bước 14: APP xác thực gửi yêu cầu xác nhận thông tin CTS đến Thuê bao

Bước 15: Thuê bao xác nhận bằng APP xác nhận gửi tới CA offine để CA offline công bố chứng thư số

4.4. Xác nhận và công bố công khai chứng thư số

4.4.1 Tổ chức bàn giao và xác nhận

- CA2 thực hiện bàn giao chứng thư số và yêu cầu thuê bao kiểm tra, xác nhận tính chính xác của thông tin thuê bao trên chứng thư số do CA2 cấp theo đề nghị của thuê bao.
- Xác nhận tính chính xác của thông tin bằng email cấp trong chứng thư số và ký nhận biên bản bàn giao.
- Xác nhận tính chính xác của chứng thư số và bàn giao qua ứng dụng CA2 Mobile App
- Thuê bao phải xác nhận trước khi CA2 công bố chứng thư số của thuê bao trên cơ sở dữ liệu trực tuyến về chứng thư số của CA2

4.4.2 Công bố chứng thư số

Trong vòng 8 giờ làm việc sau khi có xác nhận của thuê bao, CA2 tiến hành công bố chứng thư số của thuê bao trên hệ thống cơ sở dữ liệu danh bạ chứng thư số trực tuyến của CA2

4.4.3. Thông báo việc cấp Chứng thư số thuê bao đến các tổ chức, cá nhân khác

Thông báo việc cấp phát Chứng thư số thuê bao đến các tổ chức, cá nhân khác được thực hiện bằng cách công bố chứng thư số thuê bao trên hệ thống danh bạ trực tuyến về chứng thư số của CA2 và trên giấy chứng nhận do CA2 cấp cho thuê bao

4.5. Sử dụng cặp khóa và chứng thư số

4.5.1. Việc sử dụng chứng thư số và khóa riêng của thuê bao

Việc sử dụng khóa riêng tương ứng với khóa công khai trên chứng thư số của thuê bao do CA2 cấp phải tuân thủ theo đúng phạm vi trong thỏa thuận ký kết giữa hai bên

Thuê bao phải chịu trách nhiệm bảo vệ khóa riêng, và về việc sử dụng trái phép khóa riêng, và phải ngừng sử dụng khóa riêng sau khi hết hạn hoặc bị thu hồi chứng thư số

4.5.2. Việc sử dụng chứng thư số và khóa công khai của thuê bao CA2 đối với bên nhận

Khi đồng ý sử dụng chứng thư số của thuê bao CA2 tức là bên nhận đã đồng ý với các điều khoản áp dụng cho bên nhận

Bên nhận phải xác thực về thông tin của chứng thư số, sự phù hợp cho mục đích sử dụng, trạng thái của chứng thư số, và chữ ký số.

4.6. Gia hạn chứng thư số

Quy trình như cấp mới không thực hiện gia hạn khóa

4.7. Thay đổi cặp khóa của thuê bao

Thuê bao phải có đơn xin thay đổi khóa chứng thư số.

CA2 sẽ phải thẩm định và cấp một chứng thư số mới chứng thực cho khóa công khai thay đổi

4.7.1. Các trường hợp thay đổi khóa chứng thư số

Trước khi hết hạn chứng thư số hoặc sau khi hết hạn chứng thư số thuê bao có thể yêu cầu thay đổi khóa chứng thư số.

4.7.2. Người yêu cầu thay đổi khóa chứng thư số

Thuê bao phải trực tiếp yêu cầu việc thay đổi khóa chứng thư số

4.7.3. Quy trình xử lý yêu cầu thay đổi khóa chứng thư số

Khi cần thay đổi khóa chứng thư số, thuê bao phải có đơn xin thay đổi khóa chứng thư số.

CA2 và RA, đại lý thực hiện các trình tự thủ tục thẩm định đảm bảo xác minh chính xác người yêu cầu thay đổi khóa chứng thư số là thuê bao của chứng thư số được yêu cầu thay đổi khóa.

4.7.4. Thông báo cho thuê bao

Thực hiện thông báo cho thuê bao và xác nhận với thuê bao về việc cấp chứng thư số cho khóa thay đổi của thuê bao.

4.7.5. Bàn giao và xác nhận với thuê bao

CA2 thực hiện bàn giao chứng thư số và yêu cầu thuê bao kiểm tra, xác nhận tính chính xác của thông tin thuê bao trên chứng thư số với khóa thay đổi do CA2 cấp theo đề nghị của thuê bao.

Thuê bao phải xác nhận trước khi CA2 công bố chứng thư số của thuê bao trên cơ sở dữ liệu danh bạ trực tuyến về chứng thư số của CA2.

4.7.6. Công bố chứng thư số

Trong vòng 8 giờ làm việc sau khi có xác nhận của thuê bao, CA2 tiến hành công bố chứng thư số của thuê bao trên hệ thống cơ sở dữ liệu danh bạ chứng thư số trực tuyến của CA2.

4.7.7. Thông báo việc thay đổi khóa chứng thư số của thuê bao đến các tổ chức, cá nhân khác

Thông báo việc thay đổi khóa chứng thư số của thuê bao đến các tổ chức, cá nhân khác được thực hiện bằng cách công bố chứng thư số thuê bao trên hệ thống danh

bạ trực tuyến về chứng thư số của CA2, và trên giấy chứng nhận do CA2 cấp thay đổi cho thuê bao

4.8. Thay đổi thông tin chứng thư số

4.8.1. Các trường hợp thay đổi chứng thư số

Khi thuê bao có nhu cầu thay đổi thông tin trên chứng thư số đang sử dụng của thuê bao mà không thay đổi khóa chứng thư số.

4.8.2. Người yêu cầu thay đổi chứng thư số

Thuê bao phải trực tiếp yêu cầu việc thay đổi chứng thư số.

4.8.3. Quy trình xử lý yêu cầu thay đổi chứng thư số

Thuê bao phải có đơn xin thay đổi chứng thư số.

CA2 sẽ phải thẩm định và cấp đổi một chứng thư số mới chứng thực cho khóa công khai của thuê bao.

CA2 và RA, đại lý thực hiện các trình tự thủ tục thẩm định đảm bảo xác minh chính xác người yêu cầu thay đổi chứng thư số là thuê bao của chứng thư số được yêu cầu thay đổi.

4.8.4. Thông báo cho thuê bao

Thực hiện thông báo cho thuê bao và xác nhận với thuê bao về việc cấp chứng thư số cho yêu cầu thay đổi chứng thư số của thuê bao.

4.8.5. Bàn giao và xác nhận với thuê bao

CA2 thực hiện bàn giao chứng thư số và yêu cầu thuê bao kiểm tra, xác nhận tính chính xác của thông tin thuê bao trên chứng thư số thay đổi với do CA2 cấp theo đề nghị của thuê bao.

Thuê bao phải xác nhận trước khi CA2 công bố chứng thư số thay đổi của thuê bao trên cơ sở dữ liệu danh bạ trực tuyến về chứng thư số của CA2.

4.8.6. Công bố chứng thư số

Trong vòng 8 giờ làm việc sau khi có xác nhận của thuê bao, CA2 tiến hành công bố chứng thư số của thuê bao trên hệ thống cơ sở dữ liệu chứng thư số trực tuyến của CA2.

4.8.7. Thông báo việc thay đổi chứng thư số của thuê bao đến các tổ chức, cá nhân khác

Thông báo việc thay đổi chứng thư số của thuê bao đến các tổ chức, cá nhân khác được thực hiện bằng cách công bố chứng thư số thuê bao trên hệ thống danh bạ trực

tuyến về chứng thư số của CA2, và trên giấy chứng nhận do CA2 cấp thay đổi cho thuê bao.

4.9. Tạm dừng và thu hồi chứng thư số

Bước 1: Thuê bao gửi yêu cầu tạm ngưng chứng thư số tới CA Service online để tạm ngưng trạng thái CTS

Bước 2: CA Service online gửi yêu cầu tạm ngưng trạng thái ký CTS tới SCA

+ SCA chặn việc ký số bằng CTS sau đó gửi yêu cầu chặn ký bằng CTS tới APP xác thực.

Bước 3: APP xác thực chuyển trạng thái CSTS và gửi yêu cầu chặn/khóa khóa ký tới HSM

Bước 4: HSM chặn/Khóa khóa ký sau đó gửi công bố tới CA Service online

4.10. Kiểm tra trạng thái chứng thư số

4.10.1. Các đặc điểm của dịch vụ

Việc kiểm tra trạng thái của một chứng thư số có các cách sau:

- Kiểm tra qua danh sách thu hồi chứng thư số CRL công bố trên website của CA2
- Kiểm tra bằng việc tìm kiếm theo các thông tin trên chứng thư số qua hệ thống danh bạ chứng thư số LDAP của CA2
- Kiểm tra quan giao thức trạng thái chứng thư số trực tuyến OCSP được tích hợp vào ứng dụng của bên nhận

4.10.2. Tính sẵn sàng của dịch vụ

Dịch vụ luôn sẵn sàng 24/7

4.10.3. Tính tùy chọn

OCSP có tính tùy chọn vì không phải ứng dụng nào cũng có sẵn tính năng OCSP để hỗ trợ việc tự động xác thực trạng thái chứng thư số trực tuyến

4.11. Chấm dứt dịch vụ của thuê bao

Thuê bao có thể đơn phương chấm dứt dịch vụ bằng các cách:

- Hủy hợp đồng thuê bao
- Chứng thư số hết hạn nhưng không gia hạn
- Yêu cầu thu hồi trước thời hạn

4.12. Lưu trữ và phục hồi khóa bí mật của thuê bao

Quy trình lưu trữ khóa mật mã (hoặc cặp khóa) được thực hiện theo cách thức mã hóa và tuân thủ quy trình nội bộ đã phê duyệt. Việc quản lý các khóa mật mã đang lưu trữ bên trong mô-đun phần cứng chuyên dụng (HSM chuyên dụng), cần phải có xác thực kép của hai nhân sự xác thực bằng thẻ thông minh chuyên dụng để truy cập.

Một bản sao lưu của các khóa mật mã sẽ được tạo ngay sau khi tạo tất cả các khóa, hoặc sau đó khi có khóa mật mã phải tạo lại. Việc sao lưu các khóa mật mã được sao lưu trong HSM chuyên dụng có mức độ bảo mật tương đương HSM chuyên dụng sinh khóa. Để tạo bản sao dự phòng của các khóa, cần phải có hai nhân sự được phân công theo quy định, hai người này được phân quyền truy cập HSM chuyên dụng theo vai tương ứng. Sao lưu được thực hiện trong môi trường được bảo vệ. Sau khi bản sao lưu được tạo thì sẽ được cất ở một vị trí cách biệt và an toàn.

Cùng với việc tạo cặp khóa từ xa của người ký qua ứng dụng CA2 Mobile Sign cho thiết bị di động của người ký, khóa mật mã cũng được lưu trữ trong HSM chuyên dụng theo cách được mã hóa và người ký có thể truy cập khóa riêng bằng cách tuân thủ các yêu cầu ở mức SCAL2.

- Căn cứ Mục SRG_KM.2.1 của bộ TC CEN 419 241-1 về yêu cầu mô tả rõ ràng chính xác quy trình thủ tục quản lý sao lưu khóa an toàn được áp dụng

CA2 Mobile Sign áp dụng:

+ CA2 Remote Signing áp dụng cơ chế sao lưu an toàn bảo mật trong môi trường HSM chuyên dụng đối với toàn bộ khóa mật (Bao gồm khóa ký số của người ký, khóa mật mã đảm bảo an toàn cơ sở hạ tầng, khóa điều khiển).

- Căn cứ Mục SRG_KM.2.2 của bộ TC CEN 419 241-1 về yêu cầu mô tả rõ ràng chính xác quy trình thủ tục quản lý bảo vệ sao lưu an toàn được áp dụng

CA2 Remote Signing áp dụng:

+ CA2 Remote Signing áp dụng trong trường hợp khóa mật mã (bao gồm khóa ký của người ký, khóa cơ sở hạ tầng và khóa điều khiển) được kết xuất từ HSM chuyên dụng, thì khóa kết xuất sẽ được bảo vệ bằng cơ chế mã hóa của HSM chuyên dụng tương đương đảm bảo tính bảo mật và tính toàn vẹn tương tự như được quản lý bên trong HSM đạt mức an toàn bảo mật EAL4 được tăng cường bởi AVA_VAN.5. và ALC_FLR.3.

- Căn cứ Mục SRG_KM.2.3 của bộ TC CEN 419 241-1 về yêu cầu mô tả rõ ràng chính xác quy trình thủ tục quản lý an toàn kiểm soát sao lưu được áp dụng

CA2 Remote Signing áp dụng:

+ CA2 Remote Signing áp dụng cơ chế M x N với tối thiểu là 02 nhân sự có đủ thẩm quyền trong vận hành an toàn nghiệp vụ sao lưu, lưu trữ và phục hồi đối với khóa mật mã (Gồm khóa ký của người ký, khóa cơ sở hạ tầng, khóa điều khiển). Các khóa chính được sử dụng để bảo vệ cả người dùng và khóa nghiệp vụ được sao lưu, lưu trữ và nạp lại dưới sự kiểm soát áp dụng cơ chế M x N với tối thiểu 02 nhân sự. Được bảo vệ bởi bộ thẻ thông minh chuyên dụng.

- CA2 Remote Signing áp dụng quy trình nghiệp vụ kiểm soát việc sao lưu và phục hồi phải đảm bảo duy trì tính liên tục của dịch vụ.

5. KIỂM SOÁT, QUẢN LÝ VÀ VẬN HÀNH

5.1. Kiểm soát an toàn, an ninh vật lý

Căn cứ Điều OVR-6.4.2-01 bộ tiêu chí TC ETSI 119 431-1, tham chiếu Khoản 7.6 bộ tiêu chí ETSI EN 319 401.

CA2 Remote Signing thực hiện kiểm soát quyền truy cập vật lý vào các thành phần của hệ thống dịch vụ CA Remote Signing quan trọng đến tính an toàn bảo mật đối với việc cung cấp các dịch vụ đảm bảo giảm thiểu tối đa rủi ro liên quan đến bảo mật vật lý. Tuân thủ các yêu cầu theo khuyến nghị tại Khoản 11 bộ tiêu chuẩn ISO/IEC 27002:2013.

CA2 Remote Signing áp dụng, quyền truy cập vật lý vào các thành phần của hệ thống cung cấp dịch vụ có tính an toàn bảo mật quan trọng đối với việc cung cấp các dịch vụ sẽ bị giới hạn chỉ cho phép đối với các cá nhân được phân quyền.

CA2 Remote Signing triển khai các biện pháp kiểm soát đảm bảo tránh mất mát, hư hỏng hoặc xâm nhập tài sản và gián đoạn hoạt động dịch vụ.

CA2 Remote Signing triển khai các biện pháp kiểm soát đảm bảo tránh sự xâm phạm hoặc đánh cắp thông tin và các phương tiện xử lý thông tin.

Các thành phần quan trọng đối với hoạt động đảm bảo an toàn bảo mật của dịch vụ được đặt cách ly trong một khu vực riêng biệt được bảo vệ vật lý chống lại sự xâm nhập, mất kiểm soát truy cập an toàn bảo mật và áp dụng công nghệ để phát hiện xâm nhập. Tuân thủ các yêu cầu theo khuyến nghị tại Khoản 11 bộ tiêu chuẩn ISO/IEC 27002:2013.

CA2 Remote Signing áp dụng bổ sung Điều 6.4.2 đối với kiểm soát an ninh vật lý của bộ tiêu chí ETSI EN 319 411-1:

Cơ sở hạ tầng liên quan đến quản lý cấp phát và thu hồi chứng thư số chứng thực khóa công khai được vận hành trong môi trường bảo vệ vật lý chống lại những xâm phạm thông qua việc truy cập trái phép vào hệ thống hoặc dữ liệu.

Mọi hoạt động ra vào khu vực an ninh bảo mật vật lý sẽ phải chịu sự giám sát độc lập, đối với người không được ủy quyền sẽ được người có thẩm quyền đi kèm trong khi ở trong khu vực an ninh.

Mọi hoạt động vào ra khu vực bảo vệ được ghi nhật ký và bảo vệ.

Khu vực quản lý cấp phát và thu hồi chứng thư số được bảo vệ vật lý cách ly.

CA2 Remote Signing không chia sẻ dùng chung khu vực quản lý cấp phát và thu hồi chứng thư số chứng thực khóa công khai với các tổ chức khác.

Các biện pháp kiểm soát an ninh an toàn vật lý và môi trường được triển khai thực hiện để bảo vệ tài nguyên hệ thống, hạ tầng cơ sở, và các vật tư tài sản được sử dụng để hỗ trợ hoạt động của dịch vụ.

CA2 Remote Signing có hệ thống chính sách an ninh an toàn vật lý và môi trường cung cấp dịch vụ đối với các hệ thống liên quan đến dịch vụ quản lý tạo và thu hồi chứng thư số chứng thực khóa công khai đảm bảo việc kiểm soát truy cập vật lý, bảo vệ thiên tai, các yếu tố an toàn cháy nổ, sự cố của các dịch vụ hỗ trợ (ví dụ: điện, viễn thông), sập đổ cấu trúc xây dựng, rò rỉ đường ống nước, bảo vệ chống trộm, đột nhập và khắc phục hậu quả thiên tai.

CA2 Remote Signing áp dụng các biện pháp kiểm soát để bảo vệ chống lại thiết bị, thông tin, phương tiện và phần mềm liên quan đến các dịch vụ rủi ro triển khai bên ngoài địa điểm mà không được phép.

CA2 xem xét kỹ lưỡng các chức năng khác liên quan đến hoạt động của dịch vụ có thể được hỗ trợ trong cùng một khu vực được bảo mật với điều kiện là quyền truy cập được giới hạn cho người có thẩm quyền.

CA2 áp dụng phương pháp triển khai RootCA cách ly offline.

Căn cứ mục 6.4.2 của bộ TC ETSI 119.431-1 (*Điều OVR-6.4.2-01 và 02 Mục Facility, management, and operational controls của bộ TC ETSI 119.431-1*)

5.1.1. Nơi đặt hệ thống và kết cấu

Hệ thống CA2 Remote Signing được đặt trong phòng riêng, cửa ra vào được khóa bởi 2 lớp khóa là khóa cơ và khóa điện tử, chỉ có những nhân sự được giao nhiệm vụ được phép ra vào.

5.1.2. Kiểm soát ra vào

Vào phòng hệ thống Remote Signing bắt buộc phải có tối thiểu 2 người cùng một lúc, một người giữ chìa khóa cơ, một người giữ thẻ mở khóa điện tử.

Tất cả các hoạt động ra vào được camera và cán bộ giám sát ghi lại.

Tất cả các hoạt động vào ra đều được ghi log lại

Các biện pháp kiểm soát sẽ được CA2 áp dụng để tránh xâm phạm hoặc đánh cắp thông tin

Các khóa bí mật của Root CA được giữ và cách ly vật lý với các hoạt động bình thường, chỉ có nhân sự được ủy quyền mới có quyền được truy cập

5.1.3. Kiểm soát truy cập

CA2 Remote Signing ban hành Chính sách kiểm soát truy cập tuân thủ với các yêu cầu sau:

- Quyền truy cập vào hệ thống chỉ cho phép hạn chế đối với những người có thẩm quyền. CA2 Remote Signing đảm bảo kiểm soát truy cập tới thông tin nhạy cảm. Quyền truy cập vào các trang cụ thể được xác định bởi các đặc quyền và vai trò của nhân viên;
- Các biện pháp kiểm soát (tường lửa) được triển khai để bảo vệ các phân vùng mạng nội bộ khỏi bị truy cập trái phép, bao gồm cả quyền truy cập của thuê bao và bên thứ ba;
- Tường lửa được cấu hình để ngăn chặn tất cả các giao thức và quyền truy cập không cần thiết cho hoạt động của CA2 Remote Signing;
- CA2 Remote Signing quản lý quyền truy cập của thuê bao, thành viên hệ thống, quản trị viên và người kiểm tra hệ thống;
- Quản trị viên hệ thống quản lý tài khoản thành viên hệ thống và đảm bảo sửa đổi hoặc xóa quyền truy cập kịp thời;
- Quyền truy cập vào thông tin và các ứng dụng bị hạn chế theo Chính sách kiểm soát truy cập;

- Giải pháp công nghệ CA2 Remote Signing ứng dụng đảm bảo việc kiểm soát đầy đủ an ninh an toàn hệ thống máy tính đối với việc quản trị và hoạt động của nhân sự hệ thống phù hợp với vai trò được phân công, phân quyền;
- CA2 Remote Signing kiểm soát việc sử dụng phần mềm bằng việc nhân sự hệ thống bắt buộc phải chứng minh tính hợp lệ của danh tính trước khi sử dụng các ứng dụng quan trọng liên quan đến dịch vụ;
- CA2 Remote Signing có quy định rõ ràng về trách nhiệm của nhân sự hệ thống, nhân sự hệ thống của CA2 Remote Signing chịu trách nhiệm về các hành động của họ đã được hộp đen ghi nhận;
- CA2 Remote Signing đảm bảo kiểm soát việc truy cập thông tin nhạy cảm. Dữ liệu nhạy cảm được bảo vệ khỏi bị tiết lộ bởi người sử dụng trái phép;
- Xác thực lại là bắt buộc khi đã đăng xuất khỏi hệ thống. Hệ thống áp dụng các cơ chế phân quyền cho người dùng đặc quyền, giúp giảm rủi ro trong quản lý phiên người dùng, trong trường hợp thiết bị làm việc của người dùng không được giám sát, phiên người dùng sẽ bị chấm dứt sau một khoảng thời gian không hoạt động nhất định. Khi số lần thử xác thực không thành công đối với một người dùng đạt đến số lần thử tối đa có thể, hệ thống sẽ ngăn chặn bất kỳ nỗ lực xác thực nào khác của người dùng cho đến khi quản trị viên thực hiện các nghiệp vụ để gỡ chặn người dùng (hoặc trong một khoảng thời gian nhất định).

5.1.4. Điều hòa nhiệt độ và nguồn điện

Hệ thống và thiết bị CA2 Remote Signing được trang bị với hệ thống chính và hệ thống dự phòng:

- Nguồn điện gồm có: Nguồn điện lưới, hệ thống điện dự phòng UPS và máy phát điện dự phòng. Toàn bộ được giám sát.
- Hệ thống điều hòa nhiệt độ và chống ẩm. Hệ thống điều hòa không khí được trang bị nhân đôi dự phòng, duy trì nhiệt độ không khí ổn định để đảm bảo hệ thống công nghệ hoạt động bình thường.
- Nguồn điện bên ngoài từ máy phát điện diesel được duy trì, được dự phòng. Trong trường hợp sự cố của đường dây điện chính, hệ thống sẽ chuyển sang nguồn điện khẩn cấp. Môi trường làm việc trong khu vực của hệ thống máy chủ dịch vụ liên tục được giám sát độc lập với các khu vực làm việc khác.

- Hệ thống thông gió được thiết kế đảm bảo cho không cho phép làm ảnh hưởng đến việc bảo vệ vật lý và điện từ của hoạt động bình thường đối với các bộ phận máy tính vận hành cung cấp dịch vụ.
- Hệ thống điện văn phòng của CA2 Remote Signing được kết nối với hệ thống điện khẩn cấp của tòa nhà.

5.1.5. Hư hại do nước

Toàn bộ hệ thống máy chủ và thiết bị CA2 Remote Signing được cài đặt trong phòng đảm bảo không bị trong tình trạng có nước. Toàn bộ thiết bị hệ thống được lắp đặt trong hệ thống tủ Rack công nghiệp.

Phòng máy được trang bị các cảm biến để phát hiện mức độ ẩm của phòng và của hệ thống máy tính, để theo dõi độ ẩm. Các nhân viên bảo vệ và nhân viên của CA2 Remote Signing đã được hướng dẫn và có nghĩa vụ thông báo ngay cho các bộ phận liên quan, quản trị viên bảo mật và quản trị viên hệ thống trong trường hợp có mối đe dọa.

5.1.6. Phòng cháy chữa cháy

CA2 Remote Signing thực hiện công tác phòng cháy và chữa cháy theo quy định của Cục Cảnh sát phòng cháy chữa cháy Hà Nội.

CA2 Remote Signing có kế hoạch xử lý rủi ro có tính tới những thiệt hại do cháy nổ.

CA2 Remote Signing cử cán bộ tham gia đào tạo định kỳ về phòng chống cháy nổ để đảm bảo xử lý kịp thời trong trường hợp có sự cố xảy ra.

Phòng máy chủ đặt hệ thống CA2 Remote Signing được trang bị hệ thống chữa cháy bằng bột chuyên dụng.

Khu vực riêng đặt hệ thống dịch vụ được lắp đặt các thiết bị sau: hệ thống cảnh báo cháy bằng âm thanh và ánh sáng. Trong trường hợp xảy ra hỏa hoạn, việc cung cấp điện sẽ bị cắt và việc dập lửa bằng bọt được thực hiện tự động.

5.1.7. Chống nhiễu điện từ

Nơi đặt hệ thống, thiết bị không gần nguồn phát nhiễu điện từ mạnh. Vỏ sắt máy thiết bị, tủ Rack được nối đất chống nhiễu điện từ. Các thành phần thiết bị có khả năng ảnh hưởng nhiễu điện từ được bảo vệ bằng bọc màng chống nhiễu điện từ.

5.1.8. Chống chịu lũ lụt, động đất

Hệ thống chính được đặt tại Tầng 3 Tòa nhà Bohemia số 25 Nguyễn Huy Tưởng, phường Thanh Xuân Trung, Quận Thanh Xuân, thành phố Hà Nội.

Hệ thống dự phòng được đặt tại Data Center của Công ty TNHH Hanel – CSF đặt tại khu công nghiệp Sài Đồng B, Quận Long Biên, Hà Nội

Toàn bộ máy móc thiết bị được lắp đặt trong hệ thống tủ Rack công nghiệp không tiếp xúc trực tiếp với mặt sàn tầng nhà.

Cơ sở dữ liệu luôn được lưu dự phòng trên hệ thống băng từ tại chỗ và offsite tại Hanel Data Center.

Cơ sở dữ liệu dự phòng và khoá mật mã phục hồi hệ thống được quản lý bởi bộ thẻ thông minh chuyên dụng, thẻ thông minh với khả năng chịu nước, va đập. Duy trì offsite cùng quy trình phục hồi toàn diện đảm bảo việc khôi phục hoàn toàn hệ thống trong trường hợp thảm hoạ xảy ra.

5.2. Quy trình kiểm soát

Đảm bảo tính tin tưởng

CA2 là dịch vụ tin cậy, thiết kế kỹ thuật và vận hành hệ thống tuân thủ tuyệt đối yêu cầu này.

Vai trò, trách nhiệm của cán bộ vận hành được phân định rõ ràng, và được kiểm soát chặt chẽ theo chức năng, nhiệm vụ và phải là những người được tin tưởng cao. Nguyên tắc là tất cả những vị trí công việc nhậy cảm với cơ hội thỏa hiệp về khóa mật mã hệ thống, về cấp và quản lý chu kỳ hoạt động của chứng thư số phải được đảm bảo tin tưởng.

Số cán bộ yêu cầu cho mỗi nhiệm vụ

CA2 không cho phép một cán bộ thực hiện độc lập các hoạt động của hệ thống cấp và quản lý chứng thư số (CA). Từ kiểm soát vào phòng CA đến kiểm soát vận hành CA mỗi chức năng phải có tối thiểu 2 người được tin tưởng cùng tham gia.

Những chức năng nhiệm vụ sau tối thiểu phải có 2 cán bộ an ninh được tin tưởng tham gia:

- *Ra vào phòng hệ thống.*
- *Thêm và xóa cán bộ an ninh hệ thống.*
- *Kích hoạt HSM cho các hoạt động ký số của hệ thống.*
- *Khởi tạo, cập nhật, lưu trữ và dự phòng cơ sở dữ liệu.*

Xác thực và định danh với từng vai trò được tin tưởng

Mỗi cán bộ tham gia với vai trò được tin tưởng trong hệ thống CA2 được cấp sở hữu riêng một thẻ thông minh dùng cho xác thực định danh và phân quyền vận hành. Thẻ này được bảo vệ bằng mã PIN cá nhân và được cất giữ trong mỗi két an

ninh riêng.

Yêu cầu tách nhiệm vụ

Các nhiệm vụ sau phải tách ra thực hiện:

- *Thẩm định yêu cầu cấp chứng thư số.*
- *Thẩm định yêu cầu thu hồi, gia hạn chứng thư số.*
- *Cấp, thu hồi chứng thư số.*
- *Quản lý thông tin thuê bao.*
- *Đối soát.*
- *Vận hành hệ thống.*
- *An ninh hệ thống*
- *Quản trị hệ thống*

5.3. Kiểm soát nhân sự

CA2 Remote Signing tuân thủ các yêu cầu sau:

CA2 Remote Signing có các quy trình thủ tục đảm bảo nhân viên và nhà thầu tuân thủ các yêu cầu về độ tin cậy của hoạt động cung cấp dịch vụ;

CA2 Remote Signing tuyển dụng nhân viên và lựa chọn nhà thầu phụ (nếu có), có chuyên môn, độ tin cậy, kinh nghiệm và trình độ chuyên môn cần thiết và đã trải qua khóa đào tạo về các quy tắc bảo mật và bảo vệ dữ liệu cá nhân liên quan đến các công việc được pháp thực hiện;

Nhân sự của CA2 Remote Signing được đào tạo định kỳ (ít nhất 12 tháng một lần) để nâng cao chuyên môn, kinh nghiệm và trình độ của họ. Các khóa đào tạo bao gồm các khóa học về an toàn bảo mật thông tin, các mối đe dọa tiềm ẩn và trải nghiệm thực hành thực tế về an toàn bảo mật;

Các chế tài kỷ luật thích đáng được áp dụng đối với những nhân viên vi phạm các chính sách của CA2 Remote Signing;

Vai trò và trách nhiệm liên quan đến an toàn bảo mật thông tin được nêu rõ trong bản mô tả công việc;

CA2 Remote Signing quy định rõ các vai trò có yêu cầu tin cậy cao trong hệ thống căn cứ trên cơ sở yêu cầu đối với tính an toàn bảo mật của dịch vụ xác thực chữ ký / con dấu số;

Ban lãnh đạo và quản lý của CA2 Remote Signing quy định rõ trách nhiệm của các vai trò yêu cầu tin cậy cao trong hệ thống;

Các vai trò yêu cầu tin cậy cao trong hệ thống được phê duyệt và thông qua bởi ban lãnh đạo và quản lý;

Nhân sự của CA2 Remote Signing (cả tạm thời và lâu dài) đều có bản mô tả công việc liên quan đến vai trò thực hiện, với sự phân chia nhiệm vụ phù hợp với quy tắc "số đặc quyền yêu cầu ít nhất". Mức độ nhạy cảm của vị trí được xác định dựa trên trách nhiệm, cấp độ tiếp cận, trình độ chuyên môn và bằng cấp;

Bản mô tả công việc bao gồm các yêu cầu về kỹ năng và kinh nghiệm. Được phân biệt rõ giữa các nhiệm vụ chung và các nhiệm vụ cụ thể;

Nhân sự được áp dụng các thủ tục và quy trình hành chính và vận hành hoạt động của dịch vụ là một phần của quy trình quản lý an toàn thông tin của CA2 Remote Signing;

Đội ngũ quản lý có kiến thức cần thiết về dịch vụ được cung cấp, kiến thức về các thủ tục an toàn bảo mật và kinh nghiệm trong lĩnh vực an toàn bảo mật thông tin và đánh giá rủi ro đủ để thực hiện các chức năng quản lý;

Toàn bộ nhân sự của CA2 Remote Signing với vai trò yêu cầu tin cậy cao trong hệ thống không có bất kỳ xung đột lợi ích nào có thể ảnh hưởng đến tính khách quan của các hoạt động cung cấp dịch vụ;

Các vai trò yêu cầu tin cậy cao trong hệ thống được mô tả trong phần 5.4 của tài liệu này;

Nhân sự của CA2 Remote Signing được quản lý cấp cao giao các vai trò yêu cầu tin cậy cao trong hệ thống dựa trên nguyên tắc “đặc quyền thấp nhất” đối với quyền truy cập hoặc trong quá trình cấu hình các đặc quyền truy cập;

Nhân sự không được cấp quyền truy cập vào các chức năng yêu cầu tin cậy cao trong hệ thống trước khi các xác minh cần thiết được hoàn thành.

Căn cứ mục 6.4.4 của bộ TC ETSI 119.431-1 (*Điều OVR-6.4.4-01 Mục Facility, management, and operational controls của bộ TC ETSI 119.431-1*)

CA2 yêu cầu toàn bộ các nhân viên thực hiện nhiệm vụ đối với hoạt động của CA2 sẽ được bổ sung và chi tiết thêm:

- Được bổ nhiệm bằng văn bản bởi lãnh đạo của CA2 Remote Signing
- Phải tuân theo các điều khoản và điều kiện trong hợp đồng hoặc quy chế tương ứng với vị trí họ đảm nhiệm
- Các nhân sự phải thực hiện các thủ tục và quy trình hành chính và quản lý phù hợp với các quy trình,chính sách quản lý an toàn thông tin của CA2 Remote Signing.
- Đã được đào tạo một cách toàn diện về nhiệm vụ phải thực hiện;

- Tuân theo hợp đồng hoặc quy chế về việc không được tiết lộ các thông tin an ninh nhạy cảm
- Không được phân công các nhiệm vụ mà có thể gây ra xung đột trách nhiệm.
- Các nhân sự (cả cố định và tạm thời) phải có bản mô tả công việc quy định chi tiết nhiệm vụ, quyền hạn và mức độ truy cập
- Nhân viên quản lý phải có kinh nghiệm hoặc được đào tạo liên quan đến chức năng nhiệm vụ được giao, quen thuộc với các quy trình bảo mật dành cho nhân viên,có trách nhiệm bảo mật và kinh nghiệm về bảo mật thông tin và đánh giá rủi ro đủ để thực hiện các chức năng quản lý.
- Các nhân sự về hệ thống, phụ thuộc vào tính an toàn bảo mật cho hoạt động của CA2 Remote Signing được chỉ định rõ ràng
- Các nhân sự của CA2 Remote Signing sẽ không được quyền truy cập vào các chức năng quan trọng của hệ thống cho đến khi hoàn thành kiểm tra về năng lực trình độ chuyên môn.
- Tất cả nhân sự của CA2 sẽ không có xung đột lợi ích có thể ảnh hưởng đến tính công bằng trong hoạt động của CA2.

5.3.1. Yêu cầu và thủ tục về trình độ chuyên môn, kinh nghiệm

Các nhân sự của CA2 Remote Signing có khả năng đáp ứng được trình độ chuyên môn, có độ tin cậy và các bằng cấp chuyên môn cần thiết, phù hợp với vai trò và nhiệm vụ đảm trách.

CA2 Remote Signing thực hiện kiểm tra lý lịch đối với tất cả các ứng viên xin việc theo khuôn khổ pháp lý, các quy định, sự phù hợp và đặc biệt là đạo đức với các yêu cầu liên quan đến hoạt động, phân loại thông tin mà mỗi nhân sự có quyền truy cập cũng như các rủi ro giả định. Nội dung kiểm tra lý lịch bao gồm: Hồ sơ, tài liệu tham khảo, sơ yếu lý lịch, bằng cấp, mối quan hệ, lịch sử cá nhân và các tài liệu khác tùy thuộc vào công việc mà nhân sự ứng tuyển.

5.3.2. Thủ tục kiểm tra năng lực

Tất cả cán bộ công tác trong vai trò được tin tưởng được yêu cầu phải qua kiểm tra nghiêm ngặt về sự tin tưởng, trình độ chuyên môn và kinh nghiệm phù hợp.

CA2 Remote Signing tuyển nhân viên và các nhà thầu phụ (nếu có), có trình độ chuyên môn, độ tin cậy và kinh nghiệm cần thiết và đã trải qua khóa đào tạo về an toàn bảo mật và bảo vệ dữ liệu, thông tin cá nhân, cũng như các khóa đào tạo khác phù hợp với các

dịch vụ và hoạt động ủy thác dịch vụ ký số từ xa của Công ty. Nhân sự của CA2 Remote Signing đáp ứng yêu cầu "chuyên môn, kinh nghiệm và trình độ" thông qua kinh nghiệm thực tế có được, đào tạo sau khi được tuyển dụng vào một vị trí nhất định hoặc kết hợp cả hai. Nhân sự của CA2 Remote Signing trải qua các khóa đào tạo thường xuyên (ít nhất 12 tháng một lần) về an toàn bảo mật thông tin. Các khóa đào tạo bao gồm các khía cạnh an toàn bảo mật liên quan đến các mối đe dọa mới và các phương pháp bảo mật.

5.3.4. Các vai trò yêu cầu tin cậy cao trong hệ thống

Ban lãnh đạo và quản lý của CA2 Remote Signing đã phân chia các nhiệm vụ và lĩnh vực trách nhiệm của nhân sự để giảm thiểu mọi khả năng sửa đổi trái phép hoặc vô ý hoặc sử dụng sai tài sản của Công ty. Tất cả các thủ tục liên quan đến an toàn bảo mật trong việc tạo và quản lý chữ ký số được thực hiện bởi đội ngũ nhân sự tin cậy. CA2 Remote Signing duy trì đầy đủ số lượng nhân viên đủ năng lực để đảm bảo tuân thủ pháp luật hiện hành cũng như các quy tắc và quy định nội bộ của công ty tại bất kỳ thời điểm nào trong hoạt động cung cấp dịch vụ của Công ty. Việc phân chia chi tiết các chức năng và trách nhiệm của nhân viên được quy định trong tài liệu nội bộ của CA2 Remote Signing: mô tả công việc, hợp đồng lao động và các quy trình hoạt động nội bộ có liên quan. Các chức năng được phân chia theo cách để giảm thiểu đến mức thấp nhất có thể nguy cơ lạm dụng, rò rỉ thông tin bí mật hoặc xảy ra xung đột lợi ích.

CA2 Remote Signing tuân thủ các yêu cầu sau để phân chia nhiệm vụ và lĩnh vực từng nhân sự phụ trách:

- Vai trò và trách nhiệm, như được mô tả trong chính sách bảo mật thông tin của Công ty, được chỉ ra trong mô tả công việc của nhân viên;
- Các vai trò yêu cầu tin cậy cao trong hệ thống mà hoạt động an toàn bảo mật của CA2 Remote Signing tin cậy vào, được thiết lập rõ ràng;
- Các vai trò yêu cầu tin cậy cao trong hệ thống được quyết định bởi ban quản lý điều hành;
- Các vai trò yêu cầu tin cậy cao trong hệ thống được phê duyệt bởi ban quản lý điều hành và bởi nhân viên nhận đảm nhiệm vai trò đó;
- Các vai trò yêu cầu tin cậy cao trong hệ thống được đảm nhiệm bởi các nhân viên khác nhau;

- CA2 Remote Signing đảm bảo rằng tất cả nhân viên có vai trò yêu cầu tin cậy cao trong hệ thống không có bất kỳ xung đột lợi ích nào có thể làm suy yếu tính công bằng trong công việc đảm nhiệm;

Các vai trò và trách nhiệm yêu cầu tin cậy cao trong hệ thống bao gồm:

- Nhóm a: Nhân sự an ninh hệ thống: chịu trách nhiệm chung về việc quản lý việc áp dụng các chính sách và thủ tục an toàn bảo mật và truy cập thông tin; Các nhân viên an ninh là những người sử dụng hệ thống có đặc quyền;
- Nhóm b: Quản trị viên hệ thống: Được phân quyền cài đặt, cấu hình và hỗ trợ các hệ thống phục vụ vận hành các dịch vụ. Trách nhiệm của quản trị viên hệ thống bao gồm khôi phục hệ thống. Người quản trị hệ thống là người dùng hệ thống có đặc quyền;
- Nhóm c: Nhân sự vận hành hệ thống: Chịu trách nhiệm về việc vận hành hệ thống hoạt động hàng ngày. Nhân sự vận hành hệ thống được ủy quyền để thực hiện sao lưu và phục hồi hệ thống. nhân sự vận hành hệ thống có các vai trò đặc quyền nhưng không được quản lý hoặc cấu hình hệ thống dịch vụ;
- Nhóm d: Kiểm toán viên hệ thống: Kiểm toán viên hệ thống được ủy quyền để xem xét các bản sao lưu và đánh giá nhật ký của các hệ thống tham gia cung cấp dịch vụ. Nhân sự kiểm toán hệ thống có các vai trò đặc quyền nhưng không thể quản lý hoặc cấu hình hệ thống cung cấp dịch vụ.

Nhân sự của CA2 Remote Signing được quản lý cấp cao giao các vai trò yêu cầu tin cậy cao trong hệ thống dựa trên nguyên tắc “đặc quyền thấp nhất” trong quá trình cấu hình các đặc quyền truy cập.

Một số vai trò nhất định (nếu cần) yêu cầu tin cậy cao trong hệ thống có thể sẽ được xem xét áp dụng các vai trò cụ thể bổ sung.

5.3.5. Định danh và xác nhận danh tính đối với từng vai trò trong hệ thống

Nhân sự của CA2 Remote Signing bắt buộc phải được nhận dạng và xác minh danh tính trong các tình huống sau:

- Những nhân sự có trong danh sách những người bị hạn chế tiếp cận các khu vực yêu cầu kiểm soát ra vào;
- Khi nhân sự được đưa vào danh sách những người có quyền truy cập vật lý vào hệ thống công nghệ và tài nguyên mạng của CA2 Remote Signing;
- Khi họ được phân quyền để hoàn thành một vai trò cụ thể được giao;

Thực hiện tạo lập và chỉ định tài khoản, mật khẩu trong hệ thống thông tin của CA2 Remote Signing. Mỗi nhân sự được phân quyền để thực hiện một vai trò nhất định phải tuân theo các yêu cầu sau:

- Vai trò phải là duy nhất và liên quan trực tiếp đến người tương ứng;
- Không được phép chia sẻ với nhân sự khác;
- Được giới hạn trong chức năng do vai trò và sẽ được thực hiện bởi một cá nhân cụ thể. Vai trò được thực hiện thông qua công cụ phần mềm, giải pháp công nghệ và quyền truy cập vào hệ thống.

Các hoạt động do CA2 Remote Signing thực hiện yêu cầu quyền truy cập vào tài nguyên mạng chia sẻ được bảo vệ thông qua các cơ chế an toàn bảo mật để xác thực và mã hóa dữ liệu được truyền đi ở cấp độ mã hóa đủ mạnh.

5.3.6. Yêu cầu đào tạo

CA2 tổ chức đào tạo, bồi dưỡng và cập nhật cho cán bộ của mình trong phạm vi và tần suất hợp lý để đảm bảo rằng cán bộ duy trì mức độ yêu cầu về trình độ để thực hiện trách nhiệm công việc một cách thành thạo và thỏa đáng.

Các nhân sự được cập nhật thường xuyên (ít nhất 12 tháng một lần) về các mối đe dọa mới và các phương pháp bảo mật hiện tại.

Chương trình đào tạo của CA2 được thiết kế theo vai trò, nhiệm vụ và trách nhiệm của mỗi cán bộ và từng nhóm liên quan đến:

- Cơ sở pháp lý về dịch vụ chứng thực chữ ký số công cộng CA2 Remote Signing;
- Quy chế Chính sách an ninh an toàn hệ thống thông tin của Công ty;
- Quy chế chứng thực chữ ký số công cộng CA2
- Quy chế vận hành dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing – CA2Mobile Sign);
- Các điều khoản, thủ tục, quy trình và tài liệu liên quan đến vai trò đảm nhiệm;
- Các thủ tục được thực hiện trong trường hợp có sự cố hệ thống hoặc gián đoạn hoạt động cung cấp dịch vụ;
- Trách nhiệm công việc.
- Trách nhiệm phát sinh từ các vai trò và nhiệm vụ được thực hiện trong hệ thống;
- Hiểu biết về PKI.
- Sử dụng và vận hành hệ thống.
- An ninh hệ thống

- Đánh giá hệ thống
- Quản trị hệ thống
- Xử lý và báo cáo sự cố.
- Báo cáo về nguy cơ thỏa hiệp.
- Quy trình khôi phục sau thảm họa.

5.3.7. Tần suất đào tạo và yêu cầu cập nhật chuyên môn

Dựa trên các chức năng, vai trò công việc của từng cá nhân, tất cả nhân sự của CA2 Remote Signing và, nếu thích hợp, tất cả các nhà thầu phụ phải trải qua khóa đào tạo phù hợp để thực hiện các hoạt động của họ và thường xuyên cập nhật kiến thức của họ về các chính sách và thủ tục của CA2 Remote Signing. Các khóa đào tạo thường xuyên được lên kế hoạch và tiến hành bằng cách tính đến vai trò của nhân viên. Các khóa đào tạo nội bộ hoặc thuê ngoài có thể được thực hiện bằng cách tham dự trực tiếp hoặc trực tuyến.

5.3.8. Xử phạt đối với những hành động trái phép

Các biện pháp kỷ luật thích hợp sẽ được áp dụng đối với nhân viên vi phạm các chính sách hoặc quy trình của CA2 Remote Signing.

Trong trường hợp nghi ngờ hoặc phát hiện hành động trái phép, CA2 Remote Signing sẽ có biện pháp thích hợp như đình chỉ và có thể áp dụng lên đến mức chấm dứt công việc.

Ban quản lý điều hành của CA2 Remote Signing được yêu cầu bắt buộc nhân viên và nhà thầu phụ áp dụng các biện pháp an ninh bảo mật phù hợp với các chính sách và thủ tục đã thiết lập. Các biện pháp để đảm bảo ngay lập tức áp dụng quy trình xử phạt kỷ luật được thực hiện đối với những nhân viên đã vi phạm an toàn bảo mật thông tin.

5.3.9. Yêu cầu phân tách nhiệm vụ

Các nhiệm vụ sau phải tách ra thực hiện:

- Nhân viên An ninh: Chịu trách nhiệm chung trong việc quản lý việc thực hiện các quy trình bảo mật.
- Quản trị viên Hệ thống: Được ủy quyền cài đặt, cấu hình và duy trì các hệ thống đáng tin cậy của CA2 để quản lý dịch vụ CA2 Remote Signing
- Vận hành hệ thống: Chịu trách nhiệm vận hành hệ thống CA2 Remote Signing của CA2 hàng ngày. Được phép thực hiện sao lưu hệ thống.

- Kiểm toán hệ thống: Được ủy quyền để xem các lưu trữ và nhật ký đánh giá của hệ thống .

5.3.10. Tài liệu

Mỗi cán bộ thực hiện một vai trò nhất định sẽ được đào tạo và cung cấp đầy đủ tài liệu hướng dẫn vận hành, quy định, trách nhiệm và các thủ tục cho từng vai trò, nhiệm vụ để thực thi một cách thành thạo và thỏa đáng.

Các vai trò và trách nhiệm bảo mật, như được quy định trong chính sách bảo mật thông tin của CA2, sẽ được ghi lại trong mô tả công việc hoặc trong các tài liệu có sẵn cho tất cả nhân sự liên quan.

5.4. Các quy trình ghi nhật ký hệ thống

Căn cứ mục 6.4.5 của bộ TC ETSI 119.431-1 (*Điều OVR-6.4.5-01 đến 07 Mục Facility, management, and operational controls của tiêu chuẩn ETSI TS 119431-1*) và các tiêu chí SRG_AA.1, SRG_AA.2, SRG_AA.3, SRG_AA.7 và SRG_AA.8 của CEN EN 419.241-1

- CA2 sẽ ghi lại và duy trì khả năng truy cập trong một khoảng thời gian thích hợp, kể cả sau khi các hoạt động của CA2 chấm dứt, tất cả các thông tin liên quan đến dữ liệu do CA2 cung cấp và nhận nhằm mục đích cung cấp bằng chứng trong quá trình tố tụng pháp lý và nhằm mục đích đảm bảo tính liên tục của dịch vụ.
- Tính bảo mật và tính toàn vẹn của các hồ sơ hiện tại và lưu trữ liên quan đến hoạt động của các dịch vụ luôn được duy trì.
- Dữ liệu liên quan đến hoạt động của các dịch vụ sẽ được lưu trữ nguyên vẹn và bí mật theo các thông lệ được công bố.
- Dữ liệu liên quan đến hoạt động của các dịch vụ sẽ được cung cấp nếu được yêu cầu nhằm mục đích cung cấp bằng chứng về hoạt động chính xác của các dịch vụ cho mục đích tố tụng.
- Thời gian chính xác của các sự kiện quan trọng về môi trường, quản lý khóa và đồng bộ hóa đồng hồ của CA2 phải được ghi lại.
- Thời gian được sử dụng để ghi lại các sự kiện theo yêu cầu trong nhật ký kiểm tra được đồng bộ hóa với giờ UTC ít nhất một lần một ngày.
- Các hoạt động sẽ được ghi lại và không dễ dàng bị xóa hoặc phá hủy (trừ khi được chuyển một cách đảm bảo sang phương tiện truyền thông dài hạn) trong khoảng thời gian mà chúng được yêu cầu lưu trữ.

- Việc ghi log được thực hiện bằng tay và tự động. Dữ liệu ghi log tự động được tạo ra và được ghi lại do hệ thống ứng dụng, hệ thống mạng và hệ điều hành hệ thống. Dữ liệu ghi log bằng tay được thực hiện bởi cán bộ giám sát của CA2.
- Chỉ có người quản trị được phép nắm giữ vị trí lưu log và được quy định trong phân công công việc

5.4.1. Các loại sự kiện được ghi lại

CA2 thực hiện ghi lại bằng tay hoặc ghi tự động các sự kiện quan trọng sau:

- Đăng ký và thẩm định đăng ký đề nghị cấp chứng thư số.
- Các sự kiện liên quan đến khóa mật mã HSM.
- Sự kiện ký của người dùng (bao gồm chứng chỉ liên quan đến khóa ký)
- Xác thực của người dùng trong giao thức kích hoạt chữ ký
- Quản lý dữ liệu kích hoạt chữ ký của người ký bởi hệ thống;
- Khởi động và tắt chức năng tạo dữ liệu đánh giá;
- Các thay đổi của các tham số đánh giá.
- Các hoạt động liên quan đến cấp và quản lý chứng thư số.
- Các sự kiện liên quan đến hoạt động của hệ thống.
- Các hoạt động liên quan đến an ninh hệ thống.
- Các hoạt động thu hồi chứng thư số.
- Các hoạt động ra vào phòng hệ thống.
- Các sự kiện sao lưu dữ liệu, dự phòng và phục hồi.

Các sự kiện được ghi gồm các thành phần:

- Ngày, giờ sự kiện.
- Số hiệu, định danh sự kiện và danh tính của người thực hiện.
- Phân loại sự kiện.
- Sự thành công hay thất bại của sự kiện được kiểm tra

5.4.2 Tần suất xử lý bản ghi log

Việc kiểm tra và xử lý kiểm toán ghi log được thực hiện hàng ngày, hàng tuần, hàng tháng và hàng năm.

5.4.3 Bảo vệ bản ghi log và đảm bảo tính khả dụng

Các bản ghi kiểm toán được bảo vệ và phân quyền kiểm soát xem, sửa, xóa, hoặc can thiệp.

CA2 duy trì dữ liệu bản ghi log và đảm bảo các biện pháp được thực hiện để lưu trữ tất cả dữ liệu bản ghi log.

CA2 có các phương án bảo vệ các bản ghi log không bị xóa trái phép, đảm bảo tính toàn vẹn của hệ thống.

CA2 sẽ cung cấp chức năng xác minh tính toàn vẹn của bản ghi log.

Các bản ghi log có thể xóa sau khi đã được lưu trữ ra bộ nhớ ngoài.

5.5. Lưu trữ các bản ghi

Bản ghi log kiểm toán được duy trì tại chỗ trước khi lưu trữ tối đa trong thời gian 3 tháng, sau đó được chuyển lưu trữ dự phòng tại Hanel Data center Sài Đồng. Các bản ghi kiểm toán được lưu trữ trong 7 năm.

CA2 thực hiện sao lưu gia tăng hàng ngày các bản ghi kiểm toán và thực hiện các bản sao lưu dự phòng đầy đủ hàng tuần.

5.6. Thay đổi khóa

CA2 hạn chế việc thay đổi khóa hệ thống, việc thay đổi khóa là hãn hữu hoặc do yêu cầu của cơ quan quản lý Nhà Nước. Trong trường hợp có yêu cầu, CA2 mong muốn việc thay đổi khóa hệ thống được thực hiện trước một đến hai năm thời hạn hết hạn của chứng thư số CA2.

Việc thay đổi khóa hệ thống sẽ gây ảnh hưởng tới việc đảm bảo dịch vụ liên tục tới thuê bao CA2 cam kết:

- Sẽ đảm bảo ảnh hưởng là nhỏ nhất tới thuê bao
- Cung cấp đầy đủ thông tin về kế hoạch thay đổi hợp lý nhất

5.7. Xử lý sự cố, thảm họa và phục hồi

CA2 Remote Signing quản lý tính liên tục đảm bảo hoạt động kinh doanh và cung cấp dịch vụ liên tục bằng cách áp dụng các yêu cầu sau trong hoạt động của mình:

- CA2 Remote Signing xây dựng kế hoạch đảm bảo liên tục hoạt động được kiểm tra định kỳ, duy trì cập nhật phục vụ triển khai trong trường hợp xảy ra sự cố.
- Trong trường hợp xảy ra sự cố và có hỏng hóc các thành phần quan trọng của hệ thống công nghệ, bao gồm phần cứng, phần mềm hoặc có nguy cơ an toàn bảo mật đến khóa mật mã của CA2 Remote Signing, các hoạt động sẽ được khôi phục sau khoảng thời gian trì hoãn theo kế hoạch đảm bảo liên tục hoạt động dịch vụ được phê duyệt. Các nguyên nhân gây ra sự cố được phân tích, các biện pháp thích hợp để loại bỏ, giảm

thiểu được thực hiện, các biện pháp được xác định và triển khai để ngăn chặn sự cố tái diễn.

- CA2 Remote Signing áp dụng các biện pháp để tránh sự gián đoạn của dịch vụ do hành vi cố ý hoặc vô ý của thuê bao hoặc bên thứ ba tích hợp.
- CA2 Remote Signing có nghĩa vụ cung cấp cho thuê bao, bên tích hợp về tính sẵn sàng và chức năng của dịch vụ tuân thủ theo Hợp đồng và Điều khoản áp dụng. CA2 Remote Signing thực hiện báo cáo mức độ sẵn có của dịch vụ định kỳ. Thời gian thiếu khả dụng được theo dõi ở mức sự cố trong hệ thống hỗ trợ. Nếu không đạt được mức cung cấp dịch vụ đã thỏa thuận, CA2 Remote Signing phải chịu trách nhiệm bồi thường, trừ những trường hợp bất khả kháng nằm ngoài tầm kiểm soát của CA2 Remote Signing.

Căn cứ theo mục 6.4.8 của bộ TC ETSI 119.431-1 *(Điều OVR-6.4.8-01 Mục Fa*cility, management, and operational controls của tiêu chuẩn ETSI TS 119431-1)

Các hoạt động của hệ thống liên quan đến quyền truy cập vào hệ thống CNTT, sử dụng hệ thống CNTT và các yêu cầu dịch vụ phải được giám sát.

Các hoạt động bất thường của hệ thống cho thấy có khả năng xảy ra sự cố về bảo mật, bao gồm xâm nhập vào mạng của CA2, sẽ được phát hiện và báo cáo dưới dạng báo động.

CA2 sẽ giám sát các sự kiện sau :

- Khởi động hoặc tắt các chức năng ghi nhật ký
- Giám sát tính sẵn sàng và việc sử dụng các dịch vụ cần thiết với hệ thống mạng CA2

CA2 phải hành động kịp thời và phối hợp để phản ứng nhanh với các sự cố và hạn chế ảnh hưởng của các sự cố về an ninh.

Trong trường hợp sự cố về bảo mật hoặc mất tính toàn vẹn có khả năng ảnh hưởng xấu đến thể nhân hoặc pháp nhân đã được cung cấp dịch vụ, CA2 cũng sẽ thông báo cho thể nhân hoặc pháp nhân về vi phạm bảo mật hoặc mất tính toàn vẹn sớm nhất có thể.

CA2 sẽ thiết lập các thủ tục để thông báo cho các bên phù hợp với các quy tắc quản lý hiện hành về bất kỳ vi phạm bảo mật hoặc tính toàn vẹn nào có ảnh hưởng đến dịch vụ được cung cấp và dữ liệu cá nhân được duy trì trong đó trong vòng 24 giờ sau khi sự cố được xác định

CA2 sẽ giải quyết bất kỳ sự cố nghiêm trọng nào chưa được CA2 giải quyết trước đó, trong khoảng thời gian 48 giờ sau khi phát hiện.

5.7.1. Xử lý sự cố thảm họa

CA2 có trách nhiệm vận hành một kế hoạch khôi phục sự cố và đảm bảo việc giữ duy trì hoạt động . Kế hoạch chi tiết là tài liệu nội bộ không công bố, tuy nhiên sẽ được cung cấp tới những người có trách nhiệm, và được ủy quyền tiến hành kiểm tra an ninh.

Một hệ thống sao lưu đảm bảo phục hồi nguyên trạng CA2 được đặt tại Hanel Data center, Sài Đồng, Gia Lâm.

5.7.2. Tài nguyên máy tính, phần mềm, và /hoặc dữ liệu gặp sự cố

CA2 có hệ thống chỉ dẫn chi tiết về việc quản lý phục hồi dịch vụ trong các trường hợp có sự cố hỏng hóc về tài nguyên máy tính, phần mềm, và / hoặc dữ liệu. Các tài liệu này được lưu hành nội bộ.

5.7.3. Thủ tục khi khóa mật mã bị can thiệp

Trong trường hợp có sự can thiệp vào khóa mật mã của hệ thống, cho dù là bất kỳ lý do gì, các thủ tục triển khai dừng hoạt động đối với khóa mật mã bị can thiệp phải được thực hiện ngay.

CA2 phải thu hồi toàn bộ chứng thư số đã phát hành có sử dụng khóa này và đưa ra các thông báo thích hợp. Sau khi làm rõ nguyên nhân dẫn tới việc tiết lộ này, CA2 có thể:

i. Phát hành một cặp khóa mật mã CA mới;

ii. Phát hành lại chứng thư số tới toàn bộ thuê bao.

5.7.4. Khả năng duy trì hoạt động kinh doanh sau thảm họa

CA2 có hệ thống dự phòng cách ly về địa lý đảm bảo sẵn sàng phục hồi sau thảm họa trong thời gian hợp lý và không làm ảnh hưởng đến hoạt động kinh doanh.

5.8. Dừng hoạt động

CA2 Remote Signing có kế hoạch chấm dứt hoạt động để đảm bảo tính liên tục của dịch vụ và các tình huống cụ thể theo đó phù hợp với các yêu cầu của Quy định về trách nhiệm và để chấm dứt hoạt động của nhà cung cấp dịch vụ ủy thác ký số từ xa với các yêu cầu sau:

- CA2 Remote Signing áp dụng các biện pháp để giảm thiểu bất kỳ sự gián đoạn tiềm ẩn nào đối với các dịch vụ đối với thuê bao và các bên tích hợp ứng dụng nghiệp vụ do việc chấm dứt hoạt động của Công ty. Đặc biệt, CA2 Remote Signing đảm bảo duy trì liên tục kênh cập nhật cần thiết để xác nhận tính đúng đắn của thông tin.

- Kế hoạch được cập nhật kịp thời trong trường hợp cần thiết

Căn cứ mục 6.4.9 của bộ tiêu chuẩn ETSI 119.431-1 *(Điều OVR-6.4.9-01 Mục Facility, management, and operational controls của tiêu chuẩn ETSI TS 119431-1)*

- CA2 sẽ đảm bảo các gián đoạn đối với người đăng ký và các bên được giảm thiểu do việc ngừng cung cấp dịch vụ của CA và đặc biệt là việc tiếp tục duy trì thông tin cần thiết để xác minh tính đúng đắn của các dịch vụ.
- CA2 có phương án khi dừng dịch vụ được cập nhật thường xuyên. Trước khi CA2 chấm dứt các dịch vụ của mình, các thủ tục sau sẽ được áp dụng:

+ CA2 sẽ thông báo cho tất cả thuê bao và các tổ chức khác mà CA2 có thỏa thuận hoặc hình thức quan hệ đã thiết lập khác và các cơ quan chức năng theo quy định.

+ CA2 sẽ cung cấp thông tin về việc chấm dứt cho các bên liên quan theo quy định của pháp luật

+ CA2 có ký quỹ tại Ngân hàng Thương mại Cổ phần Tiên Phong – Chi nhánh Hà Nội với số tiền 5.010.000.000 đ (Năm tỷ không trăm mười triệu đồng chẵn) để giải quyết các rủi ro và các khoản đền bù có thể xảy ra trong quá trình cung cấp dịch vụ do lỗi của tổ chức cung cấp dịch vụ chứng thực chữ ký số công cộng và thanh toán chi phí tiếp nhận và duy trì cơ sở dữ liệu của doanh nghiệp trong trường hợp bị thu hồi giấy phép.

+ CA2 Remote Signing có bảo hiểm dịch vụ để trang trải các chi phí.

+ CA2 sẽ chuyển giao các nghĩa vụ cho một bên tin cậy để duy trì tất cả thông tin cần thiết để cung cấp bằng chứng về hoạt động của CA trong một thời hạn hợp lý

+ Các khóa cá nhân, bao gồm cả các bản sao lưu, phải bị hủy hoặc bị cấm sử dụng, đảm bảo khóa bí mật không thể được truy xuất.

6. ĐẢM BẢO AN TOÀN AN NINH VỀ KỸ THUẬT

6.1. Tạo và phân phối cặp khóa

6.1.1. Sinh khóa ký

- CA2 áp dụng theo các yêu cầu của TT16/2019/TT- BTTTT, đối với quy chế và kỹ thuật sinh khóa ký.
- Khóa ký của thuê bao được sinh trong thiết bị HSM chuyên dụng.
- Sử dụng thiết bị HSM chuyên dụng được cấp chứng chỉ với mức an toàn bảo mật cao nhất theo quy định, được vận hành trong môi trường và quy trình bảo vệ chống lại những lạm dụng có thể liên quan đến khóa ký.

- Các khóa mật mã (bao gồm khóa ký của người ký, khóa cơ sở hạ tầng và khóa điều khiển) không được giữ bên ngoài HSM chuyên dụng.
- CA2 Remote Signing áp dụng mức SCAL2 cho quy trình sinh cặp khóa của thuê bao được đảm bảo kiểm soát bởi SAM chuyên dụng, SAM chuyên dụng đảm bảo sự sở hữu và kiểm soát khóa ký của thuê bao. SAM chuyên dụng được bảo vệ bên trong HSM chuyên dụng vận hành trong môi trường được bảo vệ an toàn chống lại mọi nguy cơ bị lạm dụng. SAM chuyên dụng sử dụng cơ chế xác thực dữ liệu kích hoạt ký số của người ký SAD đảm bảo sự kiểm soát duy nhất khóa ký đối với người ký qua giao thức kích hoạt khóa ký Crypto-protected SAP SCAL2, khẳng định tính chống chối bỏ đối với chữ ký số.
- Căn cứ Mục SRA_SKM.1.2 của bộ TC CEN EN 419 241-1 về yêu cầu mô tả rõ ràng chính xác việc áp dụng đối với môi trường của khóa ký.

CA2 Remote Signing áp dụng:

+ Khóa ký của người ký được tạo và sử dụng bên trong HSM chuyên dụng đạt chứng chỉ EN 419 221-5:2018. Thiết bị HSM chuyên dụng drQSCD (distributed remote Qualified Signature Creation Device), đạt mức an toàn bảo mật EAL4 được tăng cường bởi AVA_VAN.5 và ALC_FLR.3

- Căn cứ Mục SRG_KM.1.2 của bộ TC CEN 419 241-1 về yêu cầu mô tả rõ ràng chính xác việc áp dụng đối với các thuật toán mật mã và độ dài khóa.

CA2 Remote Signing áp dụng:

+ Mật mã phi đối xứng và chữ ký số: RSA, phiên bản 2.1, lược đồ RSAES-OAEP để mã hóa và RSASSA-PSS để ký
+ Độ dài khóa: 2048 bit
+ Mật mã đối xứng: AES and TDEA
+ Hàm băm an toàn: SHA-256

- Căn cứ Mục SRG_KM.1.3 của bộ TC CEN 419 241-1 về yêu cầu mô tả rõ ràng chính xác việc áp dụng đối với việc bảo vệ khóa

CA2 Remote Signing áp dụng:

+ Khóa ký của người ký được tạo và sử dụng bên trong HSM chuyên dụng đạt chứng chỉ EN 419 221-5:2018. Thiết bị HSM chuyên dụng drQSCD (distributed remote Qualified Signature Creation Device), đạt mức an toàn bảo mật EAL4 được tăng cường bởi AVA_VAN.5 và ALC_FLR.3.

+ Các khóa mật mã (bao gồm khóa ký của người ký, khóa cơ sở hạ tầng và khóa điều khiển) không được giữ bên ngoài HSM chuyên dụng.

- Căn cứ Mục SRG_KM.1.4 của bộ TC CEN 419 241-1 về yêu cầu mô tả rõ ràng chính xác việc áp dụng đối với việc khởi tạo thiết bị

CA2 Remote Signing áp dụng:

+ Trước khi HSM sinh khóa HSM bắt buộc phải được khởi tạo về trạng thái thiết bị mới trước đưa vào sử dụng. Việc khởi tạo được kiểm soát bởi cơ chế an toàn kỹ thuật M x N với tối thiểu 02 cán bộ vận hành.

- Căn cứ Mục SRC_SKS.1.1 của bộ TC CEN 419 241-1 về yêu cầu mô tả rõ ràng chính xác việc áp dụng đối với các tham số thuật toán sẽ được sử dụng

CA2 Remote Signing áp dụng:

+ Các tham số thuật toán được áp dụng cho việc tạo chữ ký số đảm bảo theo thời gian hiệu lực của chứng thư số: Áp dụng lược đồ RSASSA-PSS, hàm băm SHA-256

- Căn cứ Mục SRC_SKS.1.3 của bộ TC CEN 419 241-1 về yêu cầu mô tả rõ ràng chính xác việc áp dụng đối với thời điểm sinh khóa

CA2 Remote Signing áp dụng:

+ Thời điểm sinh khóa ký của người ký: khóa ký trong HSM chuyên dụng được sinh sau khi có phương thức xác thực duy nhất từ SAM, cụ thể khóa ký phải được sinh sau khi có khóa xác thực và liên kết 1-1 với khóa xác thực.

- Dịch vụ CA2 Remote Signing và dịch vụ Chứng thực chữ ký số CA2 được quản lý tập trung.

6.1.2. Liên kết phương thức định danh điện tử

CA2 Remote Signing áp dụng triển khai mức SCAL2, đảm bảo mức cao nhất chống lại các mối đe dọa đối với giao thức kích hoạt chữ ký và dữ liệu kích hoạt chữ ký số, bằng cách áp dụng mức bảo mật quy chuẩn cao nhất đối với quy trình thủ tục, đăng ký, phương tiện định danh, cơ chế xác thực...

- CA2 Remote Signing liên kết các khóa ký với phương tiện định danh tham chiếu của người ký;

- CA2 Remote Signing cấp chứng thư chữ ký số từ xa chứng thực khóa công khai của người ký với danh tính của người ký bao gồm định danh thiết bị di động người ký sở hữu tham gia vào ký số và các tham số đảm bảo danh tính duy nhất của người ký

như: mã định thuê bao ký số từ xa, mã định danh khóa ký, mã định danh duy nhất toàn cầu.

- CA2 Remote Signing có thể cung cấp tham chiếu phương tiện định danh tương ứng cho người ký;
- CA2 Remote Signing đảm bảo dữ liệu nhận dạng của người ký trong phương tiện định danh đúng với dữ liệu được liên kết với người bằng chứng thư số liên quan;
- CA2 Remote Signing bảo vệ tính toàn vẹn của các liên kết giữa khóa ký của người ký và phương tiện định danh của người ký.
- Căn cứ Mục SRC_SA.1.1 của bộ TC CEN 419 241-1 về yêu cầu mô tả rõ ràng chính xác quy trình thủ tục xác thực đăng ký sử dụng dịch vụ được áp dụng

CA2 Remote Signing áp dụng:

+ Hồ sơ thủ tục theo quy định của Nghị định 130, Điều 23 về hồ sơ và thủ tục xác thực đăng ký thuê bao.

- Căn cứ Mục SRA_SAP.1.1 của bộ TC CEN 419 241-1 về yêu cầu mô tả rõ ràng chính xác quy trình thủ tục xác thực đăng ký phương tiện định danh điện tử sử dụng dịch vụ được áp dụng.

CA2 Remote Signing áp dụng:

+ Quy trình thủ tục xác thực theo quy định của Nghị định 130, Điều 23 về thủ tục xác thực đăng ký sử dụng dịch vụ đối với thuê bao.
+ Đăng ký sử dụng dịch vụ của thuê bao bắt buộc phải ràng buộc với thiết bị di động do thuê bao sở hữu và sử dụng để thuê bao kích hoạt chữ ký số.

- CA2 Remote Signing thực hiện cấp chứng thư ký số từ xa chứng thực khóa công khai của thuê bao đảm bảo liên kết an toàn và chính xác khóa ký với định danh danh tính của người ký.
- CA2 Remote Signing sẽ tạo tham chiếu định danh danh tính và sẽ thực hiện việc cung cấp với định danh danh tính tương ứng tới người ký.
- CA2 Remote Signing đảm bảo chắc chắn rằng dữ liệu nhận dạng người ký được liên kết chính xác với định danh danh tính người ký và giống với định danh danh tính của chứng thư số được liên kết
- CA2 Remote Signing hỗ trợ tham chiếu định danh danh tính cung cấp bởi bên thứ ba theo quy định của Bộ Thông tin và Truyền thông.

- CA2 Remote Signing áp dụng công nghệ với thuật toán mạnh bảo vệ tính toàn vẹn của các liên kết giữa khóa ký của người ký và tham chiếu định danh danh tính của người ký.
- CA2 Remote Signing cấp chứng thư ký số từ xa cho khóa công khai của thuê bao ký số từ xa. Chứng thư ký số từ xa được cấp cho danh tính của người ký bao gồm định danh thiết bị mà thuê bao sở hữu và tham gia vào sử dụng cho ký số từ xa.

6.1.3. Liên kết chứng thư số

- Căn cứ Mục SRC_SKS.1.2 của bộ TC CEN 419 241-1 về yêu cầu mô tả rõ ràng chính xác quy trình thủ tục liên kết chứng thư số được áp dụng.

CA2 Remote Signing áp dụng:

+ Liên kết khóa ký của người ký với chứng thư số chứng thực khóa công khai của người ký chính xác, an toàn, toàn vẹn được đảm bảo bởi SAM chuyên dụng.
+ Chứng thư ký số từ xa được cấp liên kết chính xác với khóa ký và thiết bị di động người ký sở hữu sử dụng để ký số từ xa.

- Căn cứ Mục SRC_SKS.1.4 của bộ TC CEN 419 241-1 về yêu cầu mô tả rõ ràng chính xác quy trình thủ tục liên kết chứng thư số được áp dụng

CA2 Remote Signing áp dụng:

+ Không cho phép sử dụng khóa ký trước khi chứng thư số chứng thực khóa công khai của người ký được liên kết và hoàn thành bàn giao.

- Căn cứ Mục SRC_SKS.1.5 của bộ TC CEN 419 241-1 về yêu cầu mô tả rõ ràng chính xác quy trình thủ tục bảo vệ liên kết chứng thư số được áp dụng

CA2 Remote Signing áp dụng:

+ CA2 Remote Signing áp dụng công nghệ với thuật toán mạnh bảo vệ tính toàn vẹn của các liên kết giữa khóa ký của người ký với chứng thư số chứng thực khóa công khai của người ký.
+ CA2 Remote Signing sử dụng SAM chuyên dụng với cơ chế Crypto-protected SAP do SAM chuyên dụng bảo vệ.

6.1.4. Cung cấp định danh danh tính điện tử

- CA2 Remote Signing cung cấp phương thức xác thực định danh điện tử danh tính người ký đảm bảo an toàn với mức tin cậy cao nhất giúp cho các dịch vụ có nhu cầu (bên nhận, bên cung cấp ứng dụng nghiệp vụ) có thể xác thực danh tính người ký an

toàn, toàn vẹn và chính xác. Chứng thực khóa công khai 2048bit, chuẩn X.509 theo quy định của Bộ TTTT.

- CA2 Remote Signing cá thể hóa định danh điện tử danh tính của người ký sử dụng dữ liệu kích hoạt ký số của người ký (chứng thư số khóa công khai), đối với dữ liệu bí mật kích hoạt ký số (mã kích hoạt, khóa bí mật) sẽ được SIC xử lý an toàn bảo mật.

6.2. Kiểm soát và bảo vệ khóa bí mật

6.2.1. Sinh khóa ký (Tham chiếu SRA_SKM.1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, SRG_KM.1.1, 2, 3, 4, SRC_SKS.1.1, 2, 3, 4, 5 of 419 241-1), (Tham chiếu Checklist Kỹ Thuật - NEAC).

○ Khách hàng đăng nhập 2FA (xác thực WYK, WYH, WYA) vào ứng dụng CA2 Mobile Sign trên thiết bị di động cá nhân (Bỏ, đã hoàn thành tại bước 5 của quy trình "Đăng ký dịch vụ CA2 RS" theo tài khoản thuê bao đã được cấp, trở thành thuê bao trong hệ thống)

○ Ứng dụng CA2 Mobile Sign (CA2 SIC) theo trình tự SAP, tự động vận hành quy trình khởi tạo khóa ký và có thông báo rõ ràng với TB

○ CA2 SIC thực hiện giao thức SAP sinh bộ dữ liệu kích hoạt khởi tạo khóa ký SAD (SAD khởi tạo khóa ký)

○ CA2 SIC ký HMAC xác nhận bộ dữ liệu SAD khởi tạo khóa ký

○ CA2 SIC thực hiện giao thức SAP gửi SAD khởi tạo khóa ký tới SAM

○ SAM thực hiện giao thức SAP xác SAD khởi tạo khóa ký của TB

○ SAM gửi kích hoạt sinh khóa ký số cho TB trong HSM nếu SAD được xác thực thành công

○ HSM nhận được kết quả xác thực thành công và yêu cầu kích hoạt khóa ký TB từ SAM, thực hiện sinh khóa ký số, kết hợp với thông tin thuê bao và định danh thiết bị di động cá nhân tạo thành CSR, gửi CSR về hệ thống CA2 Remote Signing để cấp Chứng thư số CA2 Remote Signing cho thuê bao.

○ CA2 Remote Signing CA thẩm định yêu cầu cấp bao gồm danh tính thuê bao và định danh thiết bị di động cá nhân thuê bao sở hữu

○ Server CA2 Remote Signing CA thực hiện cấp chứng thư số CA2 Remote Signing,

○ CA2 Remote Signing CA thực hiện thẩm định sau cấp, gửi thông báo cấp thành công đến thuê bao để xác nhận thông tin đã cấp, thực hiện công bố chứng thư số CA2 Remote Signing và cài đặt chứng thư số đã cấp vào HSM

○ Hệ thống CA2 Remote Signing thực hiện gửi thông tin chứng thư số và bản sao ký số file hồ sơ của thuê bao đã cấp về NEAC

6.2.2. Liên kết khóa ký với thiết bị di động của thuê bao (Tham chiếu SRA_SAP.1.1 of 419 241-1), (Tham chiếu Checklist KyThuat - NEAC LNK-6.2.2-03, 04, 05, 06, 10).

- **Bước 1:** Thuê bao nhập thông tin đăng ký trên cổng đăng ký Hồ sơ điện tử CA2 hoặc trên App CA2 Remote Signing. Hệ thống sẽ tạo ra mã đăng ký cho Thuê bao, đồng thời tạo file đăng ký sử dụng dịch vụ với các thông tin đã được nhập
- **Bước 2:** Thuê bao tải file đăng ký sử dụng dịch vụ CA2 Remote Signing trên hệ thống Hồ sơ điện tử CA2 hoặc từ App CA2 Remote Signing được tạo ra từ bước 1.
- **Bước 3:** Thuê bao sử dụng App CA2 broadcast video trực tiếp quá trình ký giấy đăng ký sử dụng dịch vụ với cán bộ thẩm định của CA2. Thời điểm này, cán bộ thẩm định sẽ xem được trực tiếp video Thuê bao ký giấy đăng ký sử dụng dịch vụ, đồng thời hệ thống sẽ ghi nhận log video quá trình ký giấy đăng ký của Thuê bao, đáp ứng tiêu chí đối chiếu với bản gốc của quy trình thẩm định, đồng thời định danh các thông tin thiết bị phục vụ cho việc đăng ký thiết bị sử dụng dịch vụ mà Thuê bao sẽ sử dụng để ký số từ xa, đồng bộ với mã đăng ký đã được tạo từ bước 1
- **Bước 4:** Thuê bao chụp bản chính và tải bản chụp lên hệ thống Hồ sơ điện tử bằng cách sử dụng app CA2 Remote Signing. Thẩm định sẽ đối chiếu bản chụp với bản chính qua camera ghi hình trực tuyến giấy đăng ký sử dụng dịch vụ đã ký. Sau khi hoàn tất thẩm định, Thuê bao sẽ nhận được thông báo qua App CA2 Mobile Sign hoặc hệ thống Hồ sơ điện tử CA2 đã đăng ký trực tuyến thành công.
- **Bước 5:** Bản đăng ký và biên bản bàn giao điện tử thành công dịch vụ ký số từ xa bao gồm các thông tin:
    - Thông tin danh tính thuê bao (theo Nghị định 130/2018/NĐ-CP)
    - Định danh thiết bị (sở hữu của thuê bao)
    - Các thông tin về đăng ký dịch vụ
    - Các điều khoản sử dụng dịch vụ

- Ký xác nhận của thuê bao và nhà cung cấp dịch vụ

6.2.3 Liên kết khóa ký với chứng thư số RS của thuê bao (Tham chiếu SRC_SKS.1.2, 1.4, 1.5 of 419 241-1), (Tham chiếu Checklist Kỹ Thuật - NEAC).

- **Bước 1**: Thuê bao gửi hồ sơ đến thẩm định (CAService online)
  + Nhập thông tin hồ sơ; Thẩm định hồ sơ…
  + CA Service online xử lý hồ sơ
- **Bước 2**: CA Service online Kiểm tra/ khởi tạo thông tin Thuê bao gửi đến SCA
  + SCA tạo Thông tin sử dụng cho khách hàng đến Thuê bao
  + Hệ thống sinh ID và gửi ID cho khách hàng
- **Bước 3**: CA Service online gửi thông tin sử dụng cho khách hàng đến Thuê bao
- **Bước 4**: Thuê bao cài đặt APP xác thực
  + Thuê bao cài đặt App trên mobile, kích hoạt thiết bị và nhập ID CA Service online cung cấp
- **Bước 5**: Thuê bao gửi thông tin APP xác thực yêu cầu cấp CTS cho CA Service online
- **Bước 6**: SAM gửi yêu cầu xác thực đến APP xác thực
- **Bước 7**: APP xác thực gửi yêu cầu xác thực Thuê bao
- **Bước 8**: Thuê bao nhập mã xác thực trên APP xác thực PIN/ Vân tay xác thực và thiết lập mã pin.
- **Bước 9**: APP xác thực sinh khoá và gửi khoá xác thực đến SAM
- **Bước 11**: SAM xác thực khoá và gửi yêu cầu sinh khóa ký đến HSM
- **Bước 12**: HSM gửi yêu cầu tạo request đến CA offline
- **Bước 13**: CA offline gửi Certificate Signing Requests - CSR đến App xác thực và sau khi CA Service online sinh CTS thì CA offline gửi tới SCA để cập nhật chứng thư số
- **Bước 14**: RA gửi CTS đến cho APP xác thực sinh thông báo tới Thuê bao
- **Bước 15**: APP xác thực gửi yêu cầu xác nhận thông tin CTS đến Thuê bao
- **Bước 16**: Thuê bao xác nhận bằng APP xác nhận gửi tới CA offline để CA offline công bố chứng thư số.

<u>6.3. Các vấn đề khác liên quan đến quản lý cặp khóa</u>

6.3.1. Sinh khóa ký (Tham chiếu SRA_SKM.1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, SRG_KM.1.1, 2, 3, 4, SRC_SKS.1.1, 2, 3, 4, 5 of 419 241-1), (Tham chiếu Checklist Kỹ Thuật - NEAC).

○ Khách hàng đăng nhập 2FA (xác thực WYK, WYH, WYA) vào ứng dụng CA2 Mobile Sign trên thiết bị di động cá nhân (Bỏ, đã hoàn thành tại bước 5 của quy trình "Đăng ký dịch vụ CA2 RS" theo tài khoản thuê bao đã được cấp, trở thành thuê bao trong hệ thống)

○ Ứng dụng CA2 Mobile Sign (CA2 SIC) theo trình tự SAP, tự động vận hành quy trình khởi tạo khóa ký và có thông báo rõ ràng với TB

○ CA2 SIC thực hiện giao thức SAP sinh bộ dữ liệu kích hoạt khởi tạo khóa ký SAD (SAD khởi tạo khóa ký)

○ CA2 SIC ký HMAC xác nhận bộ dữ liệu SAD khởi tạo khóa ký

○ CA2 SIC thực hiện giao thức SAP gửi SAD khởi tạo khóa ký tới SAM

○ SAM thực hiện giao thức SAP xác SAD khởi tạo khóa ký của TB

○ SAM gửi kích hoạt sinh khóa ký số cho TB trong HSM nếu SAD được xác thực thành công

○ HSM nhận được kết quả xác thực thành công và yêu cầu kích hoạt khóa ký TB từ SAM, thực hiện sinh khóa ký số, kết hợp với thông tin thuê bao và định danh thiết bị di động cá nhân tạo thành CSR, gửi CSR về hệ thống CA2 Remote Signing để cấp Chứng thư số CA2 Remote Signing cho thuê bao.

○ CA2 Remote Signing n CA thẩm định yêu cầu cấp bao gồm danh tính thuê bao và định danh thiết bị di động cá nhân thuê bao sở hữu

○ Server CA2 Remote Signing CA thực hiện cấp chứng thư số CA2 Remote Signing,

○ CA2 Remote Signing CA thực hiện thẩm định sau cấp, gửi thông báo cấp thành công đến thuê bao để xác nhận thông tin đã cấp, thực hiện công bố chứng thư số CA2 Remote Signing và cài đặt chứng thư số đã cấp vào HSM

○ Hệ thống CA2 Remote Signing thực hiện gửi thông tin chứng thư số và bản sao ký số file hồ sơ của thuê bao đã cấp về NEAC

6.3.2. Liên kết khóa ký với thiết bị di động của thuê bao (Tham chiếu SRA_SAP.1.1 of 419 241-1), (Tham chiếu Checklist KyThuat - NEAC LNK-6.2.2-03, 04, 05, 06, 10).

- **Bước 1:** Thuê bao nhập thông tin đăng ký trên cổng đăng ký Hồ sơ điện tử CA2 hoặc trên App CA2 Mobile Sign. Hệ thống sẽ tạo ra mã đăng ký cho Thuê bao, đồng thời tạo file đăng ký sử dụng dịch vụ với các thông tin đã được nhập
- **Bước 2:** Thuê bao tải file đăng ký sử dụng dịch vụ CA2 Remote Signing n trên hệ thống Hồ sơ điện tử CA2 hoặc từ App CA2 Mobile Sign được tạo ra từ bước 1.
- **Bước 3:** Thuê bao sử dụng App CA2 broadcast video trực tiếp quá trình ký giấy đăng ký sử dụng dịch vụ với cán bộ thẩm định của CA2. Thời điểm này, cán bộ

thẩm định sẽ xem được trực tiếp video Thuê bao ký giấy đăng ký sử dụng dịch vụ, đồng thời hệ thống sẽ ghi nhận log video quá trình ký giấy đăng ký của Thuê bao, đáp ứng tiêu chí đối chiếu với bản gốc của quy trình thẩm định, đồng thời định danh các thông tin thiết bị phục vụ cho việc đăng ký thiết bị sử dụng dịch vụ mà Thuê bao sẽ sử dụng để ký số từ xa, đồng bộ với mã đăng ký đã được tạo từ bước 1

- **Bước 4:** Thuê bao chụp bản chính và tải bản chụp lên hệ thống Hồ sơ điện tử bằng cách sử dụng app CA2 Mobile Sign. Thẩm định sẽ đối chiếu bản chụp với bản chính qua camera ghi hình trực tuyến giấy đăng ký sử dụng dịch vụ đã ký. Sau khi hoàn tất thẩm định, Thuê bao sẽ nhận được thông báo qua App CA2 Mobile Sign hoặc hệ thống Hồ sơ điện tử CA2 đã đăng ký trực tuyến thành công.
- **Bước 5:** Bản đăng ký và biên bản bàn giao điện tử thành công dịch vụ ký số từ xa bao gồm các thông tin:
    - Thông tin danh tính thuê bao (theo Nghị định 130/2018/NĐ-CP)
    - Định danh thiết bị (sở hữu của thuê bao)
    - Các thông tin về đăng ký dịch vụ
    - Các điều khoản sử dụng dịch vụ
    - Ký xác nhận của thuê bao và nhà cung cấp dịch vụ

6.3.3 Liên kết khóa ký với chứng thư số RS của thuê bao (Tham chiếu SRC_SKS.1.2, 1.4, 1.5 of 419 241-1), (Tham chiếu Checklist Kỹ Thuật - NEAC).

- **Bước 1**: Thuê bao gửi hồ sơ đến thẩm định (CAService online)
    + Nhập thông tin hồ sơ; Thẩm định hồ sơ…
    + CA Service online xử lý hồ sơ
- **Bước 2**: CA Service online Kiểm tra/ khởi tạo thông tin Thuê bao gửi đến SCA
    + SCA tạo Thông tin sử dụng cho khách hàng đến Thuê bao
    + Hệ thống sinh ID và gửi ID cho khách hàng
- **Bước 3**: CA Service online gửi thông tin sử dụng cho khách hàng đến Thuê bao
- **Bước 4**: Thuê bao cài đặt APP xác thực
    + Thuê bao cài đặt App trên mobile, kích hoạt thiết bị và nhập ID CA Service online cung cấp
- **Bước 5**: Thuê bao gửi thông tin APP xác thực yêu cầu cấp CTS cho CA Service online
- **Bước 6**: SAM gửi yêu cầu xác thực đến APP xác thực
- **Bước 7**: APP xác thực gửi yêu cầu xác thực Thuê bao

- **Bước 8**: Thuê bao nhập mã xác thực trên APP xác thực PIN/ Vân tay xác thực và thiết lập mã pin.
- **Bước 9**: APP xác thực sinh khoá và gửi khoá xác thực đến SAM
- **Bước 11**: SAM xác thực khoá và gửi yêu cầu sinh khóa ký đến HSM
- **Bước 12**: HSM gửi yêu cầu tạo request đến CA offline
- **Bước 13**: CA offline gửi Certificate Signing Requests - CSR đến App xác thực và sau khi CA Service online sinh CTS thì CA offline gửi tới SCA để cập nhật chứng thư số
- **Bước 14**: RA gửi CTS đến cho APP xác thực sinh thông báo tới Thuê bao
- **Bước 15**: APP xác thực gửi yêu cầu xác nhận thông tin CTS đến Thuê bao
- **Bước 16**: Thuê bao xác nhận bằng APP xác nhận gửi tới CA offline để CA offline công bố chứng thư số.

6.3.4 Cung cấp phương thức xác thực định danh điện tử (Tham chiếu EID-6.2.4-01, 02 of 119 431-1, SAP 419 241-2), (Tham chiếu Checklist Kỹ Thuật - NEAC).

Mô hình ký số từ xa CA2 Mobile Sign phát triển theo mô hình mở, cung cấp sẵn các API services để tích hợp và phát triển cùng những ứng dụng theo nền tảng số, sẵn sàng cung cấp thông tin và giải pháp cho mô hình danh tính số

Định dạng dữ liệu định danh điện tử của thuê bao là theo chuẩn XML

Tính chính xác của dữ liệu định danh điện tử tính đến thời điểm gửi yêu cầu và được ký số cho kết quả trả về theo chuẩn DSIG

Phương thức cung cấp liên kết là SOAP hoặc REST

6.3.5 Xóa, hủy khóa ký (Tham chiếu DEL-6.3.2-02 of 119 431-1, SRG_KM.7.1, SRG_KM.7.2, SRG_KM.7.3 of 419 241-1), (Tham chiếu Checklist Kỹ Thuật - NEAC).

6.3.5.1. Xóa khóa ký

CA2 Mobile Sign áp dụng xóa khóa ký như sau.

- Khóa ký sẽ bị xóa hủy sau khi chứng thực chữ ký số công cộng của khóa ký hết hạn, bị thu hồi, hoặc người ký không còn sử dụng.
- Khi người ký có yêu cầu.
- CA2 Mobile Sign vận hành phiên ký một cách an toàn và đảm bảo chắc chắn khóa ký sẽ bị hủy sau phiên ký trong các trường hợp liên kết giữa khóa ký và người ký không còn được duy trì sau hoạt động ký.

CA2 Mobile Sign không lưu trữ bất kỳ bản sao dự phòng nào của các khóa ký và đảm bảo việc không thể sử dụng bất kỳ thông tin còn lại nào để khôi phục các khóa ký.

- Căn cứ yêu cầu áp dụng Mục SRG_KM.7.1 của bộ TC CEN 419 241-1. Trong trường hợp chứng thực chứng thư chữ ký số công cộng bị thu hồi, khóa ký tương ứng phải bị xóa hủy.

CA2 Mobile Sign áp dụng:

+ CA2 Mobile Sign áp dụng bắt buộc thực hiện xóa hủy khóa ký khi chứng thực chứng thư số khóa công khai công cộng hết hạn hiệu lực hoặc trường hợp khóa ký không còn có giá trị sử dụng đối với người ký.
+ CA2 Mobile Sign thực hiện việc xóa hủy khóa ký khi có yêu cầu hợp lệ từ người ký

- Căn cứ Mục SRG_KM.7.2 của bộ TC CEN 419 241-1 về yêu cầu mô tả rõ ràng chính xác quy trình thủ tục quản lý phiên an toàn được áp dụng

CA2 Mobile Sign áp dụng:

+ CA2 Mobile Sign áp dụng trong trường hợp liên kết giữa khóa ký và người ký không còn được duy trì sau phiên hoạt động ký, thì khóa ký sẽ bị hủy vào cuối phiên hoạt động ký.

- Căn cứ Mục SRG_KM.7.3 của bộ TC CEN 419 241-1 về yêu cầu mô tả rõ ràng chính xác quy trình thủ tục kiểm soát sao lưu an toàn được áp dụng

CA2 Mobile Sign áp dụng:

+ CA2 Mobile Sign áp dụng Cơ chế và thủ tục xóa hủy với tất cả các bản sao lưu của khóa ký đã bị xóa hủy. Và xóa hủy toàn bộ thông tin còn lại nào (Nếu có) có thể được sử dụng để tạo lại khóa ký.

6.3.5.2. Hủy khóa

Bước 1: Thuê bao gửi yêu cầu xóa khóa chứng thư số tới CA Service online

+ CA Service online cập nhật trạng thái CTS

Bước 2: CA Service online gửi yêu cầu cập nhật trạng thái xóa khóa tới SCA

+ SCA cập nhật trạng thái xóa khóa

Bước 3: SCA gửi yêu cầu cập nhật trạng thái xóa khóa tới APP xác thực

+ APP xác thực cập nhật trạng thái xóa khóa

Bước 4: APP xác thực gửi yêu cầu xóa khóa ký tới HSM để xóa khóa ký

Bước 5: HSM gửi công bố tới CA Service online

6.3.6 Lưu trữ, sao lưu phục hồi (Tham chiếu SRG_KM.2.1, SRG_KM.2.2, SRG_KM.2.3 of 419 241-1, GEN-6.3.3-04 of 119 431-1), (Tham chiếu Checklist Kỹ Thuật - NEAC).

6.3.6.1. Quy trình sao lưu khóa ký thuê bao

Bước 1: Phân quyền sao lưu cho nhóm quyền User đặc quyền.

Bước 2: Đăng nhập bộ thẻ Mxn để thực hiện quy trình sao lưu.

Bước 3: Sử dụng công cụ (tool) của nhà cung cấp HSM Trident, thực hiện sao lưu khoá ký thuê bao.

Bước 4: Lưu trữ các phiên bản sao lưu theo quy định của nhà cung cấp HSM trong HSM có mức bảo mật tương đương HSM sinh khóa.

6.3.6.2. Quy trình khôi phục khoá ký thuê bao:

Bước 1: Đăng nhập hệ thống bằng bộ thẻ M x N theo User đặc quyền được giao chức năng sao lưu / khôi phục.

Bước 2: Thực hiện khôi phục khoá ký Thuê bao vào HSM Trident từ HSM backup theo công cụ của nhà cung cấp và tài liệu hướng dẫn

6.3.6.3. Quy trình khắc phục sự cố khi khóa mật mã bị can thiệp

Bước 1: Đăng nhập hệ thống bằng bộ thẻ M x N theo User đặc quyền được giao

Bước 2: Thực hiện tạm dừng HSM Trident

Bước 3: Thực hiện quy trình thu hồi khóa mật mã đối với khóa bị can thiệp

6.3.7 Xác thực người ký (Tham chiếu SRA_SAP.1.1, SRC_SKS.1.2, 4, 5, SRC_SA.1.2, 3, 4, 5, SRC_SA.2.1, 2 of 419 241-1, LNK-6.2.2-03, 04, 05, 06, 10 of 119 431-1), (Tham chiếu Checklist Kỹ Thuật - NEAC).

6.3.7.1. Quản lý xác thực SAD kích hoạt khóa mật mã ký số

Trident SAM chỉ được phép kích hoạt khóa ký khi thực hiện thành công việc xác thực SAD, định danh người ký, dữ liệu ký DTBS/R, xác thực người ký... và người ký xác nhận đồng ý thực hiện.Trident SAM xác thực chữ ký HMAC bộ SAD của người ký theo TridentSAP SCAL2 thành công trước khi cho phép thực thi việc kích hoạt ký chữ ký số đối với khóa bí mật của người ký được quản lý an toàn bảo mật bởi Trident CM đã được bảo vệ trong môi trường an toàn cao.

Giao thức Trident SAP Crypto-protected bảo vệ SAD chống tấn công theo phương thức đoán trực tuyến, đoán ngoại tuyến, MiTM, sao chép thông tin xác thực, lừa đảo, nghe lén, tấn công replay gian lận phiên, chiếm quyền điều khiển, tấn công trung gian, trộm cắp thông tin và các cách tấn công khác để tránh trường hợp khai thác điểm yếu để giành quyền ký gian lận.

Xác thực phân quyền truy xuất đảm bảo người ký không được phép truy cập vào các đối tượng ngoài phạm vi. Đảm bảo DBTS/R được cung cấp bởi sự kiểm soát của người ký, đã xác thực ủy quyền thành công bởi cơ chế Trident SAP Crypto-protected.

Trident SAP điều hành các tiêu chí quan trọng cho quản lý rủi ro, lường trước các rủi ro về SAD và cách sử dụng SAD như: dự đoán online, dự đoán offline, nhân bản credential, phising...

Khoá ký được kích hoạt chỉ được phép ký khi DTBS/R được xác thực thành công và hợp lệ bởi TridentSAP, với cơ chế xác thực thời gian thực OCSP

6.3.7.2. Quản lý dữ liệu kích hoạt ký số SAD

CA2 Mobile Sign quản lý dữ liệu kích hoạt ký số SAD đảm bảo chống chối bỏ chữ ký số và tuân thủ theo quy định như sau:

Dữ liệu kích hoạt ký số SAD là tập dữ liệu là kết quả của quá trình hoạt động mật mã bao gồm các tham số bắt buộc được liệt kê sau đây;

Dữ liệu kích hoạt ký số SAD được tạo bởi SIC và được kiểm soát bởi Crypto-protected SAP SCAL2 của SAM chuyên dụng.

Dữ liệu kích hoạt ký số SAD gồm tối thiểu các tham số với mức độ tin cậy cao nhất:

- Dữ liệu đại diện của tài liệu yêu cầu ký hoặc của lô tài liệu yêu cầu ký
- Các yếu tố định danh danh tính xác thực người ký
- Định danh thiết bị di động người ký sở hữu tham gia kích hoạt khóa ký và
- Tham chiếu chiếu khóa ký

Dữ liệu kích hoạt ký số SAD được sử dụng cho kích hoạt khóa ký khi việc xác thực người ký được thực hiện thành công bởi SAM chuyên dụng.

CA2 Mobile Sign áp dụng giao thức an toàn Crypto-protected SAP SAP do SAM chuyên dụng cung cấp để thực hiện việc truyền đảm bảo dữ liệu kích hoạt ký số SAD tới SAM khi xác thực.

Dữ liệu kích hoạt ký số SAD được đảm bảo chỉ thuộc sự kiểm soát của người ký với mức độ tin cậy cao nhất.

Dữ liệu kích hoạt ký số SAD được bảo vệ ở mức độ tin cậy cao nhất đảm bảo toàn bộ khóa mật mã trong HSM chuyên dụng được bảo vệ tuyệt đối.

SAD được bảo vệ chống lại những rủi ro cho an toàn như việc tái sử dụng, việc bị tấn công giả mạo… giữa người ký và HSM chuyên dụng.

Crypto-protected SAP được thiết kế chuyên dụng để đảm bảo dữ liệu kích hoạt ký số SAD mà SAM chuyên dụng nhận được chắc chắn chỉ thuộc sự kiểm soát của người ký bằng thiết bị di động mà người ký sở hữu và đã được đăng ký hợp lệ trước đó. Dữ liệu kích hoạt ký số SAD được bảo vệ và được đánh dấu hoàn thành tham gia hoạt động kích hoạt phòng tránh không để xảy ra cho những hành động, chẳng hạn như phỏng đoán, nghe lén, lặp lại hoặc can thiệp giao tiếp của tin tặc có trình độ cao, có thể gây trở ngại cho việc xác thực kích hoạt chữ ký số an toàn.

6.3.8. Kích hoạt khóa ký (Tham chiếu SRA_SAP.1.1, 2, 3, 4, 5, 6, 7, SRA_SAP.2.1, 2, 3, 4, 5, 6, 7, 8 SRA_SKM.2.1, 2, 3, 4, 5, 6, 7, 8, SRC_DSC.1.1 of 419 241-1, SIG-6.3.1-08, 09 of 119 431-1), (Tham chiếu Checklist Kỹ Thuật - NEAC).

- Khách hàng đăng nhập 2FA (xác thực WYK, WYH, WYA) vào ứng dụng CA2 Mobile Sign trên thiết bị di động cá nhân (**Bỏ, đã hoàn thành tại bước 5 của quy trình "Đăng ký dịch vụ CA2 RS"** theo tài khoản thuê bao đã được cấp, trở thành thuê bao trong hệ thống)
- Ứng dụng CA2 Mobile Sign (CA2 SIC) theo trình tự SAP, tự động vận hành quy trình khởi tạo khóa ký và có thông báo rõ ràng với TB
- CA2 SIC thực hiện giao thức SAP sinh bộ dữ liệu kích hoạt khởi tạo khóa ký SAD (SAD khởi tạo khóa ký)
- CA2 SIC ký HMAC xác nhận bộ dữ liệu SAD khởi tạo khóa ký
- CA2 SIC thực hiện giao thức SAP gửi SAD khởi tạo khóa ký tới SAM
- SAM thực hiện giao thức SAP xác SAD khởi tạo khóa ký của TB
- SAM gửi kích hoạt sinh khóa ký số cho TB trong HSM nếu SAD được xác thực thành công
- HSM nhận được kết quả xác thực thành công và yêu cầu kích hoạt khóa ký TB từ SAM, thực hiện sinh khóa ký số, kết hợp với thông tin thuê bao và định danh thiết bị di động cá nhân tạo thành CSR, gửi CSR về hệ thống CA2 Mobile Sign để cấp Chứng thư số CA2 Mobile Sign cho TB
- CA2 Mobile Sign CA thẩm định yêu cầu cấp bao gồm danh tính thuê bao và định danh thiết bị di động cá nhân thuê bao sở hữu
- Server CA2 Mobile Sign CA thực hiện cấp chứng thư số CA2 Mobile Sign,
- CA2 Mobile Sign CA thực hiện thẩm định sau cấp, gửi thông báo cấp thành công đến thuê bao để xác nhận thông tin đã cấp, thực hiện công bố chứng thư số CA2 Mobile Sign và cài đặt chứng thư số đã cấp vào HSM
- Hệ thống CA2 Mobile Sign thực hiện gửi thông tin chứng thư số và bản sao ký số file hồ sơ của thuê bao đã cấp về NEAC

6.3.9 Tạo chữ ký (Tham chiếu SRC_DSC.1.1, SRA_SKM.1.1, 2, 3, 4, 5, 6, 7), (Tham chiếu Checklist Kỹ Thuật - NEAC).

- Ký số văn bản:

- Thuê bao lựa chọn tài liệu, thông điệp dữ liệu cần ký số trên hệ thống ứng dụng nghiệp vụ
- SSA gửi thông báo yêu cầu ký số đến ứng dụng CA2 Mobile Sign của TB
- Thuê bao đăng nhập vào ứng dụng CA2 Mobile Sign trên thiết bị di động cá nhân duy nhất đã đăng ký với hệ thống, kiểm tra văn bản cần ký số (WYSIWYS) và chọn chức năng ký số
- Hệ thống quản lý văn bản thực hiện HASH văn bản để cung cấp định danh văn bản cần ký cho ứng dụng ký số (CA2 SIC). Thông qua Server TD đồng thời gửi HASH (DTBS) này tới SAM để đối chiếu với SAD.
- Ứng dụng ký số (CA2 SIC) trên thiết bị di động cá nhân thực hiện giao thức SAP kết nối SAM để lấy định danh phiên ký số, khởi tạo chuỗi SAD (bao gồm định danh thuê bao, định danh thiết bị di động, định danh văn bản, định danh khóa ký, chuỗi Global Unique ID và định danh phiên ký, DTBS), thực hiện ký HMAC chuỗi SAD bằng khóa xác thực trong thiết bị di động, gửi về SAM bằng giao thức SAP cung cấp bởi SAM API để xác thực
- SAM nhận được chuỗi SAD, thực hiện xác thực quyền thuê bao kích hoạt khóa ký số trong HSM, gửi chuỗi SAD sang HSM để thực hiện ký số
- HSM sử dụng định danh khóa ký để xác định và kích hoạt khóa ký sau khi SAM xác thực thành công, thực hiện tạo chữ ký số đối với DTBS, trả về chữ ký số cho ứng dụng ký số (CA2 SIC) trên thiết bị di động bằng giao thức SAP cung cấp bởi HSM API
- Ứng dụng ký số gửi chữ ký số và định danh văn bản về hệ thống ứng dụng nghiệp vụ để so sánh và ghép chữ ký số vào văn bản yêu cầu ký số, thực hiện verify chữ ký số với văn bản và trả về kết quả đã ký. Ứng dụng trên thiết bị di động hiển thị văn bản đã ký cho thuê bao

6.4. Kích hoạt dữ liệu

Kích hoạt khóa ký (Tham chiếu SRA_SAP.1.1, 2, 3, 4, 5, 6, 7, SRA_SAP.2.1, 2, 3, 4, 5, 6, 7, 8 SRA_SKM.2.1, 2, 3, 4, 5, 6, 7, 8, SRC_DSC.1.1 of 419 241-1, SIG-6.3.1-08, 09 of 119 431-1), (Tham chiếu Checklist Kỹ Thuật - NEAC).

- Khách hàng đăng nhập 2FA (xác thực WYK, WYH, WYA) vào ứng dụng CA2 Mobile Sign trên thiết bị di động cá nhân (**Bỏ, đã hoàn thành tại**

bước 5 của quy trình "Đăng ký dịch vụ CA2 RS" theo tài khoản thuê bao đã được cấp, trở thành thuê bao trong hệ thống)

- Ứng dụng CA2 Mobile Sign (CA2 SIC) theo trình tự SAP, tự động vận hành quy trình khởi tạo khóa ký và có thông báo rõ ràng với TB
- CA2 SIC thực hiện giao thức SAP sinh bộ dữ liệu kích hoạt khởi tạo khóa ký SAD (SAD khởi tạo khóa ký)
- CA2 SIC ký HMAC xác nhận bộ dữ liệu SAD khởi tạo khóa ký
- CA2 SIC thực hiện giao thức SAP gửi SAD khởi tạo khóa ký tới SAM
- SAM thực hiện giao thức SAP xác SAD khởi tạo khóa ký của TB
- SAM gửi kích hoạt sinh khóa ký số cho TB trong HSM nếu SAD được xác thực thành công
- HSM nhận được kết quả xác thực thành công và yêu cầu kích hoạt khóa ký TB từ SAM, thực hiện sinh khóa ký số, kết hợp với thông tin thuê bao và định danh thiết bị di động cá nhân tạo thành CSR, gửi CSR về hệ thống CA2 Mobile Sign để cấp Chứng thư số CA2 Mobile Sign cho TB
- CA2 Mobile Sign CA thẩm định yêu cầu cấp bao gồm danh tính thuê bao và định danh thiết bị di động cá nhân thuê bao sở hữu
- Server CA2 Mobile Sign CA thực hiện cấp chứng thư số CA2 Mobile Sign,
- CA2 Mobile Sign CA thực hiện thẩm định sau cấp, gửi thông báo cấp thành công đến thuê bao để xác nhận thông tin đã cấp, thực hiện công bố chứng thư số CA2 Mobile Sign và cài đặt chứng thư số đã cấp vào HSM
- Hệ thống CA2 Mobile Sign thực hiện gửi thông tin chứng thư số và bản sao ký số file hồ sơ của thuê bao đã cấp về NEAC

6.5. Kiểm soát an ninh máy tính

Căn cứ mục 6.5.3 của bộ TC ETSI 119.431-1 *(Điều OVR-6.5.3-01 Mục Technical security controls của tiêu chuẩn ETSI TS 119.431-1)*

CA2 Remote Signing thực hiện kiểm soát an ninh ra vào và sử dụng hệ thống máy tính sạch với nhiều lớp xác thực.

Hệ thống dịch vụ CA2 Remote Signing có hệ thống cảnh báo để thông báo kịp thời về bất kỳ sự kiện bất thường nào có thể ảnh hưởng đến hoạt động của máy chủ hệ thống cung cấp dịch vụ.

Hệ thống dịch vụ CA2 Remote Signing áp dụng cơ chế đưa ra cảnh báo trong trường hợp phát hiện sự kiện bất thường. Cảnh báo kích hoạt thông báo cho quản trị viên. Cảnh báo cũng có thể kích hoạt các hành động tiếp theo để phản ứng với các cuộc tấn công có thể xảy ra.

Các sự kiện bất thường liên quan đến hoạt động của người sử dụng hệ thống có thể bao gồm (nhưng không giới hạn ở):

- Hành động của người vận hành hệ thống ngoài giờ làm việc quy định;
- Những hành động của người dùng được thực hiện với mức độ bất thường (để phát hiện hành động không phải của con người);
- Hành động của người sử dụng bỏ qua các thủ tục, các nghiệp vụ tiêu chuẩn trong các quy trình nhất định;
- Trùng lặp phiên.

Đặc biệt là kiểm soát và cách ly hệ thống cấp và quản lý chứng thư số, việc tách biệt này đảm bảo ngăn chặn các truy cập hệ thống không được kiểm soát.

CA2 Remote Signing sử dụng hệ thống tường lửa để bảo vệ hệ thống cấp và quản lý chứng thư số với kết nối từ trạm cấp cũng được quản lý hoạt động cách ly hoàn toàn với hệ thống mạng nghiệp vụ khác.

CA2 Remote Signing áp dụng quy định sử dụng mật khẩu đủ mạnh sử dụng cơ chế mã hóa MD5, và yêu cầu thay đổi định kỳ thường xuyên.

Quyền truy cập hệ thống CA2 Remote Signing chỉ được cấp cho những nhân sự đã được ủy quyền

CA2 Remote Signing có các quy trình để đảm bảo các dữ liệu nhạy cảm được bảo vệ, không bị tiết lộ thông qua các đối tượng lưu trữ được sử dụng lại (ví dụ: tệp đã xóa) mà người dùng trái phép có thể truy cập được.

CA2 Remote Signing áp dụng hệ thống giám sát và cảnh báo đối với hệ thống cung cấp dịch vụ. Hệ thống cảnh báo sẽ thông báo kịp thời các sự kiện bất thường có thể ảnh hưởng đến hệ thống CA2 Remote Signing để đáp ứng các yêu cầu bảo mật. Mỗi khi có cảnh báo, thông báo về sự kiện bất thường sẽ được gửi đến nhân viên quản trị có liên quan để có giải pháp xử lý kịp thời.

6.6. Kiểm soát an ninh quy trình sử dụng

6.6.1 Giám sát triển khai hệ thống

Các ứng dụng được phát triển và triển khai sử dụng trong CA2 Remote Signing tuân theo các tiêu chuẩn thiết kế, phát triển và triển khai phần mềm của CA2 Remote Signing. CA2 Remote Signing cũng cung cấp phần mềm cho các RA và đại lý

6.6.2 Giám sát quản lý an ninh

CA2 Remote Signing có các thủ tục và biện pháp kiểm soát an ninh trong quá trình thiết lập hệ thống. Các thủ tục và biện pháp này tuân theo tiêu chuẩn quản lý an ninh thông tin ISO 27001:2013

6.6.3 Giám sát an ninh vòng đời

CA2 Remote Signing không quy định cụ thể quy trình giám sát an ninh vòng đời phát triển, triển khai và vận hành hệ thống cung cấp dịch vụ của CA2 Remote Signing.

6.7. Giám sát an ninh hệ thống mạng

Cơ sở hạ tầng của CA2 Remote Signing sử dụng các công cụ kỹ thuật tân tiến phục vụ trao đổi và bảo vệ thông tin nhằm đảm bảo an ninh mạng của hệ thống chống lại bất kỳ sự can thiệp hoặc mối đe dọa nào từ bên ngoài.

Hệ thống dịch vụ CA2 Remote Signing bảo vệ mạng và hệ thống cung cấp dịch vụ khỏi các cuộc tấn công bằng cách áp dụng các yêu cầu sau:

- CA2 Remote Signing tổ chức chia hệ thống thành các mạng hoặc các vùng theo vùng chức năng, vùng logic và vùng vật lý (kể cả theo vị trí) dựa trên việc đánh giá rủi ro và mối liên kết giữa các hệ thống và dịch vụ. Mô tả chi tiết về cấu hình mạng và các phương tiện bảo vệ được trình bày trong tài liệu kỹ thuật cơ sở hạ tầng. Tài liệu này ban hành "nội bộ" và chỉ những người được phân quyền mới có thể truy cập được.
- CA2 Remote Signing áp dụng chỉ một và cùng các biện pháp kiểm soát bảo mật giống nhau cho tất cả các hệ thống nằm trong cùng một khu vực.
- CA2 Remote Signing giới hạn quyền truy cập và giao tiếp giữa các khu vực cần thiết để thực hiện các hoạt động liên quan. Mọi nỗ lực truy cập trái phép vào hệ thống đều được ghi lại thông qua Hệ thống ngăn chặn xâm nhập (IPS).
- CA2 Remote Signing cấm hoặc hủy ngăn chặn triệt để các liên kết và dịch vụ không cần thiết.
- CA2 Remote Signing thường xuyên tổ chức xem xét bộ quy tắc đã thiết lập.

- CA2 Remote Signing duy trì toàn bộ các hệ thống thiết yếu cho hoạt động của dịch vụ trong hai khu vực được bảo vệ. Các máy chủ và hệ thống công nghệ quan trọng của CA2 Remote Signing được kết nối với mạng LAN nội bộ. Việc truy cập từ xa vào mạng thuộc cơ sở hạ tầng (PKI) của CA2 Remote Signing phải thông qua một máy chủ VPN chuyên biệt, với cơ chế xác thực mạnh chỉ cho những nhân sự được ủy quyền liên quan đến việc dịch vụ chữ ký / con dấu số và việc quản lý cơ sở hạ tầng (Cơ sở hạ tầng khóa công khai / PKI).
- CA2 Remote Signing trang bị một vùng mạng đặc biệt riêng phục vụ quản trị hệ thống CNTT và mạng vận hành.
- CA2 Remote Signing không sử dụng các hệ thống được sử dụng phục vụ cho mục đích quản trị chính sách bảo mật cho các mục đích sử dụng khác.
- CA2 Remote Signing tổ chức triển khai tách biệt hệ thống phục vụ cung cấp dịch vụ với các hệ thống được sử dụng để phát triển và thử nghiệm.
- CA2 Remote Signing chỉ cho phép thực hiện thiết lập giao tiếp giữa các hệ thống bảo mật thông qua kênh an toàn tin cậy có sự khác biệt về mặt logic với các kênh giao tiếp khác, đảm bảo xác thực an toàn đầu cuối và bảo vệ kênh dữ liệu không bị sửa đổi hoặc để lộ.
- Khi dịch vụ bên ngoài có yêu cầu Tính sẵn sàng cao (HA) đối với sử dụng dịch vụ CA2 Remote Signing, thì kết nối mạng bên ngoài của dịch vụ đó phải đảm bảo yêu cầu Tính sẵn sàng cao, đảm bảo khả năng truy cập của dịch vụ trong trường hợp một trong các thành phần của nó bị lỗi.
- CA2 Remote Signing thường xuyên quét lỗ hổng bảo mật của các địa chỉ IP công cộng và IP nội bộ đã được xác định và ghi lại bằng chứng từ quá trình này. Để đảm bảo các báo cáo đủ tin cậy, mỗi lần quét lỗ hổng bảo mật được thực hiện bởi người được ủy quyền với các kỹ năng, trình độ và công cụ cần thiết và tuân thủ quy tắc ứng xử và yêu cầu không có xung đột lợi ích.

Sau mỗi lần cập nhật, sửa đổi hoặc nâng cấp các ứng dụng quan trọng, CA2 Remote Signing thực hiện các bài kiểm tra đánh giá xâm nhập hệ thống.

- CA2 Remote Signing ghi lại bằng chứng mỗi lần kiểm tra xâm nhập đã được thực hiện bởi người được ủy quyền với các kỹ năng và công cụ cần thiết, tuân thủ quy tắc ứng xử và không có xung đột lợi ích, để đảm bảo một báo cáo đáng tin cậy.

Căn cứ mục 6.5.5 của bộ TC ETSI 119.431-1 *(Điều OVR-6.5.5-01 Mục Technical security controls của tiêu chuẩn ETSI TS 119431-1)*

CA2 áp dụng mô hình an ninh an toàn hệ thống thông tin theo 7 lớp gồm:

- Lớp hệ thống dữ liệu
- Lớp hệ thống ứng dụng
- Lớp hệ thống dịch vụ
- Lớp hệ thống mạng nội bộ
- Lớp hệ thống mạng ngoại vi
- Lớp hệ thống phòng ốc
- Lớp hệ thống quy trình thủ tục

CA2 tuân thủ theo hướng dẫn và yêu cầu kiểm toán để ngăn chặn sự truy cập trái phép và gây độc hại. Các thông tin, dữ liệu nhạy cảm trao đổi qua mạng được mã hóa .

CA2 áp dụng các biện pháp bảo mật giống nhau cho tất cả các hệ thống trong cùng một khu vực

Tất cả các hệ thống quan trọng được giữ trong 1 vùng bảo mật,chỉ nhân sự có quyền hạn mới được phép truy cập. Hệ thống mạng chuyên dụng để quản trị CNTT được tách riêng khỏi hệ thống mạng dùng chung. Ngoài ra, các kết nối và các dịch vụ không cần thiết sẽ không được sử dụng.

Các hệ thống vận hành CA2 Remote Signing không được sử dụng cho các mục đích khác

Các thiết lập giao tiếp với hệ thống CA2 Remote Signing được thực hiện trên kết nối đáng tin cậy và khác biệt về mặt logic với các kênh giao tiếp khác

CA2 tiến hành quét lỗ hổng bảo mật một cách thường xuyên đối với các địa chỉ IP công cộng, được thực hiện bởi nhân sự có trình độ chuyên môn phù hợp

Mỗi khi tiến hành thay đổi hoặc nâng cấp hạ tầng, CA2 tiến hành thực hiện các kiểm tra xâm nhập hệ thống để đảm bảo hệ thống được an toàn sau khi nâng cấp. Việc thực hiện kiểm tra được tiến hành bởi nhân sự có chuyên môn.

6.8. Quản lý an ninh an toàn hệ thống

Căn cứ mục 6.5.1 của bộ TC ETSI 119.431-1 *(Điều OVR-6.5.1-01 Mục Technical security controls của tiêu chuẩn ETSI TS 119431-1)* và mục 3.1 của bộ TC EN 419.241-1

Đối với quản lý bảo mật, an ninh an toàn hệ thống trong quá trình cung cấp dịch vụ ủy thác ký số từ xa, CA2 Remote Signing tuân thủ và đáp ứng các yêu cầu sau:

- CA2 Remote Signing kiểm soát an toàn bảo mật đảm bảo quản lý giải pháp hệ thống dịch vụ cung cấp dịch vụ với mức độ tin cậy cao nhất.
- Giải pháp công nghệ hệ thống dịch vụ ký số từ xa CA2 Remote Signing hỗ trợ phân định các nhóm vai trò với những đặc quyền được phân vai khác nhau:

+ Tối thiểu, giải pháp hệ thống dịch vụ hỗ trợ các nhóm vai trò đặc quyền sau: nhân viên an ninh bảo mật; quản trị viên hệ thống; nhân sự vận hành hệ thống và nhân sự kiểm toán viên hệ thống;

● Nhân viên an ninh bảo mật: Quản trị triển khai chính sách, quy trình an ninh. Có quyền tiếp cận thông tin liên quan đến an ninh.

● Quản trị viên hệ thống: Phân quyền cài đặt, cấu hình và đảm bảo duy trì vận hành. Bị kiểm soát quyền truy cập thông tin liên quan đến an ninh.

● Nhân viên vận hành hệ thống: Phân quyền vận hành hệ thống nghiệp vụ thường xuyên. Phân quyền sao lưu dự phòng và phục hồi hệ thống. Không có quyền quản trị, cấu hình.

● Nhân sự kiểm toán viên hệ thống: Phân quyền nghiệp vụ Audit cho mục đích đảm bảo an toàn hệ thống. Không có quyền quản trị, cấu hình.

+ Tối thiểu, giải pháp công nghệ hệ thống dịch vụ CA2 Remote Signing hỗ trợ các nhóm vai trò không đặc quyền sau:

● Người ký từ xa: Thuê bao được cấp quyền sử dụng hệ thống dịch vụ ký số từ xa CA2 Remote Signing bằng cách gửi SAD thông qua giao thức SAP để ký tài liệu hoặc DTBS / R (nếu có) được gửi bằng đường SAP;

● Hệ thống ứng dụng nghiệp vụ tích hợp: Hệ thống được ủy quyền gửi yêu cầu ký số DTBS / R tới Hệ thống dịch vụ ký số từ xa CA2 Remote Signing để yêu cầu ký số có thể được ký bởi người ký;

● RA quản lý đăng ký cấp chứng thư số ký số từ xa: Phân quyền CA/RA gửi chứng thư số chứng thực khóa công khai của người ký từ xa tới hệ thống dịch vụ CA Mobile Sign trả kết quả phản hồi cho yêu cầu cấp chứng thư số tương ứng.

+ Một nhân sự hệ thống với phân quyền đặc quyền không được đảm nhận nhiều hơn một phân vai trong các vai trò đặc quyền.

+ Nhân sự vận hành hệ thống có liên kết với vai trò đặc quyền không được liên kết với vai trò không đặc quyền. Người dùng được liên kết với vai trò không đặc quyền không được liên kết với vai trò đặc quyền trong hệ thống.

+ Hệ thống dịch vụ CA2 Remote Signing áp dụng chính sách nhân sự vận hành hệ thống được phân quyền đảm nhận vai trò nhân viên an ninh bảo mật không có quyền trong vai trò kiểm toán viên hệ thống.

+ Hệ thống dịch vụ CA2 Remote Signing áp dụng chính sách nhân sự vận hành hệ thống được phân quyền đảm nhận vai trò quản trị viên hệ thống và / hoặc vai trò người điều hành hệ thống không có quyền trong vai trò nhân sự kiểm toán viên hệ thống và / hoặc vai trò của nhân viên an ninh bảo mật.

+ Những nhân sự thuộc nhóm người dùng hệ thống đặc quyền được đặt tên theo vai trò phân quyền, vai trò được mô tả trong bản mô tả công việc được giao và được đào tạo.

Chỉ những nhân sự có đặc quyền của hệ thống dịch vụ mới có quyền tiếp cận vật lý đến phần cứng và có quyền truy cập quản lý theo phân vai trong hệ thống.

6.9. An ninh an toàn vận hành hệ thống

Căn cứ mục 6.5.2 của bộ TC ETSI 119.431-1 *(Điều OVR-6.5.2-01 Mục Technical security controls của tiêu chuẩn ETSI TS 119431-1)* và mục 4.1,4.2 của bộ TC EN 419.241-1

CA2 Remote Signing vận hành hệ thống dịch vụ với đầy đủ quy trình nghiệp vụ tuân thủ theo quy định của Quy chế đảm bảo các chức năng quản lý vận hành được bảo vệ phù hợp để hoàn thành dịch vụ với chất lượng cao.

CA2 Remote Signing xây dựng bộ tài liệu hướng dẫn vận hành hệ thống CA2 Remote Signing cho nhân viên vận hành hệ thống. Tài liệu hướng dẫn vận hành hệ thống CA2 Remote Signing gồm:

- Hướng dẫn tuân thủ vận hành thích hợp, chính xác và an toàn;
- Các thủ tục tuân thủ giúp giảm thiểu tối đa rủi ro hỏng hóc hệ thống có thể xảy ra;
- Các các thủ tục đảm bảo tính toàn vẹn của hệ thống và bảo vệ thông tin dữ liệu xử lý khỏi vi rút và phần mềm độc hại;

CA2 Remote Signing đảm bảo đầy đủ bộ tài liệu gồm các tài liệu hướng dẫn chi tiết dành cho các vị trí được phân quyền như ở mục 7.1 (như hướng dẫn cài đặt, hướng dẫn quản trị, hướng dẫn vận hành, hướng dẫn sử dụng …)

6.10. Đồng bộ hóa thời gian hệ thống

Hoạt động chữ ký số và xác minh chữ ký số sau này dựa vào thời gian. CA2 Remote Signing thực hiện hợp đồng gắn nguồn thời gian chuẩn theo quy định của Bộ TTTT, đảm bảo hệ thống dịch vụ ký số CA2 Remote Signing được đồng bộ hóa đúng quy chuẩn với nguồn thời gian tiêu chuẩn.

Hệ thống dịch vụ CA2 Remote Signing được đồng bộ thời gian theo quy chuẩn còn nhằm phục vụ việc kiểm tra kiểm toán hệ thống và giám sát an toàn thông tin.

Hệ thống dịch vụ đồng bộ hóa thời gian sử dụng thiết bị chuyên dụng độ chính xác cao, đồng bộ hóa thời gian UTC với nguồn thời gian chuẩn được tự động hóa, dựa trên giao thức NTP với bất kỳ sự khác biệt nào giữa thời gian nguồn và thời gian hệ thống. Trong trường hợp có sự cố về nguồn thời gian với thiết bị chuyên dụng, nếu cần phải thay thế nguồn thời gian bằng nguồn dự phòng, máy chủ thời gian dựa trên internet sẽ được sử dụng làm nguồn thời gian chính xác. Đồng bộ hóa thời gian dựa trên ít nhất hai nguồn thời gian thông qua một giao thức NTP. Thời gian đồng bộ chính xác đối với UTC (Giờ phối hợp quốc tế) có độ chính xác lên đến 0,05 giây.

Để đảm bảo độ chính xác của các sự kiện đã được xác minh, CA2 Remote Signing sử dụng nguồn thời gian được đồng bộ hóa đúng quy chuẩn với nguồn thời gian tiêu chuẩn

6.11. Kiểm soát an ninh an toàn vòng đời

Căn cứ mục 6.5.4 của bộ TC ETSI 119.431-1 *(Điều OVR-6.5.4-01 Mục Technical security controls của tiêu chuẩn ETSI TS 119431-1)*

CA2 sử dụng các hệ thống và các sản phẩm tin cậy, được bảo vệ chống lại sự sửa đổi, đảm bảo an ninh kỹ thuật và độ tin cậy của các quy trình

CA2 tiến hành phân tích các yêu cầu bảo mật ở giai đoạn thiết kế các dự án để đảm bảo rằng yếu tố bảo mật được tích hợp trong hệ thống CNTT

Tính toàn vẹn của hệ thống CA2 Remote Signing luôn được bảo vệ khỏi virus cũng như các phần mềm độc hại, trái phép

CA2 có quy trình đảm bảo các phương tiện, thiết bị được sử dụng trong hệ thống của CA được xử lý an toàn để bảo vệ các phương tiện,thiết bị khỏi bị hư hỏng, trộm cắp,

truy cập trái phép và lỗi thời,đảm bảo các phương tiện,thiết bị chống lại sự hư hỏng,lỗi thời trong khoảng thời gian mà dữ liệu được yêu cầu lưu giữ

CA2 có các thủ tục được áp dụng cho tất cả các vai trò quản trị trong hệ thống có ảnh hưởng đến việc cung cấp dịch vụ. Các thủ tục này được áp dụng để đảm bảo :

- Các bản vá bảo mật được áp dụng trong một thời gian hợp lý sau khi ban hành
- Các bản vá bảo mật không được áp dụng nếu chúng tạo ra các lỗ hổng hoặc tính bất ổn lớn hơn lợi ích của việc áp dụng chúng
- Lý do không áp dụng bất kỳ bản vá bảo mật nào phải được ghi lại.

6.12. An ninh an toàn hệ thống mật mã

CA2 Remote Signing đã công bố các biện pháp kiểm soát bảo mật thích hợp để quản lý hệ thống khóa mật mã và tất cả các thiết bị mật mã trong toàn bộ vòng đời hoạt động. Thuật toán băm và thuật toán bất đối xứng tuân thủ các yêu cầu đặt ra trong Thông tư 16/2019/TT-BTTTT được kết hợp để tạo cặp khóa mật mã (bí mật và công khai). Độ dài khóa tuân thủ các yêu cầu đặt ra trong Thông tư 16/2019/TT-BTTTT: độ dài của cặp khóa chữ ký / con dấu số là 2048 bit, với sự kết hợp áp dụng của thuật toán băm và bất đối xứng: sha 256-with-RSA.

CA2 Remote Signing tạo các cặp khóa mật mã (RSA) bên trong thiết bị bảo mật phần cứng chuyên dụng (HSM / Mô-đun bảo mật phần cứng) với mức độ bảo mật CC EAL 4+ AVA_VAN.5 và ALC_FLR.3 chứng chỉ EN 419 221-5. CA2 Remote Signing chỉ sử dụng các khóa mật mã cho mục đích với các hoạt động như sau:

- Ký chứng thư số cấp ra cho hoạt động hạ tầng;
- Ký vào danh sách thu hồi chứng thư số (CRL) đã được cấp và công bố;
- Ký các chứng thư số đủ điều kiện cho chữ ký / con dấu số của người sử dụng đã được cấp và công bố;

Chữ ký / con dấu số đủ tiêu chuẩn được đảm bảo bằng cách sử dụng các phương tiện kỹ thuật và quy trình phù hợp, tối thiểu sẽ đạt được những điều sau:

- Tính bảo mật của dữ liệu được sử dụng để kích hoạt chữ ký / con dấu số được đảm bảo mức độ an toàn bảo mật cao nhất;
- Thời gian không trùng lặp
- Dữ liệu để tạo chữ ký / con dấu số được bảo mật an toàn, không thể bị trích xuất, chữ ký / con dấu số được bảo vệ một cách đáng tin cậy chống giả mạo bằng cách sử dụng công nghệ có sẵn;

CA2 Remote Signing đảm bảo chỉ duy nhất người ký kiểm soát kích hoạt khóa chữ ký số sử dụng giải pháp công nghệ tân tiến và áp dụng mức độ kiểm soát cao nhất theo quy định của Châu Âu, mức SCAL2, sử dụng giải pháp kích hoạt khóa ký 2 trong 1, với SAM và Mô-đun mật mã tích hợp bên trong thiết bị bảo mật phần cứng chuyên dụng (HSM / Mô-đun bảo mật phần cứng) với mức độ bảo mật CC EAL 4+ AVA_VAN.5 và ALC_FLR.3.

SAM đạt chứng chỉ EN 419 241-2:2019 theo ISO/IEC 18045.

Mô-đun mật mã đạt chứng chỉ EN 419 221-5:2018 theo ISO/IEC 18045/

6.13. Dấu thời gian (Time-Stamping)

Chứng thư số, danh bạ chứng thư số, danh sách thu hồi chứng thư số đều được gắn thông tin thời gian.

7. ĐỊNH DẠNG CHỨNG THƯ SỐ, DANH SÁCH THU HỒI CHỨNG THƯ SỐ (CRL), GIAO THỨC KIỂM TRA TRẠNG THÁI CHỨNG THƯ SỐ TRỰC TUYẾN (OCSP)

7.1. Định dạng của chứng thư số

Chứng thư số CA2 cấp tuân thủ theo tiêu chuẩn X.509 v.3, các quy định tại nội dung về khuôn dạng chứng thư số theo RFC 3280.

Các trường thông tin trong chứng thư số tối thiểu gồm các thông tin sau:

Bảng lược tả các trường cơ bản trong chứng thư số CA2

Tên trường	**Giá trị**
Serial number	Số seri chứng thư số có giá trị duy nhất.
Signature Algorithm	Thuật toán được sử dụng để ký chứng thư số
Issue DN	Tên tổ chức cấp chứng thư số
Valid From	Thời điểm hiệu lực của chứng thư số
Valid To	Thời điểm hết hiệu lực của chứng thư số
Subject DN	Tên của thuê bao
Subject Public Key	Khoá công khai của thuê bao
Signature	Chữ ký số của tổ chức cấp chứng thư số

7.1.1. Số phiên bản

CA2 cung cấp chứng thư số X509 phiên bản 3

a) Phiên bản

Phiên bản X509 V.3.

b) *Số hiệu*

7 3c a9 00 00 00 00 00 10.

7.1.2. Trường mở rộng

Trường mở rộng sẽ được thống nhất bằng thỏa thuận giữa CA2 và thuê bao.

7.1.3. Định danh thuật toán ký số

CA2 không có quy định riêng.

7.1.4. Định dạng tên

CA2 áp dụng theo quy định tại Mục 3.1.1.

7.1.5. Ràng buộc tên

CA2 áp dụng theo quy định tại Mục 3.1.4.

7.1.6. Định danh chính sách

CA2 không áp dụng.

7.1.7. Mở rộng chính sách

CA2 không quy định riêng.

7.1.8. Cú pháp và ngữ nghĩa

CA2 không có quy định riêng.

7.1.9. Xử lý ngữ nghĩa ở các trường mở rộng

CA2 không có quy định riêng.

7.2. Định dạng danh sách thu hồi chứng thư số (CRL)

CRL được phát hành theo phiên bản X509 v.2

CRL được CA2 ký và công bố trên website www.cavn.vn

Đường dẫn và các giao thức hỗ trợ:

http://www.cavn.vn/ca2crl.crl

http://www.cavn.vn/CertEnroll/CA2.crl

http://www.cavn.vn/ca2crl+.crl

http://www.cavn.vn/CertEnroll/ca2crl.crl

Bảng lược tả các trường cơ bản trong CRL CA2:

Tên	Giá trị
Version	Phiên bản CRL
Signature Algorithm	Thuật toán ký số áp dụng
Issue	Tổ chức phát hành
This Update	Ngày phát hành
Next Update	Lịch sẽ phát hành bản CRL mới

Revoke Certificates	Danh sách chứng thư số bị thu hồi

7.2.1. Số phiên bản
CA2 cung cấp CRL phiên bản 2

7.2.2. Trường mở rộng
CA2 không quy định riêng.

7.3. Định dạng giao thức kiểm tra trạng thái chứng thư số trực tuyến (OCSP)

7.3.1 Số phiên bản
CA2 áp dụng theo giao thức RFC 6960

7.3.2 Trường mở rộng
CA2 không quy định riêng.

8. KIỂM ĐỊNH TÍNH TUÂN THỦ VÀ CÁC ĐÁNH GIÁ KHÁC

Công tác kiểm toán hệ thống dịch vụ CA2 Remote Signing tập trung nhiều vào hai nhóm hoạt động, xử lý dữ liệu và hệ thống quản lý các quy trình nghiệp vụ quan trọng. Đảm bảo mục đích kiểm soát thực tiễn cung cấp dịch vụ tuân thủ tuyên bố chất lượng và an ninh an toàn dịch vụ theo quy chế và các điều khoản điều kiện áp dụng.

Chất lượng và an ninh an toàn của CA2 Remote Signing được thực hiện kiểm toán nội bộ định kỳ ít nhất một lần hàng năm, hoặc theo yêu cầu từ Bộ Thông tin và Truyền thông.

Ít nhất hai năm một lần đoàn công tác kiểm tra của Bộ Thông tin và Truyền thông thực hiện kiểm tra toàn diện về chất lượng và đảm bảo an ninh an toàn thực tế triển khai cung cấp dịch vụ theo những quy định và công bố mới nhất của CA2 Remote Signing.

Công tác kiểm toán có thể được thực hiện bởi một đơn vị ngoài có uy tín.

CA2 Remote Signing luôn tuân thủ và thực hiện theo các Thông tư, Nghị định liên quan đã ban hành.

CA2 Remote Signing chấp hành đúng các quy định, thông báo của Bộ Thông tin và Truyền thông, Trung tâm Chứng thực Điện tử Quốc gia (NEAC).

Cơ quan giám sát có thể tiến hành đánh giá hoặc yêu cầu đơn vị phù hợp thực hiện đánh giá sự tuân thủ của CA2 Remote Signing theo quy định của NĐ 130/2018/NĐ-CP, CV 105/NEAC-TDPC ngày 26/3/2021, quy định (EU) số 910/2014, và tiêu chuẩn ISO/IEC 27001 vào bất kỳ lúc nào.

8.1. Tần suất và các tình huống kiểm tra kỹ thuật

Ban quản lý điều hành CA2 Remote Signing lên lịch kiểm tra định kỳ về sự phù hợp của hoạt động hiện tại với các chính sách và quy chế, quy trình đã thiết lập để đảm bảo

luôn cung cấp dịch vụ ủy thác ký số từ xa đủ điều kiện. Ban quản lý điều hành thực hiện kiểm soát hoạt động liên tục để nhân viên CA2 Remote Signing thực hiện chính xác các chỉ dẫn.

8.2. Đơn vị, người thực hiện kiểm tra kỹ thuật

Đơn vị, người thực hiện kiểm định phải là đơn vị độc lập có năng lực thành thạo về công nghệ hạ tầng khóa công khai, công cụ và kỹ thuật an toàn thông tin và được thông qua bởi NEAC, Bộ TTTT.

Việc đánh giá nội bộ được thực hiện bởi các kiểm toán viên CA2 Remote Signing có kinh nghiệm và trình độ chuyên môn cần thiết. Đối với mục đích kiểm toán, CA2 Remote Signing định kỳ tổ chức tập huấn nhân viên kiến thức kỹ thuật cần thiết liên quan đến cơ sở hạ tầng khóa công khai, hoạt động dịch vụ CA, ký số từ xa và an toàn của hệ thống công nghệ, bảo mật thông tin, cũng như kinh nghiệm thực tế sâu rộng trong kiểm toán.

8.3. Các nội dung kiểm tra kỹ thuật

Phạm vị được kiểm toán, kiểm định bao gồm: môi trường hoạt động của CA2 Remote Signing, hạ tầng hệ thống CA2 Remote Signing, hệ thống dịch vụ và xử lý dữ liệu của CA2 Remote Signing, Công tác quản lý và các quy trình quản trị, vận hành, kiểm soát an ninh an toàn, kiểm toán nội bộ của CA2 Remote Signing và các nội dung khác theo yêu cầu của đơn vị kiểm toán.

Việc kiểm tra đánh giá do cơ quan QLNN thực hiện bao gồm các yêu cầu pháp luật đối với các hoạt động của CA2 Remote Signing theo luật hiện hành trong lĩnh vực dịch vụ ủy thác ký số từ xa được cấp phép. Kiểm tra đánh giá do CQ QLNN đánh giá sự phù hợp thực hiện bao gồm toàn bộ hoạt động của CA2 Remote Signing liên quan đến việc cung cấp các dịch vụ và thực hiện tất cả các tiêu chuẩn và tài liệu tiêu chuẩn hóa liên quan đến Quy định của pháp luật: tài liệu; lưu trữ thông tin liên quan đến việc cấp và quản lý các chứng thư số; an ninh vật lý, độ tin cậy của hệ thống công nghệ; các tổ chức cấp chứng nhận.

Phạm vi đánh giá nội bộ bao gồm: kiểm tra hoạt động cung cấp và việc tuân thủ các chính sách, quy chế, quy trình cung cấp dịch vụ ủy thác ký số từ xa được cấp phép; so sánh thực hành và thủ tục được tuyên bố trong tài liệu này với việc triển khai thực tế trong quá trình thực hiện hoạt động của CA2 Remote Signing; kiểm tra hoạt động của

đại lý ủy quyền thẩm định; các tình huống, sự kiện và hoạt động khác liên quan đến cơ sở hạ tầng của CA2 Remote Signing, theo quyết định của ban quản lý điều hành.

8.4. Xử lý khi phát hiện sai sót

Các báo cáo đánh giá bao gồm các phát hiện về việc kiểm tra tài liệu của CA2 Remote Signing, việc tuân thủ các yêu cầu của tiêu chuẩn áp dụng và các quy định, báo cáo phân tích rủi ro an toàn thông tin, các nội dung được đánh giá và thời gian đánh giá. Báo cáo sẽ kiểm tra tính tuân thủ trong tổ chức nội bộ và các thủ tục của CA2 Remote Signing để nâng cao lòng tin vào dịch vụ cung cấp.

Dựa trên các đánh giá của báo cáo, ban quản lý điều hành của CA2 Remote Signing sẽ xác định các biện pháp và thời hạn để khắc phục các thiếu sót và sự không phù hợp. Nhân sự của CA2 Remote Signing sẽ thực hiện các hành động cụ thể để khắc phục trong thời hạn quy định.

Sau khi có báo cáo kiểm toán, căn cứ vào kết quả các vấn đề sai sót, thiếu hụt phải được chỉ ra và xử lý bởi bộ phận quản lý điều hành của CA2 Remote Signing.

CA2 sẽ làm việc với NEAC về những nội dung chưa phù hợp được chỉ ra.

Nếu các vấn đề sự cố và thiếu sót có ảnh hưởng nghiêm trọng tới tính an toàn và toàn vẹn của CA2 Remote Signing, CA2 Remote Signing sẽ xây dựng kế hoạch hành động và thực hiện trong khoảng thời gian sớm nhất, nhưng không quá 48 giờ.

Đối với các sai sót, thiếu hụt kém nghiêm trọng hơn CA2 sẽ xem xét và xác định các hành động cần thực hiện hợp lý.

8.5. Công bố kết quả kiểm tra kỹ thuật

Kết quả kiểm toán, kiểm định sẽ được CA2 công bố trên website https://cavn.vn/

8.6. Tần suất và các trường hợp đánh giá

CA2 tuân thủ chế độ kiểm toán quy định. Ngoài ra CA2 thực hiện tự đánh giá hoạt động của CA2, RA, đại lý ít nhất mỗi năm một lần bởi đơn vị kiểm toán đáp ứng yêu cầu theo quy định của pháp luật và yêu cầu của CA2.

8.7. Danh tính và khả năng của đơn vị, người kiểm tra

Việc thực hiện các hoạt động kiểm toán sẽ được thực hiện bởi những nhân sự không xung đột lợi ích với CA2 Remote Signing

Kiểm toán viên bên ngoài phải độc lập, không liên quan trực tiếp hoặc gián tiếp đến CA2 Remote Signing và không có xung đột lợi ích với CA2 Remote Signing. Các mối

quan hệ giữa CA2 Remote Signing và người kiểm toán bên ngoài được quy định rõ trong hợp đồng

8.8. Lưu trữ kết quả

Kết quả đánh giá nội bộ và bên ngoài thực hiện được lưu trữ an toàn trong kho lưu trữ của CA2 Remote Signing. Tài liệu chứng nhận nhận được từ cơ quan đánh giá sự phù hợp sẽ được công bố trên trang web CA2 Remote Signing.

8.9. Thu thập bằng chứng

CA2 Remote Signing có quy trình thủ tục thu thập bằng chứng bao gồm:

CA2 Remote Signing ghi và lưu trữ đảm bảo truy cập được trong thời gian phù hợp, kể cả trong trường hợp ngừng hoạt động, tất cả thông tin liên quan đến dữ liệu phát sinh và nhận được trong quá trình hoạt động của dịch vụ, nhằm mục đích cung cấp bằng chứng trong thủ tục pháp lý và nhằm mục đích đảm bảo tính liên tục của dịch vụ;

CA2 Remote Signing triển khai thực hiện các biện pháp kỹ thuật và tổ chức thích hợp để chống lại việc xử lý trái phép hoặc bất hợp pháp dữ liệu cá nhân và chống lại việc vô tình làm mất, hủy hoặc làm hỏng dữ liệu cá nhân;

Duy trì tính bảo mật và tính toàn vẹn của hồ sơ làm việc và hồ sơ lưu trữ liên quan đến hoạt động của các dịch vụ;

Hồ sơ liên quan đến hoạt động của dịch vụ được lưu trữ an toàn và bảo mật theo quy định đảm bảo an toàn, bảo mật thông tin cá nhân;

Hồ sơ liên quan đến hoạt động của dịch vụ được cung cấp khi được yêu cầu nhằm mục đích cung cấp bằng chứng về hoạt động chính xác của dịch vụ cho mục đích tố tụng pháp lý theo quy định của pháp luật;

Thời gian chính xác của các sự kiện quản lý hoạt động quan trọng, chẳng hạn như quản lý khóa và đồng bộ hóa đồng hồ, được ghi lại;

Thời gian được sử dụng để ghi lại các sự kiện theo yêu cầu trong nhật ký kiểm toán được đồng bộ hóa với UTC ít nhất một lần một ngày;

Hồ sơ liên quan đến dịch vụ được lưu giữ trong thời gian hợp lệ đảm bảo việc cung cấp bằng chứng pháp lý cần thiết và như được nêu trong Điều khoản và Điều kiện chung và hợp đồng;

Dữ liệu sự kiện được ghi lại đảm bảo không thể bị xóa hoặc phá hủy. Dữ liệu này có thể được chuyển đến phương tiện lưu trữ dài hạn, dữ liệu lưu trữ có thể kiểm chứng được tính toàn vẹn với dữ liệu do hệ thống đang hoạt động quản lý.

CA2 Remote Signing áp dụng các yêu cầu bổ sung sau cho nhật ký phục vụ kiểm tra, đánh giá:

- Hệ thống dịch vụ CA2 Remote Signing lưu trữ nhật ký đánh giá theo luật hiện hành trong thời gian 10 (mười) năm.
- CA2 Remote Signing ghi lại tất cả các sự kiện liên quan đến bảo mật, bao gồm các thay đổi liên quan đến chính sách bảo mật, khởi động và tắt hệ thống, lỗi hệ thống và lỗi phần cứng, hoạt động của tường lửa và bộ định tuyến cũng như các nỗ lực truy cập hệ thống dịch vụ
- CA2 Remote Signing tạo dữ liệu kiểm toán: các sự kiện quan trọng liên quan đến môi trường, cũng như các sự kiện liên quan đến quản lý khóa (tạo, sử dụng và phá hủy; tất cả các nỗ lực truy cập hệ thống dịch vụ); sự kiện ký số (ví dụ: ký số thành công, quản lý yêu cầu ký số DTBS / R và cấp chứng thư số); xác thực người dùng qua SAP; quản lý SAD của người ký; bật và tắt chức năng tạo dữ liệu kiểm toán; thay đổi các thông số kiểm toán…
- CA2 Remote Signing đảm bảo tính khả dụng của nhật ký. Chức năng kiểm toán chỉ cho phép bổ sung thông tin. CA2 Remote Signing hành động ngay trong trường hợp có lỗi không ghi thông tin kiểm toán.
- Giải pháp công nghệ hệ thống bảo vệ các bản ghi được lưu trữ khỏi bị xóa trái phép. CA2 Remote Signing không áp dụng xóa nhật ký hệ thống vận hành.
- Tất cả nhật ký kiểm tra đều chứa: ngày và giờ của sự kiện, loại sự kiện, danh tính chủ thể (người sử dụng, quản trị viên, quy trình), sự kiện thành công hay không thành công, người chịu trách nhiệm cho hành động.
- Hệ thống hỗ trợ tìm kiếm các sự kiện trong nhật ký kiểm tra dựa trên ngày diễn ra sự kiện, loại sự kiện và / hoặc danh tính người dùng. Theo mặc định, hệ thống từ chối tất cả người sử dụng quyền truy cập đọc vào nhật ký kiểm tra, ngoại trừ những người sử dụng được cấp đặc quyền truy cập đọc rõ ràng (ví dụ: người kiểm tra hệ thống).
- CA2 Remote Signing đảm bảo tính toàn vẹn của nhật ký, hệ thống đảm bảo tính toàn vẹn của nhật ký sử dụng chữ ký số và dấu thời gian số. Hệ thống cung cấp chức năng xác minh tính toàn vẹn của dữ liệu kiểm toán. Hệ thống đảm bảo thời gian chính xác của các sự kiện được kiểm tra bằng cách sử dụng nguồn thời gian được đồng bộ hóa đúng quy chuẩn sử dụng nguồn thời gian chuẩn. Thông tin nhạy cảm được lưu trữ một cách an toàn để đảm bảo tính toàn vẹn và bí mật.

CA2 Remote Signing thiết lập kho lưu trữ ngoài. Các thiết bị lưu trữ bên ngoài để giúp thuận lợi cho việc cung cấp bằng chứng pháp lý cần thiết. Tất bộ nhật ký được lưu trữ. Mỗi bản ghi trong kho lưu trữ bao gồm cả thời gian lưu trữ. Kho lưu trữ không bao gồm thông tin nhạy cảm (ví dụ: mật khẩu). CA2 Remote Signing đảm bảo tính toàn vẹn của dữ liệu được lưu trữ và ngăn chặn các sửa đổi trái phép đối với hồ sơ lưu trữ

9. CÁC NỘI DUNG NGHIỆP VỤ VÀ PHÁP LÝ KHÁC

9.1. Phí/Giá

Tất cả những thông báo về việc tính phí phải được gửi tới thuê bao

9.1.1. Phí cấp phát, gia hạn, tạm dừng, khôi phục, thu hồi chứng thư số ký số từ xa và chữ ký số từ xa

- Phí cấp phát, gia hạn chứng thư số ký số từ xa: Theo "Phương án Kinh doanh Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Remote Signing)"
- Phí ký chữ ký số từ xa: Theo "Phương án Kinh doanh Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Remote Signing)"
- Phí tạm dừng, khôi phục, thu hồi chứng thư chữ ký số từ xa: miễn phí

9.1.2. Phí truy cập danh bạ chứng thư chữ ký số từ xa

Miễn phí

9.1.3. Phí truy cập thông tin trạng thái thu hồi (Dịch vụ xác minh hiệu lực của chứng thư số)

Miễn phí

91.4. Phí những dịch vụ khác như là thông tin về chính sách

Không áp dụng

9.1.5. Phí duy trì hệ thống kiểm tra trạng thái chữ ký số

a) Chứng thư số doanh nghiệp

Cơ sở pháp lý: Thông tư 305/2016/TT-BTC ngày 15/11/2016 quy định mức thu, chế độ thu, nộp, quản lý và sử dụng phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số.

- Mức thu phí dịch vụ duy trì hệ thống kiểm tra trạng thái chứng thư số: 3.000 đồng / chữ ký số / tháng.
- Chứng thư số phát sinh hiệu lực hoạt động tại bất cứ thời điểm nào của tháng được tính là 01 (một) tháng sử dụng.

b) Chứng thư số cá nhân, cá nhân thuộc tổ chức

Không áp dụng

9.1.6. Chính sách hoàn phí

Bất kỳ các khoản phí nào cho việc đề nghị cấp chữ ký số từ xa mà không được phê chuẩn sẽ được hoàn trả.

9.2. Trách nhiệm tài chính

9.2.1. Bảo lãnh Ngân hàng theo Nghị định 130/2018/NĐ-CP

CA2 Remote Signing ký quỹ tại Ngân hàng Thương mại Cổ phần Tiên Phong – Chi nhánh Hà Nội với số tiền 5.010.000.000 đ (Năm tỷ không trăm mười triệu đồng chẵn) để giải quyết các rủi ro và các khoản đền bù có thể xảy ra trong quá trình cung cấp dịch vụ do lỗi của CA2.

9.2.2. Bảo hiểm dịch vụ

CA2 Remote Signing ký bảo hiểm cho dịch vụ ủy thác ký số từ xa. Bảo hiểm được giao kết trong thời gian liên tục và được gia hạn hàng năm. Bảo hiểm sẽ bao gồm trách nhiệm của CA2 Remote Signing đối với người sử dụng và các bên đối với các thiệt hại vật chất và phi vật chất trong giới hạn được quy định trong luật hiện hành. Khi xảy ra sự kiện có thể dẫn đến yêu cầu bồi thường thiệt hại thuộc phạm vi bảo hiểm, đương sự phải thông báo bằng văn bản cho CA2 Remote Signing và công ty bảo hiểm trong vòng 7 ngày sau khi biết về sự kiện. Phạm vi bảo hiểm cho những thiệt hại phi vật chất và / hoặc vật chất mà chủ sở hữu / người chữ ký số phải chịu sẽ không vượt quá số tiền được quy định bởi luật.

9.2.3. Trách nhiệm bồi thường thiệt hại cho thuê bao

CA2 có trách nhiệm bồi thường thiệt hại cho thuê bao trong những trường hợp sau:

- Thiệt hại xảy ra là hậu quả của việc để lộ thông tin của thuê bao mà CA2 có nghĩa vụ lưu trữ bí mật.
- Thiệt hại xảy ra do cung cấp chứng thư chữ ký số những thông tin không chính xác so với những thông tin do thuê bao cung cấp.
- Thiệt hại xảy ra là hậu quả của việc không tuân thủ các quy định tại khoản 2.1
- CA2 có trách nhiệm bồi thường theo các mức bảo hiểm đã công bố

9.2.4. Trách nhiệm bồi thường của bên khác

(1) Bồi thường bởi bên vi phạm

Trong phạm vi của luật áp dụng, bên vi phạm bồi thường cho CA2 và cho các bên liên quan trong các trường hợp:

- Xuyên tạc sự thật trong đơn đăng ký cấp chữ ký số từ xa.
- Vi phạm tiết lộ những tài liệu trên đơn xin cấp chữ ký số từ xa, 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.
- Thiếu sót trong việc bảo vệ dữ liệu 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 dữ liệu 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.

(2) Bồi thường do bên nhận

Trong phạm vi của luật áp dụng, thỏa thuận bên nhận và các thỏa thuận khác yêu cầu bên nhận bồi thường cho CA2 Remote Signing và cho các bên liên quan về:

- Bên nhận thiếu sót trong việc thực hiện các nghĩa vụ của mình
- Sự tin tưởng của bên nhận vào chữ ký số không phù hợp với một số trường hợp
- Bên nhận thiếu sót trong việc kiểm tra tình trạng của chữ ký số để xác định xem liệu chữ ký số đó đã hết hạn hay bị thu hồi chưa.

9.3. Bảo mật các thông tin nghiệp vụ

CA2 Remote Signing sẽ tập hợp tất cả các thông tin của thuê bao: tên đầy đủ, số điện thoại, chứng minh thư…. thông tin trong số các thông tin đó được dùng vào các trường thích hợp khi CA2 Remote Signing cung cấp dịch vụ chữ ký số từ xa

- Các thông tin đã được ban hành trong chứng thư chữ ký số và CRL không được coi là bí mật.
- CA2 Remote Signing sẽ không thu thập bất kỳ một thông tin bí mật nào ngoại trừ những thông tin phục vụ cho CA2 Remote Signing, RA, đại lý trong việc xác minh danh tính, nhận dạng cá nhân phục vụ cho việc cấp chữ ký số của thuê bao.
- CA2 Remote Signing đảm bảo các thông tin cá nhân CA2 Remote Signing đã thu thập sẽ không được dùng cho bất cứ mục đích nào khác.

9.4. Bảo mật thông tin cá nhân

Các thông tin cá nhân được thu thập để phục vụ cho việc đăng ký như:

- Tên của người đăng ký
- Địa chỉ

- Tên tổ chức
- Vị trí
- Điện thoại
- Email
- Định danh điện thoại di động
- …

CA2 Remote Signing đảm bảo không cung cấp thông tin này cho bên thứ ba trừ trường hợp khi có yêu cầu của cơ quan quản lý Nhà Nước có thẩm quyền theo quy định của pháp luật.

9.5. Quyền sở hữu trí tuệ

9.5.1. Khóa riêng

Khóa riêng sẽ được xem là một tài sản riêng của người sở hữu chữ ký số hợp pháp bao gồm cả khóa công khai tương ứng

9.5.2. Quyền sở hữu trong các thông tin chữ ký số và thông tin thu hồi chữ ký số

CA2 Remote Signing có quyền sở hữu trí tuệ đối với toàn bộ thông tin chứng thư chữ ký số và thông tin thu hồi chứng thư chữ ký số mà CA2 Remote Signing phát hành

9.5.3. Quyền sở hữu trong văn bản này

CA2 Remote Signing có quyền sở hữu trí tuệ đối với văn bản này và tất cả các tài liệu liên quan do CA2 Remote Signing phát hành.

9.6. Tuyên bố và cam kết

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

9.7. Từ chối trách nhiệm

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

9.8. Giới hạn trách nhiệm

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

9.9. Bồi thường thiệt hại

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

9.10. Hiệu lực của Quy chế chứng thực

Văn bản này có hiệu lực và được công nhận từ khi CA2 Remote Signing được cấp phép Kết thúc trong các trường hợp:

- Hết hạn chứng thư chữ ký số từ xa CA2 Remote Signing
- Dịch vụ của CA2 Remote Signing chấm dứt

- Một phiên bản mới được phát hành.

9.11. Thông báo và trao đổi thông tin với các bên tham gia

Được quy định cụ thể khi chính thức cung cấp dịch vụ

9.12. Bổ sung và sửa đổi

Mỗi lần thay đổi, tất cả các thay đổi này được công bố trên hệ thống trực tuyến của CA2 Remote Signing

9.13. Thủ tục giải quyết tranh chấp

Quy định cụ thể trong hợp đồng cung cấp và các tài liệu phục vụ cung cấp Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign).

9.14. Hệ thống pháp lý điều chỉnh

Luật pháp Việt Nam

9.15. Phù hợp với pháp luật hiện hành

Quy định cụ thể trong hợp đồng cung cấp

9.16. Các điều khoản chung

Quyền và nghĩa vụ các bên:

9.16.1. Quyền và nghĩa vụ của CA2 Mobile Sign

CA2 Remote Signing là đơn vị cung cấp chữ ký số từ xa và có các đơn vị RA, đại lý được ủy quyền làm nhiệm vụ thẩm định, đăng ký chữ ký số cho người dùng cuối.

Quyền của CA2 Mobile Sign

- Thay đổi các quy trình nghiệp vụ theo quy định mới ban hành của cơ quan quản lý Nhà nước có thẩm quyền.
- Được miễn trách nhiệm trong trường hợp hệ thống xử lý, hệ thống truyền tin,... bị trục trặc, hoặc vì bất cứ lý do gì ngoài khả năng kiểm soát của CA2 Remote Signing.
- Tạm dừng, thu hồi chứng thư chữ ký số từ xa, hủy khóa ký số từ xa khi phát hiện tài liệu, thông tin do thuê bao cung cấp còn thiếu, không chính xác, không trung thực, sai sự thật.
- Cung cấp thông tin của thuê bao cho cơ quan quản lý Nhà nước phục vụ công tác đảm bảo an ninh thông tin, điều tra phòng chống tội phạm theo đúng trình tự, thủ tục pháp luật về tố tụng quy định.

Nghĩa vụ của CA2 Remote Signing

- Không cung cấp những thông tin sai lệch.
- Không mắc lỗi thông tin trong chứng thư chữ ký số từ xa được cấp.

- Đảm bảo cho chứng thư số của thuê bao theo tiêu chuẩn trong Quy chế này và Quy chế CA2 CP/CPS phiên bản mới nhất.
- Đảm bảo các dịch vụ theo tiêu chuẩn trong Quy chế này.

9.16.2. Quyền và nghĩa vụ của thuê bao

Quyền của thuê bao

- Dịch vụ chữ ký số và chứng thực chữ ký số từ xa được cung cấp trực tiếp tới thuê bao theo đúng gói dịch vụ mà thuê bao đã yêu cầu
- Chữ ký số của thuê bao được chấp nhận và hoạt động trong thời gian có hiệu lực của chứng thực chữ ký số

Thuê bao có quyền yêu cầu cấp mới dịch vụ

- Thuê bao có quyền yêu cầu CA2 Remote Signing tạm dừng, thu hồi dịch vụ và tự chịu trách nhiệm về yêu cầu đó.

Nghĩa vụ của thuê bao

- Mọi cam kết của thuê bao liên quan đến dịch vụ chữ ký số và chứng thực chữ ký số từ xa là đầy đủ, chính xác và hợp lệ. Tất cả các thông tin cung cấp bởi thuê bao và chứa bên trong chứng thư chữ ký số từ xa là đầy đủ, chính xác và hợp lệ. Chứng thư chữ ký số và chữ ký số từ xa phải được sử dụng cho các mục đích hợp pháp và tuân theo những yêu cầu trong Quy chế này.
- Thuê bao có nghĩa vụ bảo mật dữ liệu riêng tư, sử dụng thiết bị điện thoại di động tin cậy. Ngăn chặn việc mất cắp, lộ thông tin, hay sửa đổi, phá hủy thiết bị. Phải thông báo tới CA2 Remote Signing, RA, đại lý ngay khi khóa bí mật bị lộ hay sửa đổi, phá hủy
- Đồng ý để CA2 Remote Signing công khai thông tin về chứng thư chữ ký số từ xa của thuê bao trên cơ sở dữ liệu về chứng thư số của CA2 Remote Signing.
- Thuê bao có nghĩa vụ cung cấp những thông tin cần thiết cho các cơ quan tiến hành tố tụng, cơ quan an ninh để phục vụ việc đảm bảo an ninh quốc gia hoặc điều tra theo quy định của pháp luật.
- Không được giả mạo chữ ký số.
- Nếu có bất kỳ sự thay đổi thông tin nào, đều phải thông báo tới CA2 Remote Signing.
- Yêu cầu thu hồi chứng thư chữ ký số trong trường hợp có nhu cầu.

9.16.3. Quyền và nghĩa vụ của người nhận

Quyền của người nhận

- Người nhận là cá nhân hay một tổ chức tin tưởng dịch vụ chữ ký số và dịch vụ chứng thực chữ ký số từ xa, kiểm tra tính hợp lệ chữ ký số của đối tác theo thỏa thuận và cam kết giữa hai bên
- Người nhận có quyền xác nhận các thông tin của người kýđối với chữ ký số là đúng sự thật
- Người nhận dựa vào các thông tin của chữ ký số và các thông tin trong Quy chế này để đưa ra quyết định thực hiện thỏa thuận và cam kết giữa hai bên đối tác
- Người nhận có thể là một thuê bao hoặc không là một thuê bao của dịch vụ CA2 Remote Signing

Nghĩa vụ của người nhận

- Chỉ tin tưởng chữ ký số của người ký do dịch vụ CA2 Remote Signing cung cấp khi kiểm tra thấy hợp lệ và cập nhật thường xuyên.
- Chỉ tin tưởng và chữ ký số CA2 Remote Signing đang hoạt động
- Phải thông báo cho CA2 Remote Signing, RA, đại lý ngay lập tức nếu nghi ngờ rằng khóa bí mật bị can thiệp, mất kiểm soát hay sai sót, phá hủy.

9.16.4. Quyền và nghĩa vụ của RA, đại lý CA2 Remote Signing

Quyền của RA, đại lý CA2 Remote Signing

- Thẩm định thông tin của thuê bao theo ủy quyền của CA2 Remote Signing
- Hỗ trợ đăng ký dịch vụ cho thuê bao

Nghĩa vụ của RA, đại lý CA2 Remote Signing

- RA, đại lý CA2 Remote Signing tổ chức thực hiện kinh doanh đúng loại dịch vụ sản phẩm đã được ủy quyền bởi CA2 Remote Signing và tuân theo các quy định tại Hợp đồng đại lý
- Khi RA, đại lý CA2 Remote Signing yêu cầu cấp dịch vụ chữ ký số từ xa CA2 Remote Signing phải cung cấp đầy đủ hồ sơ, địa chỉ liên hệ của thuê bao để CA2 Remote Signing xác minh trước khi cấp phát.
- RA, đại lý CA2 có nghĩa vụ tuân thủ Quy chế vận hành Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign)
- RA, đại lý CA2 Remote signing được CA2 Remote Signing ủy quyền để cung cấp Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2

Mobile Sign) tới khách hàng và là thành phần không thể tách rời với CA2 về mặt pháp lý

- Các hồ sơ xin cấp chữ ký số của thuê bao phải được lập bởi cán bộ của RA, đại lý CA2 Mobile Sing có hiểu biết pháp luật về chữ ký số và chứng thực chữ ký số từ xa.
- RA, đại lý CA2 Remote signing có trách nhiệm tư vấn đầy đủ, trung thực cho khách hàng về sản phẩm, dịch vụ của CA2 Remote signing và chịu trách nhiệm pháp lý trước khách hàng nếu nội dung của sản phẩm dịch vụ không đúng như CA2 Remote signing cung cấp.
- RA, đại lý CA2 Mobile Sign phải sử dụng các mẫu biểu, tài liệu liên quan đến việc cung cấp và sử dụng dịch vụ do CA2 Mobile Sign cung cấp. Nếu có bổ sung thì phải có công văn đề nghị kèm cùng biểu mẫu mới
- Chịu trách nhiệm về thuê bao bị tạm dừng, thu hồi chứng thư chữ ký số,hủy khóa ký số từ xa, khóa tài khoản do lỗi của RA, đại lý CA2 Mobile Sign
- RA, đại lý CA2 Mobile Sign có nghĩa vụ giải trình trước CA2 Mobile Sign khi có khiếu nại từ khách hàng và các đại lý khác. Trong trường hợp kết luận xác định lỗi thuộc về RA, đại lý CA2 Mobile Sign thì RA, đại lý CA2 Mobile Sign chịu trách nhiệm hoàn trả đầy đủ các khoản chi phí đã nhận từ khách hàng, bồi thường đầy đủ tất cả thiệt hại cho bên khiếu nại cũng như tổn thất về uy tín gây ra cho CA2 Mobile Sign.
- RA, đại lý CA2 Mobile Sign có trách nhiệm cung cấp các số liệu, thông tin về công việc định kỳ hoặc đột xuất theo yêu cầu của CA2 Mobile Sign.
- RA, đại lý CA2 Mobile Sign phải thực hiện đầy đủ theo đúng quy trình bán hàng, cấp lại, đối soát và thanh toán quy định tại Hợp đồng hợp tác.

9.17. Các điều khoản khác

9.17.1. Tổ chức

Căn cứ mục 6.8.1 của bộ TC ETST 119.431-1 *(Điều OVR-6.8.1-01 và mục 7.1 của bộ TC ETSI EN 319 401)*

CA2 là tổ chức chứng thực chữ ký số công cộng được NEAC RootCA cấp chứng thư số theo giấy phép của Bộ Thông tin và Truyền thông.

CA2 Mobile Sign cung cấp Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing- CA2 Mobile Sign) cho các tổ chức, doanh nghiệp và cá nhân để thực hiện giao dịch trong môi trường mạng mở an toàn và có giá trị pháp lý theo quy định của pháp luật Việt Nam.

CA2 Remote Signing xây dựng một mô hình PKI có mức độ tin cậy cao trong việc sử dụng chữ ký số phục vụ chống chối bỏ, xác thực và toàn vẹn các dữ liệu và giao dịch điện tử.

CA2 Remote Signing đảm bảo các dịch vụ của mình có thể sử dụng được đối với tất cả những người đăng ký có hoạt động nằm trong lĩnh vực hoạt động đã được công bố của CA2 Remote Signing và đồng ý tuân thủ các nghĩa vụ của họ được quy định trong các điều khoản và điều kiện của CA2 Remote Signing.

CA2 Remote Signing có sự ổn định về tài chính và các nguồn lực cần thiết để hoạt động phù hợp với chính sách này.

CA2 Remote Signing có các chính sách và thủ tục để giải quyết các khiếu nại và tranh chấp từ khách hàng hoặc các bên khác về việc cung cấp dịch vụ hoặc bất kỳ vấn đề liên quan nào khác.

9.17.2. Kiểm thử bổ sung

CA2 Remote Signing không áp dụng

9.17.3. Khuyết tật

CA2 Remote Signing không áp dụng

9.17.4. Phương án cung cấp trực tuyến thông tin thuê bao tới Trung tâm Chứng thực điện tử quốc gia (NEAC)

Hệ thống Dịch vụ chữ ký số và chứng thực chữ ký số từ xa CA2 (CA2 Remote signing-CA2 Mobile Sign) sẵn sàng cung cấp thông tin thuê bao trực tuyến theo như yêu cầu của NEAC.

10. TỔ CHỨC NỘI BỘ

10.1. Đánh giá rủi ro

CA2 Mobile Sign phân loại và quản lý danh mục đăng ký của tất cả các tài sản phù hợp với các yêu cầu của ISO / IEC 27001. Chính sách bảo mật của CA2 Remote Signing quy định, phân tích đánh giá lỗ hổng được tiến hành đối với tất cả các thủ tục, ứng dụng và hệ thống thông tin nội bộ. Các yêu cầu phân tích cũng có thể được xác định bởi một tổ chức bên ngoài.

Quản lý rủi ro là một quy trình có cấu trúc, nhất quán và liên tục được tích hợp trong hoạt động của CA2 Remote Signing, các quyết định được xác định, đánh giá và thực hiện và các sự kiện có thể xảy ra được báo cáo có thể tác động bất lợi hoặc tích cực đến việc hoàn thành các mục tiêu của Công ty. CA2 Remote Signing xác định các yêu cầu

bảo mật và quy trình hoạt động cần thiết để thực hiện các biện pháp đã chọn để ngăn chặn các hoạt động rủi ro, được ghi lại trong Chính sách bảo mật thông tin và trong Thực tiễn cung cấp các dịch vụ ủy thác ký số từ xa đủ điều kiện. Đánh giá rủi ro được thực hiện và xem xét ít nhất mỗi năm một lần. Ban quản lý của CA2 Remote Signing phê duyệt đánh giá rủi ro và ghi nhận rủi ro còn lại đã được xác định.

CA2 Remote Signing tuân thủ các yêu cầu sau liên quan đến việc đánh giá rủi ro:

CA2 Remote Signing thực hiện đánh giá rủi ro để xác định, phân tích và đánh giá các rủi ro liên quan đến việc cung cấp các dịch vụ ủy thác ký số từ xa qua việc tính đến các vấn đề kinh doanh và kỹ thuật;

CA2 Remote Signing lựa chọn các biện pháp xử lý rủi ro thích hợp, bằng cách tính đến các kết quả đánh giá rủi ro. Các biện pháp xử lý rủi ro đảm bảo rằng mức độ an toàn tương xứng với mức độ rủi ro;

CA2 Remote Signing xác định tất cả các yêu cầu bảo mật và quy trình hoạt động cần thiết để thực hiện các biện pháp đã chọn để xử lý rủi ro, như được nêu trong Chính sách bảo mật thông tin và trong Thực tiễn cung cấp các dịch vụ ủy thác ký số từ xa được cấp phép;

Ban quản lý điều hành của CA2 Remote Signing thường xuyên xem xét và sửa đổi đánh giá về rủi ro;

Ban quản lý điều hành của CA2 Remote Signing chịu trách nhiệm phê duyệt đánh giá rủi ro và ghi nhận rủi ro còn lại đã được xác định.

10.2. Quản lý và theo dõi sự cố

CA2 Remote Signing thực hiện giám sát và quản lý sự cố bằng cách áp dụng các yêu cầu sau:

- CA2 Remote Signing có ra các quy trình nghiêm ngặt để giám sát hoạt động của hệ thống công nghệ, việc truy cập vào hệ thống thông tin, cũng như các yêu cầu về dịch vụ ủy thác ký số từ xa;
- Các hoạt động giám sát phân tích và báo cáo tính nhạy cảm của từng phần thông tin được thu thập;
- Các trường hợp dịch vụ không khả dụng hoặc hoạt động bất thường của hệ thống cho thấy có khả năng vi phạm bảo mật, bao gồm cả việc xâm nhập vào mạng của CA2 Remote Signing, được phát hiện và báo cáo;
- Nhân sự được ủy quyền của CA2 Remote Signing giám sát các sự kiện sau:

+ Việc bắt đầu và tạm ngừng hoạt động vận hành;

+ Sự sẵn sàng và việc sử dụng các dịch vụ cần thiết thông qua mạng của CA2 Remote Signing;

- Trong các trường hợp vi phạm an ninh, CA2 Remote Signing có các thủ tục được đưa ra để phản ứng kịp thời, nhanh chóng và phối hợp nhằm hạn chế rủi ro vi phạm an ninh;

Các cảnh báo về sự cố an ninh được theo dõi và báo cáo bởi các nhân viên có vai trò tin cậy theo quy trình của Công ty;

- CA2 Remote Signing đã thiết lập một thủ tục để thông báo cho các cơ quan giám sát có liên quan phù hợp với các quy tắc quản lý hiện hành về bất kỳ vi phạm nào đối với bảo mật thông tin hoặc mất tính toàn vẹn có ảnh hưởng đáng kể đến dịch vụ ủy thác ký số từ xa được cung cấp, trong vòng 24 giờ sau khi phát hiện vi phạm;

Trong trường hợp vi phạm hoặc mất tính toàn vẹn bảo mật thông tin có khả năng ảnh hưởng xấu đến bất kỳ thể nhân hoặc pháp nhân nào được cung cấp dịch vụ ủy thác ký số từ xa, CA2 Remote Signing sẽ thông báo cho thể nhân hoặc pháp nhân tương ứng ngay lập tức;

- CA2 Remote Signing giám sát hệ thống công nghệ của mình và thường xuyên xem xét các dữ liệu kiểm toán để xác định bằng chứng cho bất kỳ hành vi sai trái nào. Công ty đã áp dụng các cơ chế tự động để xử lý các dữ liệu kiểm toán và cảnh báo cho nhân viên về các sự kiện quan trọng có thể xảy ra liên quan đến bảo mật;

- Hệ thống dịch vụ tạo ra các cảnh báo kịp thời để cảnh báo các sự kiện bất thường có thể ảnh hưởng đến khả năng của hệ thống đối với dịch vụ ký số theo các yêu cầu bảo mật (ví dụ: hoạt động của người dùng ngoài giờ làm việc tiêu chuẩn; các hành động gây ra bởi sự can thiệp không phải của con người; hoạt động của người dùng bên ngoài phạm vi hoạt động quy định tiêu chuẩn);

- Đối với mỗi lỗ hổng nghiêm trọng mới được phát hiện, trong vòng 48 giờ bắt buộc phải có giải pháp để giải quyết sau khi phát hiện;

- Đối với từng mối nguy cơ, căn cứ tác động tiềm tàng có thể, CA2 Remote Signing thực hiện:

+ Xây dựng kế hoạch giảm thiểu thiệt hại;

+ Ghi lại các dữ kiện và báo cáo cho ban quản lý điều hành.

- Các thủ tục báo cáo sự cố cho ban quản lý điều hành và phản hồi cho các quyết định được đưa ra được sử dụng để các biện pháp đã thực hiện có thể giảm thiểu bất kỳ thiệt hại nào và do đó các biện pháp trong tương lai được thực hiện để ngăn ngừa các sự cố đó.

10.3. Chính sách bảo mật thông tin

Chính sách An toàn Thông tin tập trung vào các yêu cầu liên quan đến chiến lược hoạt động, các quy định, luật pháp và hợp đồng, cũng như về môi trường hiện tại và có thể có của bất kỳ mối đe dọa nào đối với an ninh thông tin. Chính sách bảo mật bao gồm các tuyên bố, mục tiêu và nguyên tắc sẽ chi phối tất cả các hành động trong việc phân công các trách nhiệm chung và cụ thể liên quan đến việc quản lý an ninh cho các vai trò và quy trình nhất định để khắc phục mọi sai lệch, vi phạm và các tình huống khẩn cấp. Đặc biệt hơn, Chính sách An toàn Thông tin bao gồm các thủ tục mô tả các cơ chế kiểm soát an toàn thông tin: kiểm soát truy cập, phân loại thông tin, bảo mật vật lý và bảo mật của môi trường xung quanh, tài sản, trao đổi thông tin, làm việc từ xa, phần mềm được sử dụng, cơ chế mật mã cho kiểm soát, bảo mật thông tin liên lạc, bảo vệ dữ liệu cá nhân và mối quan hệ với các nhà cung cấp.

CA2 Remote Signing có Chính sách bảo mật thông tin đã được hoàn thiện và được ban quản lý điều hành phê duyệt, bao gồm những điều sau:

- Chính sách Bảo mật Thông tin xác định cách tiếp cận của CA2 Remote Signing đối với việc quản lý các hoạt động.
- Bất kỳ thay đổi nào đối với Chính sách bảo mật thông tin đều được thông báo cho bên thứ ba (người dùng, bên liên quan, cơ quan giám sát hoặc cơ quan quản lý khác, cơ quan đánh giá tuân thủ), nếu có.
- Chính sách bảo mật thông tin của CA2 Remote Signing được lập thành văn bản, triển khai và duy trì cập nhật.
- Tất cả nhân viên của CA2 Remote Signing đã được làm quen với Chính sách Bảo mật Thông tin.
- CA2 Remote Signing chịu trách nhiệm tuân thủ các quy trình được mô tả trong Chính sách Bảo mật Thông tin trong trường hợp CA2 Remote Signing ký hợp đồng phụ một phần hoạt động của mình. Nếu có các nhà thầu phụ, CA2 Remote Signing xác định trách nhiệm pháp lý của họ và đảm bảo rằng họ bị ràng buộc áp dụng nghiêm ngặt tất cả các biện pháp kiểm soát bảo mật thông tin theo yêu cầu của CA2 Remote Signing.

Chính sách Bảo mật Thông tin của CA2 Remote Signing và việc kiểm kê các tài sản bảo mật thông tin được xem xét theo các khoảng thời gian đã lên kế hoạch theo thời gian hoặc trong trường hợp có những thay đổi quan trọng, để đảm bảo tính phù hợp, đầy đủ và hiệu quả liên tục của chúng.

- Bất kỳ thay đổi nào có thể ảnh hưởng đến mức độ an toàn bảo mật được cung cấp đều phải được cơ quan quản lý Nhà nước chấp thuận.
- Cấu hình của hệ thống CA2 Remote Signing thường xuyên được kiểm tra để phát hiện những thay đổi vi phạm các quy tắc bảo mật thông tin. Khoảng thời gian tối đa giữa hai lần xác nhận dựa trên các quy trình nội bộ của CA2 Remote Signing.

Ngoài ra những yêu cầu sau được áp dụng:

- Tài liệu chính sách Bảo mật Thông tin ghi lại các biện pháp kiểm soát bảo mật được phổ biến để bảo vệ dữ liệu cá nhân. Trong quá trình xử lý dữ liệu cá nhân, CA2 Remote Signing tuân thủ tất cả các quy định bảo vệ dữ liệu cá nhân áp dụng cho hoạt động của mình, bao gồm nhưng không giới hạn ở Quy định của pháp luật. Chính sách Bảo vệ Dữ liệu Cá nhân là một phần không thể tách rời của Hợp đồng sử dụng dịch vụ. Trong trường hợp có bất kỳ thay đổi nào đối với Chính sách Bảo vệ Dữ liệu Cá nhân, các thay đổi được công bố trên trang web của CA2 Mobile Sign: https://www.mobilesign.vn/. CA2 Mobile Sign thực hiện tất cả các bước cần thiết, bao gồm các biện pháp kỹ thuật và tổ chức, dựa trên mức độ rủi ro của quá trình xử lý dữ liệu cá nhân được thực hiện, nhằm đảm bảo an ninh dữ liệu để không có sự phá hủy, mất mát, thay đổi ngẫu nhiên hoặc trái phép, tiết lộ trái phép, truy cập hoặc khác Có thể cho phép sự kiện bất hợp pháp hoặc không mong muốn có thể ảnh hưởng đến tính bảo mật của dữ liệu cá nhân được xử lý. CA2 Remote Signing thu thập thông tin số lượng tương ứng với mục đích và yêu cầu sử dụng. Từng cá nhân phải đồng thuận với việc xử lý dữ liệu cá nhân. Sự đồng ý này được tuyên bố bằng cách ký Hợp đồng cung cấp và sử dụng dịch vụ ủy thác ký số từ xa. Dữ liệu cá nhân chỉ được sử dụng liên quan đến việc cung cấp dịch vụ ủy thác ký số từ xa.

10.4. Quản lý tài sản

CA2 Remote Signing quản lý tài sản áp dụng theo các yêu cầu sau:

CA2 Mobile Sign thiết lập mức độ bảo vệ thích hợp đối với tài sản của mình, bao gồm cả tài sản thông tin của nó.

CA2 Remote Signing quản lý danh sách kiểm kê của tất cả các tài sản thông tin và phân loại tài sản này dựa trên đánh giá rủi ro.

Đối với các thư viện mật mã CA2 Remote Signing chỉ sử dụng thư viện mật mã tiêu chuẩn đã được kiểm nghiệm công nhận quốc tế.

10.5. Sao lưu dự phòng

CA2 Remote Signing sao lưu điện tử tất cả các sự kiện quan trọng, tất cả dữ liệu và tệp liên quan đến thủ tục đăng ký và thẩm định thuê bao, bảo mật hệ thống, hợp đồng với các bên và nhà cung cấp, các thông tin thiết yếu khác liên quan đến việc cung cấp dịch vụ ủy thác ký số từ xa. Bản sao lưu điện tử được quản lý và lưu trữ an toàn, quyền truy cập chỉ giới hạn ở các nhân viên có thẩm quyền. Bản sao lưu điện tử được ký bằng dấu thời gian số. Dữ liệu bản ghi trong nhật ký được ghi định kỳ trên các phương tiện lưu trữ vật lý, lưu giữ bảo vệ trong két sắt gửi an toàn đặt trong phòng có mức độ bảo vệ vật lý và kiểm soát truy an ninh cập cao. Bản sao lưu trên giấy được lưu trữ tuân thủ tất cả các yêu cầu về quy trình lưu trữ tài liệu an toàn.

Thời gian lưu trữ theo quy định của pháp luật, CA2 Remote Signing lưu trữ tối thiểu 7 năm.

10.6. Sử dụng các phương tiện vận hành khác nhau

Tất cả các phương tiện được xử lý an toàn phù hợp với các yêu cầu của quy định phân loại thông tin. Phương tiện chứa dữ liệu nhạy cảm không còn cần thiết sẽ được xử lý theo quy trình an toàn. Tất cả các phương tiện chứa phần mềm, bản sao lưu dữ liệu hoặc thông tin kiểm toán được lưu trữ trong hộp chống cháy trong phòng có kiểm soát an ninh ra vào. CA2 Remote Signing thực hiện các biện pháp nghiêm ngặt chống lại thiệt hại do vô tình hoặc cố ý đối với phương tiện dữ liệu.

10.7. Hủy rác

Tất cả các phương tiện giấy và phương tiện điện tử có chứa thông tin quan trọng tiềm ẩn về tính an toàn bảo mật của CA2 Remote Signing đều bị hủy, sử dụng các thiết bị băm nhỏ chuyên biệt sau khi hết thời hạn lưu trữ theo quy định và quy trình nội bộ.

Phương tiện với thông tin về khóa mật mã và mã PIN / PUK bị nghiền nát bằng cách sử dụng các thiết bị phù hợp. Quy định áp dụng cho phương tiện không thể xóa vĩnh viễn dữ liệu.

Trong một số trường hợp nhất định, thông tin trong thiết bị sẽ bị phá hủy theo quy trình xóa hoặc format để thiết bị không có khả năng khôi phục.

11. YÊU CẦU KỸ THUẬT APP CA2 GIAO TIẾP KÝ CHỮ KÝ SỐ TỪ XA

11.1. Giao diện (Lược đồ các thành phần theo kiến trúc VN hiện tại)

- Căn cứ Mục ASI-8.1-01 của bộ TC ETSI 119 431-2 về yêu cầu giao thức truy cập giữa SCASC (Hệ thống ứng dụng nghiệp vụ hay Hệ thống xử lý trung gian của dịch vụ CA2 Remote Signing) và các dịch vụ của nó (CA2 Remote Signing), APP CA2 áp dụng: giao thức truy cập theo chuẩn RESTful API, đáp ứng giao diện quy định trong ETSI 119 432
- Căn cứ Mục ASI-8.1-02 của bộ TC ETSI 119 431-2 về bảo mật kết nối giữa SCASC và SCDev (HSM), APP CA2 đảm bảo tuân thủ bảo mật kết nối với SCASC sử dụng cơ chế an toàn, bảo mật dựa trên chữ ký số.
- APP CA2 đảm bảo đáp ứng tiêu chí WYSIWYS theo mục ASI-8.1-03 của bộ TC ETSI 119 431-2
- Đối với các tài liệu được trình bày theo cách diễn giải (VD: XML document), APP CA2 chỉ rõ phần mềm sử dụng tài liệu đó cũng như cấu trúc diễn giải cụ thể, đáp ứng mục ASI-8.1-04 của bộ TC ETSI 119 431-2
- APP CA2 sẽ chỉ định rõ loại tài liệu nào sẽ được trình bày đầy đủ khi nhận được yêu cầu trình tài liệu cho người ký từ SCASC, đáp ứng mục ASI-8.1-05 của bộ TC ETSI 119 431-2
- APP CA2 sẽ có giao diện cảnh báo với người dùng nếu không thể trình bày chính xác tất cả các phần dữ liệu ký theo kiểu dữ liệu, đáp ứng đáp ứng mục ASI-8.1-06 của bộ TC ETSI 119 431-2
- APP CA2 đáp ứng đầy đủ các yêu cầu về giao diện từ U1 đến U2, được quy định trong bộ TC ETSI TS 119 101, đáp ứng mục ASI-8.1-07 của bộ TC ETSI 119 431-2
- APP CA2 áp dụng quy trình xác thực chính xác người ký đồng ý với việc ký tài liệu được xuất trình từ SCASC, đáp ứng mục ASI-8.1-08 của bộ TC ETSI 119 431-2
- APP CA2 đảm bảo đáp ứng yêu cầu SD được trình ký với người ký sẽ giống với SD sẽ được ký theo mục ASI-8.1-09 của bộ TC ETSI 119 431-2
- APP CA2 cho phép tải về tài liệu cần ký, đáp ứng mục ASI-8.1-10 của bộ TC ETSI 119 431-2
- Thành phần SCASC giao tiếp với APP CA2 ghi nhận thời gian tài liệu xuất trình cho người ký, đáp ứng mục ASI-8.1-11 của bộ TC ETSI 119 431-2

- Thành phần SCASC giao tiếp với APP CA2 cũng ghi nhận thời gian tài liệu xuất trình cho người ký được tải xuống, đáp ứng mục ASI-8.1-12 của bộ TC ETSI 119 431-2

11.2. Yêu cầu về tạo chữ ký số AdES

- CA2 Remote Signing áp dụng chữ ký số DSV
- Chữ ký số AdES sẽ được triển khai áp dụng khi có quy định của Bộ TTTT.